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

(11) EP 0 996 097 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
26.04.2000 Patentblatt 2000/17

(51) Int. Cl.[7]: **G07B 17/04**

(21) Anmeldenummer: **00250033.8**

(22) Anmeldetag: **21.11.1995**

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
LT LV SI

(30) Priorität: **15.12.1994 DE 4446667**

(62) Dokumentnummer(n) der früheren Anmeldung(en) nach Art. 76 EPÜ:
95250286.2 / 0 717 379

(71) Anmelder:
Francotyp-Postalia Aktiengesellschaft & Co.
16547 Birkenwerder (DE)

(72) Erfinder:
- **Bischoff, Enno**
  13189 Berlin (DE)
- **Gelfer, George G.**
  Glen Ellyn, IL 60137 (US)
- **Thiel, Wolfgang, Dr.**
  13503 Berlin (DE)
- **Wagner, Andreas**
  13503 Berlin (BE)

Bemerkungen:
Diese Anmeldung ist am 02 - 02 - 2000 als Teilanmeldung zu der unter INID-Kode 62 erwähnten Anmeldung eingereicht worden.

(54) Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen bei der Guthabenübertragung

(57) Die Erfindung betrifft ein Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen bei der Guthabenübertragung, mit mindestens zwei Modi. Im Ergebnis des Überwachens einer autorisierten Handlung an der Frankiermaschine, wird in einem Schritt (209) der Systemroutine (200) ein. Sicherheits-Flag X gelöscht und bei seinem Fehlen die Frankiermaschine in einen ersten Modus überführt (Schritt 409), um sie damit wirksam außer Betrieb zu setzen. Anderenfalls wird in einem Sondermodus negative Fernwertvorgabe durch Setzen eines Sonder-Flags N eingetreten, wenn die vorbestimmte Bedienhandlung zum Seiteneinstieg in den Sondermodus beim Einschalten vorgenommen wird. Die Kommunikation (300) mit der Datenzentrale läuft unter zeitlicher und zustandsmäßiger (Flags) Überwachung durch die Steuereinheit der Frankiermaschine bis zur Vollendung der Transaktion ab. Von der Datenzentrale wird das Verhalten des Frankiermaschinenbenutzers auf der Basis von während der Kommunikation übermittelten Daten überwacht.

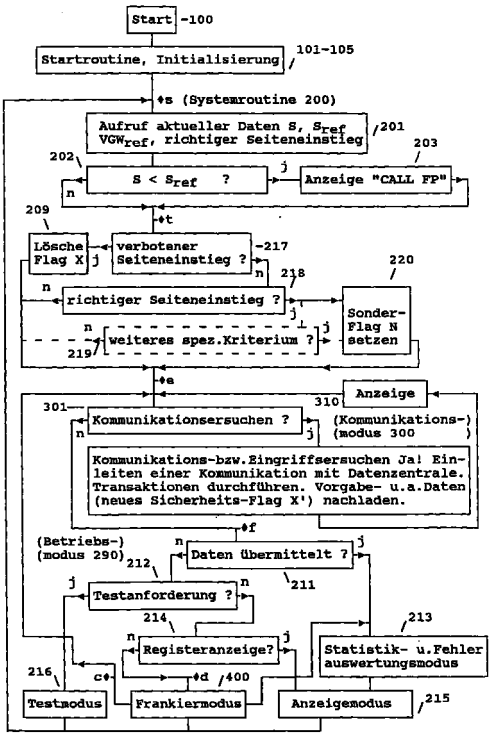

Fig. 2

EP 0 996 097 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen bei der Guthabenübertragung, speziell bei der Fondsrückübertragung zur Datenzentrale, gemäß der im Oberbegriff des Anspruchs 1 bzw. 3 angegebenen Art.

[0002] Eine Frankiermaschine erzeugt in der Regel einen Aufdruck in einer mit der Post vereinbarten Form rechtsbündig, parallel zur oberen Kante des Postgutes beginnend mit dem Inhalt Postwert im Poststempel, Datum im Tagesstempel und Stempelabdrucke für Werbeklischee und ggf. Sendungsart im Wahldruckstempel. Der Postwert, das Datum und die Sendungsart bilden hierbei die entsprechend dem Poststück einzugebenden variablen Informationen.

[0003] Beim Postwert handelt es sich meist um die vom Absender vorausbezahlte Beförderungsgebühr (Franko), die einen wiederauffüllbaren Guthabenregister entnommen und zum Freimachen der Postsendung verwendet wird. Im Gegensatz dazu wird beim Kontokorrentverfahren ein Register in Abhängigkeit von den mit dem Postwert vorgenommenen Frankierungen lediglich hochgezählt und in regelmäßigen Abständen, von einem Postinspektor abgelesen.

[0004] Grundsätzlich ist jede vorgenommene Frankierung abzurechnen und jede Manipulation, welche zu einer nichtabgerechneten Frankierung führt, muß verhindert werden.

[0005] Eine bekannte Frankiermaschine ist mit mindestens einem Eingabemittel, einem Ausgabemittel, einem Ein/Ausgabe-Steuermodul, einer Programm-, Daten- und insbesondere die Abrechnungsregister tragenden Speichereinrichtung, einer Steuereinrichtung und einem Druckermodul ausgerüstet. Bei einem Drukkermodul mit Druckmechanik müssen auch Maßnahmen ergriffen werden, damit im ausgeschalteten Zustand die Druckmechanik nicht für unabgerechnete Abdrucke mißbraucht werden kann.

[0006] Die Erfindung betrifft ein Verfahren für Frankiermaschinen, die einen vollelektronischen erzeugten Abdruck zum Frankieren von Postgut einschließlich Abdruck eines Werbeklischees liefern. Das hat zur Folge, daß nur noch im eingeschalteten Zustand ein nicht abgerechnetes gültiges Frankieren verhindert werden muß.

[0007] Bei einer aus der US 4 746 234 bekannten Frankiermaschine werden feste und variable Informationen in Speichermitteln (ROM, RAM) gespeichert, um diese dann, wenn ein Brief auf dem Transportpfad vor der Druckposition einen Mikroschalter betätigt, mittels eines Mikroprozessors auszulesen und um ein Drucksteuersignal zu bilden. Beide sind danach elektronisch zu einem Druckbild zusammengesetzt und können durch Thermotransferdruckmittel auf einen zu frankierenden Briefumschlag ausgedruckt werden.

[0008] Es wurde auch bereits ein Verfahren zum Steuern des spaltenweisen Druckens eines Postwertzeichenbildes in einer Frankiermaschine vorgeschlagen EP 578 042 A2, welches getrennt voneinander in graphische Pixelbilddaten umgesetzte feste und variable Daten während des spaltenweisen Druckens zusammensetzt. Es wäre daher schwierig, ohne großen und teuren Aufwand eine Manipulation am Drucksteuersignal vorzunehmen, wenn das Drucken mit einer hohen Geschwindigkeit erfolgt.

[0009] Andererseits umfaßt die Speichereinrichtung mindestens einen nichtflüchtigen Speicherbaustein, der das aktuell verbliebene Restguthaben enthält, welches daraus resultiert, daß von einem früher in die Frankiermaschine geladenen Guthaben der jeweilige zu druckenden Portowert abgezogen wird. Die Frankiermaschine blockiert, wenn das Restguthaben Null ist.

[0010] Bekannte Frankiermaschinen enthalten in mindestens einem Speicher drei relevante Postregister für verbrauchten Summenwert (steigendes Register), noch verfügbares Restguthaben (fallendes Register) und Register für eine Kontrollsumme. Die Kontrollsumme wird mit der Summe aus verbrauchten Summenwert und aus verfügbaren Guthaben verglichen. Bereits damit ist eine Überprüfung auf richtige Abrechnung möglich.

[0011] Weiterhin ist es auch möglich von einer Datenzentrale über eine Fernwertvorgabe eine Wiederaufladeinformation zur die Frankiermaschine zu übertragen, um in das Register für das Restguthaben (Restwert) ein Guthaben nachzuladen. Es versteht sich von selbst, daß hierfür geeignete Sicherheitsmaßnahmen getroffen werden müssen, damit das in der Frankiermaschine gespeicherte Guthaben nicht in unbefugter Art und Weise aufgestockt werden kann. Die vorgenannten Lösungen gegen Mißbrauch und Fälschungsversuche zu schützen, erfordert einen zusätzlichen materiellen und zeitlichen Aufwand.

[0012] Aus der US 48 64 506 ist bekannt, daß wenn der Wert des Guthabens im fallenden Register unter einem Schwellwert liegt und eine vorbestimmte Zeit erreicht ist, eine Kommunikation zur entfernten Datenzentrale von der Frankiermaschine aufgenommen wird.

[0013] Aus o.g. Patent ist weiterhin bekannt, daß die Datenzentrale zum Empfang von Registerdaten und zur Kontrolle, ob die Frankiermaschine noch an eine bestimmte Telefonnummer angeschlossen ist - die Verbindung mit der Frankiermaschine nach einer definierten Zeitdauer aufnimmt und die Frankiermaschine nur zu vorbestimmten Zeiten antwortet.

[0014] Es ist nach o.g. Patent außerdem vorgesehen, vor einer Guthabennachladung in die Frankiermaschine, zur Autorisierung durch die Datenzentrale die Identitätsnummer der Frankiermaschine und die Werte im fallenden und steigenden Register abzufragen.

[0015] Weiterhin ist aus o.g. Patent bekannt, daß die Kommunikation der Datenzentrale mit der Frankiermaschine nicht auf bloße Guthabenübertragung in die Frankiermaschine beschränkt bleiben braucht. Vielmehr wird im Falle einer Abmeldung der Frankierma-

schine die Kommunikation der Datenzentrale mit der Frankiermaschine zur Übertragung des Restguthabens der Frankiermaschine in die Datenzentrale genutzt. Der Wert im fallenden Postregister der Frankiermaschine ist dann Null, was die Frankiermaschine wirksam außer Betrieb setzt.

[0016] Ein Sicherheitsgehäuse für Frankiermaschinen, welches innere Sensoren aufweist, ist aus der DE 41 29 302 A1 bekannt. Die Sensoren sind insbesondere mit einer Batterie verbundene Schalter, welche beim Öffnen des Sicherheitsgehäuses aktiv werden, um einen das Restwertguthaben speichernden Speicher (fallendes Postregister) durch Unterbrechen der Energiezufuhr zu löschen. Es ist bekanntlich aber nicht vorhersagbar, welchen Zustand ein spannungsloser Speicherbaustein beim Wiederkehr der Spannung einnimmt. Somit könnte auch ein nicht bezahltes höheres Restguthaben entstehen. Andererseits kann nicht ausgeschlossen werden, daß sich auf oben genannte Weise, das Restwertguthaben zumindest teilweise entlädt. Das wäre aber bei einer Inspektion nachteilig, da das Restwertguthaben, welches vom Frankiermaschinennutzer bezahlt worden war, auch wieder geladen werden muß, die Höhe dieses Restguthabens jedoch durch o.g. Einflüsse verfälscht sein kann. Schließlich ist der Beschreibung nicht entnehmbar, wie verhindert werden kann, daß ein Manipulator ein nicht bezahltes Restguthaben wieder herstellt.

[0017] Bei bekannten Frankiermaschinen FM sind bereits weitere Sicherheitsmaßnahmen wie Wegbrechschrauben und gekapseltes abgeschirmtes Sicherheitsgehäuse bekannt. Üblich sind auch Schlüssel und ein Zahlenschloß um den Zugriff auf die Frankiermaschine zu erschweren.

[0018] In der US 4 812 994 soll ein unautorisierter Zugriff einer Benutzung der Frankiermaschine darüber hinaus durch Sperrung der Frankiermaschine bei Falscheingabe eines vorbestimmten Paßwortes verhindert werden. Außerdem kann die Frankiermaschine mittels Paßwort und entsprechender Eingabe über Tastatur so eingestellt werden, daß ein Frankieren nur während eines vorbestimmten Zeitintervalls bzw. Tageszeiten möglich ist.

[0019] Das Paßwort kann durch einen Personalcomputer über MODEM, durch eine Chipkarte oder manuell in die Frankiermaschine eingegeben werden. Nach positiven Vergleich mit einem in der Frankiermaschine gespeicherten Paßwort wird die Frankiermaschine freigegeben. Im Steuermodul der Abrechnungseinheit ist ein Sicherheitsmodul (EPROM) integriert. Als weitere Sicherheitsmaßnahme ist ein Verschlüsselungsmodul (separater Mikroprozessor oder Programm für FM-CPU basierend auf DES-oder RSA-Code) vorgesehen, der eine den Portowert, die Teilnehmernummer, eine Transaktionsnummer und ähnliches umfassende Erkennungsnummer im Frankierstempel erzeugt. Bei genügend krimineller Energie könnte aber auch ein Paßwort ausgeforscht und samt Frankiermaschine in den Besitz eines Manipulators gebracht werden.

[0020] Es ist bereits in der US 4,812,965 ein Ferninspektionssystem für Frankiermaschinen vorgeschlagen worden, welches auf speziellen Mitteilungen im Abdruck von Poststücken, die der Zentrale zugesandt werden müssen, oder auf einer Fernabfrage über MODEM basiert. Sensoren innerhalb der Frankiermaschine sollen jede vorgenommene Verfälschungshandlung detektieren, damit in zugehörigen Speichern ein Flag gesetzt werden kann, falls in die Frankiermaschine zu Manipulationszwecken eingegriffen wurde. Ein solcher Eingriff könnte erfolgen, um ein nicht bezahltes Guthaben in die Register zu laden.

[0021] Bei Feststellung einer Manipulation wird die Frankiermaschine während der Ferninspektion über Modem durch ein von der Datenzentrale ausgehendes Signal gesperrt. Eine geschickte Manipulation könnte aber andererseits darin bestehen, nach der Herstellung von nicht abgerechneten Frankieraufdrucken, das Flag und die Register in den ursprünglichen Zustand zurückzuversetzen. Eine solche Manipulation wäre über Ferninspektion durch die Datenzentrale nicht erkennbar, wenn diese rückgängig gemachte Manipulation vor der Ferninspektion lag. Auch der Empfang der Postkarte von der Datenzentrale, auf welche eine zu Inspektionszwecken vorzunehmende Frankierung erfolgen soll, gestattet dem Manipulator die Frankiermaschine in ausreichender Zeit in den ursprünglichen Zustand zurückzuversetzen. Damit ist also noch keine höhere Sicherheit erreichbar.

[0022] Der Nachteil eines solchen Systems besteht darin, daß nicht verhindert werden kann, daß ein genügend qualifizierter Manipulator, welcher in die Frankiermaschine einbricht, seine hinterlassenen Spuren nachträglich beseitigt, indem die Flags gelöscht werden. Auch kann damit nicht verhindert werden, daß der Abdruck selbst manipuliert wird, welcher von einer ordnungsgemäß betriebenen Maschine hergestellt wird. Bei bekannten Maschinen besteht die Möglichkeit, einer Herstellung von Abdrucken mit dem Portowert Null. Derartige Nullfrankierungen werden zu Testzwecken benötigt, und könnten auch nachträglich gefälscht werden, indem ein Portowert größer Null vorgetäuscht wird.

[0023] Ein Sicherheitsabdruck gemäß der FP-eigenen europäische Patentanmeldung EP 576 113 A2 sieht Symbole in einem Markierungsfeld im Frankierstempel vor, die eine kryptifizierte Information enthalten. Dies gestattet der Postbehörde, welche mit der Datenzentrale zusammenwirkt, aus dem jeweiligem Sicherheitsabdruck eine Erkennung einer Manipulation an der Frankiermaschine zu beliebigen Zeitpunkten. Zwar ist eine laufende Kontrolle solcher mit einem Sicherheitsabdruck versehenen Poststⁿcke ⁿber entsprechende Sicherheitsmarkierungen im Stempelbild technisch möglich, jedoch bedeutet das einen zusätzlichen Aufwand im Postamt. Bei einer auf Stichproben beruhenden Kontrolle, wird aber eine Manipulation in

der Regel erst spät festgestellt.

[0024] Andererseits kann im Datenzentrum eine zusätzliche Auswertung hinsichtlich eines Nutzers einer Frankiermaschine, die vom Nutzer über das Inspektionsdatum hinaus weiterbetrieben wurde, erfolgen. Jedoch kann bisher aus diesen Informationen noch nicht eine in Fälschungsabsicht vorgenommene Manipulation geschlußfolgert werden.

[0025] In der US 4 251 874 wird ein mechanisches Druckwerk, das zum Drucken voreingestellt werden muß, mit einer Detektoreinrichtung verwendet, um die Voreinstellung zu überwachen. Ferner sind im elektronischen Abrechnungssystem Mittel zum Feststellen von Fehlern in Daten- und Steuersignalen vorgesehen. Erreicht diese Fehlerzahl einen vorgegebenen Wert, wird der weitere Betrieb der Frankiermaschine unterbrochen. Der plötzliche Ausfall der Frankiermaschine ist aber für den Frankiermaschinenbenutzer nachteilig. Bei einem nichtmechanischen Druckprinzip sind andererseits kaum solche internen Fehler zu erwarten und bei einem schweren Fehler ist die Frankiermaschine ohnehin sowieso sofort abzuschalten. Außerdem wird die Sicherheit gegenüber einer Manipulation der Frankiermaschine dadurch kaum größer, indem die Frankiermaschine nach einer vorbestimmten Fehleranzahl abgeschaltet wird.

[0026] Aus der US 4 785 417 ist eine Frankiermaschine mit einer Programmsequenzüberwachung bekannt. Der korrekte Ablauf eines größeren Programmstücks wird mittels eines jedem Programmteil zugeordneten speziellen Codes kontrolliert, der bei Aufruf des Programmstücks in einer bestimmten Speicherzelle im RAM abgelegt wird. Es wird nun überprüft, ob der in der vorgenannten Speicherzelle abgelegte Code im gerade ablaufenden Programmteil immer noch vorhanden ist. Würde bei einer Manipulation der Lauf eines Programmteils unterbrochen und ein anderer Programmteil läuft ab, kann durch eine solche Kontrollfrage ein Fehler festgestellt werden. Der Vergleich kann aber nur im Hauptablauf durchgeführt werden. Nebenabläufe, beispielsweise sicherheitsrelevante Berechnungen, welche von mehreren Hauptabläufen benutzt werden, können durch eine solche Überwachung auf Ausführung des Programmteils jedoch nicht kontrolliert werden, weil die Programmkontrolle unabhängig vom Programmablauf erfolgt. Wird auf der Basis von erlaubten Programmteilen und Nebenabläufen so manipuliert, daß Nebenabläufe zusätzlich in Hauptabläufe eingebunden oder aus lezteren weggelassen werden oder auf Nebenabläufe verzweigt wird, dann würde kein Fehler festgestellt werden, da weder die Länge des Programmteils festgestellt, noch festgestellt werden kann, welcher Programmzweig wie oft durchlaufen wurde.

[0027] Eine andere Art einer erwarteten Manipulation ist das Nachladen der Frankiermaschinenregister mit einem nicht abgerechneten Guthabenwert. Damit ergibt sich das Erfordernis einer gesicherten Nachladung. Eine zusätzliche Sicherheitsmaßnahme ist nach US 4 549 281 der Vergleich einer internen in einem nichtflüchtigen Register gespeicherten festen Kombination mit einer eingegebenen externen Kombination, wobei nach einer Anzahl an Fehlversuchen, d.h. Nichtidentität der Kombinationen, die Frankiermaschine mittels einer Hemmungselektronik gesperrt wird. Nach US 4 835 697 kann zur Verhinderung eines unautorisierten Zugriffs auf die Frankiermaschine die Kombination grundsätzlich gewechselt werden.

[0028] Aus der US 5,077,660 ist außerdem eine Methode zum Wechsel der Konfiguration der Frankiermaschine bekannt, wobei die Frankiermaschine mittels geeigneter Eingabe über eine Tastatur vom Betriebsmode in einen Konfigurationsmode umgeschaltet und eine neue Metertypnummer eingegeben werden kann, welche der gewünschten Anzahl an Merkmalen entspricht. Die Frankiermaschine generiert einen Code für die Kommunikation mit dem Computer der Datenzentrale und die Eingabe der Identifikationsdaten und der neuen Metertypnummer in vorgenannten Computer, der ebenfalls einen entsprechenden Code zur Übermittlung und Eingabe in die Frankiermaschine generiert, in der beide Code verglichen werden. Bei Übereinstimmung beider Code wird die Frankiermaschine konfiguriert und in den Betriebsmode umgeschaltet. Die Datenzentrale hat dadurch vom jeweils eingestellten Metertyp für die entsprechende Frankiermaschine immer genaue Aufzeichnungen. Jedoch ist die Sicherheit allein von der Verschlüsselung der übertragenen Code abhängig.

[0029] Darüber hinaus ist aus der EP 388 840 A2 eine vergleichbare Sicherheitstechnik für ein Setzen einer Frankiermaschine bekannt, um diese von Daten zu säubern, ohne daß die Frankiermaschine zur Herstellerfirma transportiert werden muß. Auch hier ist die Sicherheit allein von der Verschlüsselung der übertragenen Code abhängig.

[0030] Die gesicherte Nachladung einer Frankiermaschine mit einem Guthaben wurde in US 3 255 439 einerseits bereits mit einer automatischen Signalübertragung von der Frankiermaschine zur Datenzentrale verbunden, wenn immer eine vorbestimmte Geldmittelsumme, welche frankiert wurde, oder Stückzahl an bearbeiteten Poststücken oder eine vorbestimmte Zeitperiode erreicht wurde. Alternativ kann ein der Geldmittelsumme, Stückzahl oder Zeitperiode entsprechendes Signal übermittelt werden. Dabei erfolgt die Kommunikation mittels binärer Signale über miteinander über eine Telefonleitung verbundene Konverter. Die Maschine erhält eine ebenso gesicherte Nachladung entsprechend der Kreditbalance und blockiert in dem Fall, wenn kein Kredit nachgeliefert wird.

[0031] Aus der US 4 811 234 ist bekannt, die Transaktionen verschlüsselt durchzuführen und dabei die Register der Frankiermaschine abzufragen und die Registerdaten der Datenzentrale zu übermitteln, um einen zeitlichen Bezug der Verringerung des im Register gespeicherten verfügungsberechtigten Betrages

anzuzeigen. Einerseits identifiziert sich die Frankiermaschine bei der Datenzentrale, wenn ein voreinstellbarer Schwellwert erreicht ist, mittels ihres verschlüsselten Registerinhaltes. Andererseits modifiziert die Datenzentale durch entsprechende Berechtigungssignale den gewünschten Frankierbetrag, bis zu dem frankiert werden darf. Die Verschlüsselung ist somit die einzige Sicherheit gegen eine Manipulation der Registerstände. Wenn also ein Manipulator zwar ordnungsgemäß immer den gleichen Betrag in gleichen zeitlichen Intervallen lädt, aber zwischenzeitlich mit der manipulierten Frankiermaschine einen viel höheren Betrag frankiert, als er bezahlt hat, kann die Datenzentrale keine Manipulation feststellen.

[0032] Aus der EP 516 403 A2 ist bekannt, die in der Vergangenheit protokollierten und in einem Speicher gespeicherten Fehler der Frankiermaschine regelmäßig zu einem entfernten Fehleranalysecomputer zur Auswertung zu übertragen. Eine solche Ferninspektion erlaubt eine frühe Warnung vor einem auftretenden Fehler und ermöglicht weitere Maßnahmen (Service) zu ergreifen. Allein dies bietet noch kein ausreichendes Kriterium für eine Manipulation.

[0033] Gemäß der GB 22 33 937 A und US 5 181 245 kommuniziert die Frankiermaschine periodisch mit der Datenzentrale. Ein Blockiermittel gestattet die Frankiermaschine nach Ablauf einer vorbestimmten Zeit bzw. nach einer vorbestimmten Anzahl an Operationszyklen, zu blockieren und liefert eine Warnung an den Benutzer. Zum Freischalten muß von außen ein verschlüsselter Code eingegeben werden, welcher mit einem intern erzeugten verschlüsselten Code verglichen wird. Um zu verhindern, daß falsche Abrechnungsdaten an die Datenzentrale geliefert werden, werden in die Verschüsselung des vorgenannten Codes die Abrechnungsdaten mit einbezogen. Nachteilig ist, daß die Warnung zugleich mit dem Blockieren der Frankiermaschine erfolgt, ohne daß der Benutzer eine Möglichkeit hat, sein Verhalten rechtzeitig entsprechend zu ändern.

[0034] Aus der US 5 243 654 ist eine Frankiermaschine bekannt, wo die laufenden von Uhr/Datumsbaustein gelieferten Zeitdaten mit gespeicherten Stillegungszeitdaten verglichen werden. Ist die gespeicherte Stillegungszeit durch die laufende Zeit erreicht, wird die Frankiermaschine deaktiviert, das heißt ein Drucken verhindert. Bei Verbindungsaufnahme mit einer Datenzentrale, welche die Abrechnungsdaten aus dem steigenden Register ausliest, wird der Frankiermaschine ein verschlüsselter Kombinationswert übermittelt und eine neue Frist gesetzt, wodurch die Frankiermaschine wieder betriebsfähig gemacht wird. Dabei ist der Verbrauchssummenbetrag, der das verbrauchte Porto summiert enthält und von der Datenzentrale gelesen wird, ebenfalls Bestandteil des verschlüsselt übermittelten Kombinationswertes. Nach der Entschlüsselung des Kombinationswertes wird der Verbrauchssummenbetrag abgetrennt und mit dem in der Frankiermaschine gespeicherten Verbrauchssummenbetrag verglichen. Ist der Vergleich positiv, wird die Sperre der Frankiermaschine automatisch aufgehoben. Durch diese Lösung wird erreicht, daß sich die Frankiermaschine bei der Datenzentrale periodisch meldet, um Abrechnungsdaten zu übermitteln. Es sind jedoch Benutzungsfälle durchaus denkbar, wo das zu frankierende Postaufkommen schwankt (Saisonbetrieb). In diesen Fällen würde in nachteiliger Weise die Frankiermaschine unnötig oft blockiert werden.

[0035] Aus der US 4.760.532 ist ein Postbehandlungssystem mit Postwertübertragungs- und Abrechnungsfähigkeit bekannt. Dabei werden Informationen an das Datenzentrum via Telefon mittels des in den USA verbreiteten touch-tone Verfahrens übermittelt. Durch Drücken einer entsprechenden Taste des Telefons kann der Bediener eine Ziffer übertragen. Informationen vom Datenzentrum werden mittels Computerstimme an den Bediener übertragen, welcher die übertragenen Werte in die Frankiermaschine eingeben muß. Zur Fondsrückübertragung ist das Transferieren eines negativen postalischen Funds zu einem Postgerät in einem ersten Schritt zur Errichtung einer Kommunikation mit einer Zentralstation vorgesehen. Die Zentralstation überwacht die Gesamtsumme an Post (Restwertguthaben), die in dem Postgerät gespeichert ist. In einem zweiten Schritt erfolgt die Versorgung der vorgenannten Zentralstation mit einer auf einen gewünschten Wechsel bezogene Information, um die Gesamtsumme an Postwerten zu reduzieren, die in vorgenannten Postgerät verfügbar ist, und mit einer eindeutigen Identifikation betreff des vorgenannten Postgerätes. Ein dritter Schritt beinhaltet ein, Empfangen von der Zentralstation und Eingabe eines ersten eindeutigen Codes in das vorgenannte Postgerät, wobei das Eingeben betrieben wird, um die Gesammtsumme an Postwerten, die in dem Postgerät gespeichert sind, in Übereinstimmung mit vorgenanntem Wunsch zu reduzieren. Und im vierten Schritt ist ein Generieren eines zweiten eindeutigen Codes in dem Postgerät vorgesehen, wenn der erste eindeutige Code in das Postgerät eingegeben wurde, wobei der zweite eindeutige Code eine Indikation derart liefert, daß der vorgenannte Postwert, der zum Bedrucken der Post zur Verfügung steht, in vorgenannten Postgerät reduziert worden ist. Ist jedoch die Übertragung gestört bzw. unterbrochen, dann wird von der Datenzentrale kein erster Code empfangen und der Fonds in der Frankiermaschine bliebe unverändert, während in der Datenzentrale bereits eine Rückbuchung vorgenommen worden ist. Zur Überprüfung könnten natürlich die Registerstände der Frankiermaschine abgefragt werden, um diese mit den in der Datenzentrale gespeicherten zu vergleichen. Es ist zu befürchten, daß ein potentieller Manipulator letzteres unterlassen würde. In US 4,760,532 ist als abschliessender Verfahrensschritt das Übertragen des vorgenannten zweiten eindeutigen Codes zu der Zentralstation vorgesehen. Unter den

Bedingungen des touch-tone Verfahrens ist wieder das Betätigen von Zifferntasten erforderlich, was bei mehrstelligen Code umständlich und in der Regel nicht frei von Eingabefehlern abläuft. Außerdem ist vorgesehen, seitens der Datenzentrale einen dritten eindeutigen Code zu generieren, um das rückübertragene Guthaben an eine andere Frankiermaschine zu übertragen. Somit kann die verantwortliche Behörde durch Fehler während der Übertragung geschädigt werden. Damit tritt bei der positiven wie negativen Fernwertvorgabe die selbe Frage auf, nämlich danach, wie auf einfache Art und Weise eine Synchronität der Daten in der Zentrale und Frankiermaschine erreicht werden kann.

[0036] Es war die Aufgabe zu lösen, ein Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen zu schaffen und einen signifikanten Zuwachs an Sicherheit bei der Guthabenübertragung zu gewährleisten.

[0037] Dabei soll zwischen autorisiertem Handeln (Service-Techniker) und unautorisiertem Handeln (Manipulationsabsicht) unterschieden und die Manipulationssicherheit erhöht werden. Eine weitere Aufgabe ist es, die Sicherheit bei einer Kommunikation mit dem Datenzentrum zu verbessern, wenn Daten in beiden Richtungen übermittelt werden.

[0038] Die Aufgabe wird mit den Merkmalen des Anspruchs 1 bzw. 3 gelöst.

[0039] Die erfindungsgemäße Lösung beruht einerseits auf der Erkenntnis, daß nur zentral in einer Datenzentrale gespeicherte Daten vor einer Manipulation hinreichend geschützt werden können. Ein signifikanter Zuwachs an Sicherheit und Synchronität in den gespeicherten Daten wird durch ein Daten-Melden vor jeder vorbestimmten Handlung an der Frankiermaschine erreicht. Ebenfalls erhöht das in mehr oder weniger großen Zeitabständen erfolgende Melden, insbesondere zum Nachladen eines Guthabens in Verbindung mit der o.g. Protokollierung die Sicherheit gegen eine eventuelle Manipulation. Die zentral zu speichernden Daten umfassen mindestens Datum, Uhrzeit, Identifikationsnummer der Frankiermaschine (ID-Nr. bzw. PIN) und die Art der Daten (z.B. Registerwerte, Parameter), wenn die Frankiermaschine eine Kommunikation mit der Datenzentrale aufnimmt. Zwecks Vorsynchronisation der Daten der Frankiermaschine mit den Daten der Datenzentrale kann ein bestimmter Vorgabewunsch für eine erste Transaktion verwendet werden.

[0040] Andererseits erfolgt zur Erhöhung der Sicherheit ein Unterscheiden zwischen autorisiertem Handeln (Service-Techniker) und unautorisiertem Handeln (Manipulationsabsicht) mittels der Steuereinheit der Frankiermaschine in Verbindung mit Schritten für die Ausführung einer negativen Fernwertvorgabe zur Rückübertragung eines Guthabenwerts in die Datenzentrale, wobei seitens der Frankiermaschine ein Vorgabewunsch an die Datenzentrale übermittelt und dort und in der Frankiermaschine gespeichert wird.

[0041] Dabei wird von der Steuereinheit der Frankiermaschine geprüft, ob mit vorbestimmten Betätigungsmitteln ein definierter Ablauf zum Seiteneinstieg in den Sondermodus zur negativen Fernwertvorgabe vorgenommen und ein vorbestimmter Zeitablauf während der negativen Fernwertvorgabe eingehalten wurde, und ob gegebenenfalls weitere Schritte zur automatischen Durchführung der Kommunikation ausgeführt werden müssen, um die Rückübertragung zu vollenden, wenn die vorausgegangenen Schritte zur Ausführung einer negativen Fernwertvorgabe unterbrochen oder an die Frankiermaschine fehlerhafte verschlüsselte Daten übermittelt wurden.

[0042] Erfindungsgemäß erfolgt eine Kommunikation zwischen Frankiermaschine und Datenzentrale mindestens mit verschlüsselten Meldungen, wobei vorzugsweise der DES-Algorithmus verwendet wird.

[0043] Zur Lösung der Aufgabe weist damit die Frankiermaschine mindestens zwei spezielle Modi auf. Ein erster Mode ist vorgesehen, um bei betrügerischen Handlungen bzw. bei Manipulationsabsicht die Frankiermaschine am Frankieren mit Portowerten zu hindern (Kill-Mode). Diese Hemmung kann anläßlich der nächsten Inspektion vor Ort von einer dazu berechtigten Person aufgehoben werden. Die Frankiermaschine weist einen weiteren Mode auf, um bei Erfüllung ausgewählter Kriterien die Frankiermaschine gegebenenfalls zur automatischen Kommunikation mit der Datenzentrale zu veranlassen. Bei einem solchen weiteren Mode handelt es sich erfindungsgemäß um den Sondermodus negative Fernwertübertragung bzw. um einen zweiten (Sleeping) Mode. Nach Vollendung des Sondermodus ist zwecks Überprüfung der Frankiermaschine nur noch eine beschränkte Anzahl an NULL-Frankierungen möglich. Ist die vorgesehene Stückzahl verbraucht, wird zwangsweise eine automatische Kommunikation mit der Datenzentrale ausgelöst, welche somit informiert wird und relevante Registerdaten erfährt. Die Frankiermaschine ist solange im Sleeping Mode gehemmt. Durch das Zusammenwirken mindestens zweier vorgenannter Modi wird die Sicherheit bei der Handhabung von Guthaben, welche in die Frankiermaschine geladen oder daraus zur Datenzentrale rückübertragen werden sollen, gegenüber einer betrügerischen Manipulation erhöht.

[0044] Wird jedoch ein anderer als der vorbestimmte Bedienablauf während des Einschaltens der Frankiermaschine für einen Seiteneinstieg in den Sondermodus negative Fernwertvorgabe gewählt, welcher verboten ist, schaltet die Frankiermaschine in den vorgenannten ersten Mode, um die Frankiermaschine für ein Frankieren mit einem Portowert zu sperren (Kill-Mode).

[0045] Gegebenenfalls wird zwecks Erhöhung der Manipulationssicherheit ein bereits früher dem autorisierten Bediener (Service-Techniker) von der Datenzentrale mitgeteilter Seiteneinstieg in den Sondermodus negative Fernwertvorgabe geändert. Der zukünftig gültige Bedienablauf kann in Verbindung mit mindestens

einer Transaktion während einer positiven oder negativen Fernwertvorgabe wenigsten teilweise übermittelt werden.

[0046] Ein authorisierter Bediener der Frankiermaschine, vorzugsweise der Service-Techniker, führt zum Seiteneinstieg in den Sondermodus negative Fernwertvorgabe eine vorbestimmte Bedienhandlung aus, welche außer dem Service-Techniker nur noch der Datenzentrale bekannt ist. Dabei wird ein Sonder-Flag gesetzt, welches als spezielles Transaktionsersuchen gewertet wird.

[0047] Eine Überwachung durch die Steuereinheit der Frankiermaschine während der Ausführung einer Transaktion im Sondermodus sichert, daß bei unvollendet gebliebener Transaktion die Transaktionen im Sondermodus negative Fernwertvorgabe bis zum Ende durchgeführt werden. Bei vollendeter Transaktion im Sondermodus wird das Sonder-Flag zurückgesetzt.

[0048] Hinzu tritt eine Zeitüberwachung durch die Steuereinheit der Frankiermaschine während der Ausführung einer Transaktion im Sondermodus, welche bei Zeitüberschreitung bzw. bei unvollendet gebliebener Transaktion wirksam werden, um die Transaktion zuende durchzuführen.

[0049] Eine Zeitüberwachung erfolgt ebenfalls seitens der Datenzentrale, wenn eine Transaktion im Sondermodus negative Fernwertvorgabe vorgenommen wird. Die Registerdaten der Frankiermaschine sind zentral überprüfbar, wenn wieder eine Verbindungsaufnahme zur Durchführung einer Fernwertvorgabe erfolgt, um beispielsweise ein Guthaben nachzuladen. Entweder nimmt bei unvollendet gebliebener Transaktion die Frankiermaschine automatisch wieder die Verbindung auf, um die Transaktion zuende durchzuführen oder der autorisierte Service-Techniker übergibt der Datenzentrale bis zum Tagesende eine Mitteilung über den aktuellen Zustand der Frankiermaschine zwecks Annullierung der im Sondermodus negative Fernwertmodus übertragenen Daten. Andernfalls ergibt die Zeitüberwachung seitens der Datenzentrale nach Ablauf des vorbestimmten Zeitabschnittes, eine Anerkennung der im Sondermodus negative Fernwertvorgabe übertragenen Daten.

[0050] In einer bevorzugten Variante wird die Sicherheit durch eine Prüfung des Bedienablaufes auf Übereinstimmung mit einem vorgegebenen Bedienablauf in der Frankiermaschine und durch eine Prüfung des Vorgabewunsches in der Datenzentrale auf Übereinstimmung mit einem dort gespeicherten Code für einen vorbestimmten Vorgabewunsch erhöht. Es ist möglich, den Bedienablauf zeitabhängig zu ändern, wobei in der Datenzentrale und in der Frankiermaschine der gleiche Berechnungsalgorithmus verwendet wird, um einen aktuellen Bedienablauf zu ermitteln. Eine Übertragung eines gültigen Bedienablaufes von der Datenzentrale zur Frankiermaschine wird damit überflüssig.

[0051] In einer weiteren Variante wird die Sicherheit durch eine Kombination einer Reihe von Maßnahmen erhöht. In einer ersten Transaktion erfolgt ein unterscheidbares Anmelden bei der Datenzentrale. Diese übermittelt in Reaktion darauf ein neues Sicherheits-Flag X und/oder einen vorbestimmten Bedienablauf für einen Seiteneinstieg in den Sondermodus negative Fernwertvorgabe zur Frankiermaschine, wenn die Frankiermaschine normal eingeschaltet wurde und die Kommunikationsverbindung aufnimmt, wobei in einer ersten Transaktion ein vorbestimmter Vorgabe-Wunsch in der Datenzentrale und in der Frankiermaschine gespeichert wurde. In der Datenzentrale wird geprüft, ob der übermittelte Vorgabe-Wunsch einem vorbestimmten Vorgabe-Wunsch entspricht. In der ersten Transaktion wird beispielsweise ein neues Codewort bzw. Sicherheits-Flag und/oder Bedienablauf zur Frankiermaschine übermittelt und in einer zweiten Transaktion wird die angemeldete Transaktion durchgeführt und entsprechend des Vorgabewunsches ein Vorgabewert im entsprechenden Speicher der Frankiermaschine und zwecks Überprüfung der Transaktion auch in einem entsprechenden Speicher der Datenzentrale addiert.

[0052] Für einen Seiteneinstieg in den Sondermodus negative Fernwertvorgabe muß vom Service-Techniker der Bedienablauf während des Einschaltens der Frankiermaschine so, wie er von der Datenzentrale übermittelt wurde, durchgeführt werden,d.h. gleichzeitig mit dem Einschalten ist eine bestimmte Tastenkombination zu drücken.

[0053] In der zweiten Transaktion erfolgt das Nachladen der Frankiermaschine - gemäß dem entsprechenden Vorgabe-Wert - mit einem negativen Guthaben, so daß sich im Ergebnis ein Restwertguthaben von NULL ergibt.

[0054] Die erfindungsgemäße Lösung geht weiterhin davon aus, daß die in der Frankiermaschine gespeicherten Geldmittel vor unautorisiertem Zugriff geschützt werden müssen. Die Verfälschung von in der Frankiermaschine gespeicherten Daten wird so weit erschwert, daß sich der Aufwand für einen Manipulator nicht mehr lohnt.

[0055] Handelsübliche OTP-Prozessoren (ONE TIME PROGRAMMABLE) können alle sicherheiterelevanten Programmteile im Inneren des Prozessorgehäuses enthalten, außerdem den Code zur Bildung des Message Authentification Code (MAC). Letzterer ist eine verschlüsselte Checksumme, die an eine Information angehängt wird. Als Kryptoalgorithmus ist beispielsweise Data Encryption Standard (DES) geeignet. Damit lassen sich MAC- Informationen an die relevanten Sicherheits- und Sonder-Flags bzw. an die Registerdaten anhängen und somit die Schwierigkeit der Manipulation an den vorgenannten Flags bzw. Postregistern maximal erhöhen.

[0056] Das Verfahren zur Verbesserung der Sicherheit einer Frankiermaschine, welche zur Kommunikation mit einer entfernten Datenzentrale fähig ist und einen Mikroprozessor in einer Steuereinrichtung der

Frankiermaschine aufweist, umfaßt außerdem ein Bilden einer Checksumme im OTP-Prozessor über den Inhalt des externen Programmspeichers und Vergleich des Ergebnisses mit einem im OTP-Prozessor gespeicherten vorbestimmten Wert vor und/oder nach Ablauf des Frankiermodus bzw. Betriebsmodus, insbesondere während der Initialisierung (d.h. wenn die Frankiermaschine gestartet wird), oder in Zeiten, in welchen nicht gedruckt wird (d.h. wenn die Frankiermaschine im Standby-Modus betrieben wird). Im Fehlerfall erfolgt dann eine Protokollierung und anschließende Blockierung der Frankiermaschine.

[0057] Zur Verbesserung der Sicherheit von Frankiermaschinen gegen Manipulation erfolgt ein Unterscheiden zwischen nichtmanipuliertem und manipuliertem Betrieb einer Frankiermaschine mittels der Steuereinrichtung, indem während eines Betriebsmodus eine Überwachung der Zeitdauer des Ablaufes von Programmen, Programmteilen bzw. sicherheitsrelevanter Routinen vorgenommen wird und durch einen nach Ablauf von Programmen, Programmteilen bzw. sicherheitsrelevanten Routinen anschließenden Vergleich der gemessenen Laufzeit mit einer vorgegebenen Laufzeit. Auch während einer Kommunikation soll damit eine Manipulation in Betrugsabsicht vereitelt werden, insbesondere durch eine im Kommunikationsmodus vorgenommene Überwachung der Einhaltung eines bestimmten Zeitablaufes im Sondermodus negative Fernwertvorgabe. Es wird die Zeitdauer vom Senden einer dritten verschlüsselten Mitteilung seitens der Frankiermaschine bis zum Empfang der von der Datenzentrale an die Frankiermaschine gesendeten vierten verschlüsselten Mitteilung in der Frankiermaschine, welche bei Verifizierung ein Null-Setzen des Guthabenwerts auslöst, überwacht. Es ist vorgesehen, daß ein decrementaler Zähler oder ein incrementaler Zähler verwendet wird, um ein Überschreiten der Zeit t1 im Sondermodus als ein sicheres Indiz für eine mißglückte Übertragung zu detektieren und daß ein spezielles Unterprogrammm aufgerufen wird, welches eine erneute Durchführung des Sondermodus negative Fernwertvorgabe vorbereitet und automatisch auslöst, so daß die erste und zweite Transaktion automatisch wiederholt werden.

[0058] In einer optionalen Variante wird die Sicherheit durch ein zusätzliches Eingabesicherheitsmittel erhöht, welches mit der Frankiermaschine in Kontakt gebracht wird, um ein Restguthaben von einer autorisierten Person zurück zur Datenzentrale zu übertragen.

[0059] Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1,	Blockschaltbild einer Frankiermaschine,
Figur 2,	Ablaufplan nach der erfindungsgemäßen Lösung,
Figur 3a und 3b,	Darstellung der Sicherheitsabläufe der im Kommunikationsmodus befindlichen Frankiermaschine und Datenzentrum,
Figur 4,	Ablaufplan für den Frankiermodus nach einer bevorzugten Variante,
Figur 5,	allgemene Blockdarstellung eines Ablaufes mit zwei Transaktionen für das Nachladen mit einem Null-Guthabenwert,
Figur 6,	Blockdarstellung eines Ablaufes mit zwei Transaktionen für das Nachladen mit einem negativen-Guthabenwert,
Figur 7,	Ablaufplan zur Einspeicherung eines Sicherheits-Flags bzw. Codewortes nach der erfindungsgemäßen Lösung

[0060] Die Figur 1 zeigt je ein Blockschaltbild der erfindungsgemäßen Frankiermaschine mit einem Drukkermodul 1 für ein vollelektronisch erzeugtes Frankierbild, mit mindestens einem mehrere Betätigungselemente aufweisenden Eingabemittel 2, einer Anzeigeeinheit 3, und einem die Kommunikation mit einer Datenzentrale herstellenden MODEM 23, welche über einen Ein/Ausgabe-Steuermodul 4 mit einer Steuereinrichtung 6 gekoppelt sind und mit einem nichtflüchtigen Speicher 5 bzw. 11 für die variablen bzw. die konstanten Teile des Frankierbildes.

[0061] Ein Charakterspeicher 9 liefert die nötigen Druckdaten für einen flüchtigen Arbeitsspeicher 7. Die Steuereinrichtung 6 weist einen Mikroprozessor µP auf, der mit dem Ein/Ausgabe-Steuermodul 4, mit dem Charakterspeicher 9, mit dem flüchtigen Arbeitsspeicher 7 und mit dem nichtflüchtigen Arbeitspeicher 5, mit einem Kostenstellenspeicher 10, mit einem Programmspeicher 11, mit dem Motor einer Transport- bzw. Vorschubvorrichtung ggf. mit Streifenauslösung 12, einem Encoder (Codierscheibe) 13 sowie mit einem Uhren/Datums-Baustein 8 in Verbindung steht. Die einzelnen Speicher können in mehreren physikalisch getrennten oder in nicht gezeigter Weise in wenigen Bausteinen zusammengefaßt verwirklicht sein, welche durch mindestens eine zusätzliche Maßnahme, beispielsweise Aufkleben auf der Leiterplatte, Versiegeln oder Vergießen mit Epoxidharz, gegen Entnahme gesichert sind.

[0062] In der Figur 2 ist ein Ablaufplan für eine Frankiermaschine mit einem Sicherheitssystem nach einer bevorzugten Variante der erfindungsgemäßen Lösung dargestellt.

[0063] Nach dem Einschalten der Frankiermaschine im Schritt Start 100 wird anschließend innerhalb einer Startroutine 101 eine Funktionsprüfung mit anschließender Initialisierung vorgenommen.

[0064] Dieser Schritt umfaßt auch mehrere - in der

Figur 7 näher dargestellte - Subschritte 102 bis 105 zur Einspeicherung eines Sicherheits-Flags bzw. Codewortes. Mit einem Schritt 103 wird, wenn gemäß Schritt 102 ein neues Sicherheits-Flag X'in einem anderen vorbestimmten Speicherplatz E des nichtflüchtigen Speichers 5 existiert, dieses neue Sicherheits-Flag X' in den Speicherplatz des alten Sicherheits-Flags X kopiert, falls dort kein gültiges Sicherheits-Flag X mehr gespeichert vorliegt. Letzteres betrifft gleichermaßen den Fall eines autorisierten als auch unautorisierten Eingriffs, weil bei jedem Eingriff das alte Sicherheits-Flag X gelöscht wird. Ebenso kann bei einer anderen unautorisierten Handlung das Sicherheits-Flag X gelöscht werden (Kill-Mode). Falls kein gültiges Sicherheits-Flag X mehr gespeichert vorliegt, kann im Frankiermodus 400 kein Portowert mehr gedruckt werden. Bei Nichteingriff ist kein neues Codewort übermittelt worden. In diesen Fall wird nicht kopiert und nach Schritt 104 bleibt das alte Sicherheits-Flag X im Speicher erhalten. Abschließend wird mit Punkt s die Systemroutine 200 erreicht.

[0065] Die Systemroutine 200 umfaßt mehrere Schritte 201 bis 220 des Sicherheitssystems. Im Schritt 201 erfolgt der Aufruf aktueller Daten, was weiter unten in Verbindung mit der Erfindung für einen zweiten Mode, nämlich für den Sleeping-Mode ausgeführt wird. Wie in der Figur 2 dargestellt wird im Schritt 202 überprüft, ob die Kriterien für den Eintritt in den Sleeping-Mode erfüllt sind. Ist das der Fall wird zum Schritt 203 verzweigt, um mindestens eine Warnung mittels der Anzeigeeinheit 3 anzuzeigen. Nach den o.g. Schritten wird im jeden Fall der Punkt t erreicht.

[0066] Bei Feststellung eines verbotenen Seiteneinstieges (Schritt 217), wird das vorgenannte Sicherheits-Flag X gelöscht. Dabei kann es sich beim Sicherheits-Flag X ebenso um ein MAC-gesichertes SicherheitsFlag handeln, wie auch um einen verschlüsselten Code. Die Überprüfung auf Gültigkeit des Sicherheits-Flags X wird beispielsweise im Schritt 409 eines Frankiermodus 400 mittels einem ausgewählten Prüfsummenverfahren innerhalb eines OTP-Prozessors (ONE TIME PROGRAMMABLE) durchgeführt, der intern die entsprechenden Programmteile und außerdem den Code zur Bildung eines MAC (MESSAGE AUTHENTIFICATION CODE) gespeichert enthält, weshalb der Manipulator die Art des Prüfsummenverfahrens nicht nachvollziehen kann. Auch weitere sicherheitsrelevante Schlüsseldaten und Abläufe sind ausschließlich im Inneren des OTP-Prozessors gespeichert, beispielsweise um Schlüsseldaten mit dem von der Datenzentrale zur Frankiermaschine übertragenen neuen Schlüssel zu ergänzen, damit mit den so ergänzten Schlüsseldaten eine Verschüsselung von Meldungen vorgenommen werden kann, welche zur Datenzentrale übermittelt werden. Andererseits erlauben die gleichen sicherheitsrelevanten Schlüsseldaten bzw. Abläufe eine Absicherung über die Postregister zu legen.

[0067] Eine weitere Sicherungsvariante, welche ohne OTP-Prozessor auskommt, besteht im Erschweren des Auffindens der Schlüssel durch dessen Kodierung und partielle Ablage in unterschiedlichen Speicherbereichen. Wieder werden MAC an jede Information in den sicherheitsrelevanten Registern angehängt. Eine Manipulation der Registerdaten kann durch Kontrolle über den MAC erkannt werden. Diese Routine erfolgt im Schritt 406 im Frankiermodus, der in der Figur 4 dargestellt ist. Damit läßt sich die Schwierigkeit der Manipulation an den Postregistern maximal erhöhen.

[0068] Bei erfolgter Prüfung im Schritt 217, wobei ein relevanter Mangel festgestellt und das Sicherheits-Flag X im Schritt 209 gelöscht wurde, wird der Punkt e, d.h. der Beginn eines Kommunikationsmodus 300 erreicht und in einem - in den Figuren 2 und 3a dargestellten - Schritt 301 abgefragt, ob ein Transaktionsersuchen vorliegt. Ist das nicht der Fall, wird der Kommunikationsmodus 300 verlassen und der Punkt f, d.h. der Betriebsmodus 290 erreicht. Wurden relevante Daten im Kommunikationsmodus übermittelt, dann ist zur Datenauswertung auf den Schritt 213 zu verzweigen. Oder anderenfalls, wenn im Schritt 211 die Nichtübermittlung festgestellt wird, ist auf den Schritt 212 zu verzweigen. Nun wird überprüft, ob entsprechende Eingaben getätigt worden sind, um bei Testanforderung 212 in den Testmodus 216, anderenfalls um bei beabsichtigter Registerstandüberprüfung 214 in einen Anzeigemodus 215 zu gelangen. Ist das nicht der Fall, wird automatisch der Punkt d, d.h. der Frankiermodus 400 erreicht.

[0069] Im Falle einer Manipulation wird der Schritt 213 zur Statistik- und Fehlerauswertung erreicht. Über den Schritt 213 wird der Anzeigemodus 215 erreicht und dann zur Systemroutine zurückverzweigt. Das Sperren kann also vorteilhaft dadurch erfolgen, indem die Verzweigung auf den Frankiermodus 400 nicht mehr ausgeführt wird. Erfindungsgemäß ist weiterhin vorgesehen, daß im Schritt 213 eine Statistik- und Fehlerauswertung durchgeführt wird, um weitere aktuelle Daten zu gewinnen, welche nach Verzweigung zur Systemroutine 200 in Schritt 201 ebenfalls aufrufbar sind, beispielsweise für einen vorgenannten zweiten Mode oder einen anderen Sondermode.

[0070] Zwischen den Punkten s und t der Systemroutine 200 können eine Vielzahl von weiteren Abfragen nach Erfüllung weiterer Kriterien für weitere Modi liegen. Nähere Ausführungen bezüglich einer Abfrage nach einem ersten Mode, welcher zum Verhindern des Drucken bzw. zum Sperren der Frankiermaschine dient, sind der deutschen Anmeldung P 43 44 476.8, Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen, zu entnehmen. Im Falle einer Öffnung des Frankiermaschinengehäuses durch dazu befugte Personen ist eine schriftliche ggf. fernmündliche Anmeldung im Datenzentrum zur autorisierte Öffnung vorgeschlagen worden, welche das Öffnungsdatum und die Uhrzeit für den ungefähren Öffnungsbeginn mitteilt. Bevor dann die Frankiermaschine tatsächlich geöffnet

werden kann, muß über MODEM eine Kommunikation mit dem Datenzentrum aufgenommen werden, um die Öffnungsbefugnis zu ersuchen und einen neuen zukünftigen Code Y' zu laden, der den alten ersetzen kann.

[0071] Im Unterschied dazu wird jedoch das Vorhandensein des Sicherheits-Flags X nicht zwischen den Punkten s und t sondern ausschließlich im Schritt 409 im Frankiermodus abgefragt. Dadurch kann der Service-Techniker durch Laden des neuen Sicherheits-Flags X' dennoch auch nach einer Löschung des vorgenannten Flags anschließend die volle Funktionsfähigkeit der Frankiermaschine wiederherstellen. Das erlaubt nun beispielsweise auch eine Überprüfung durchzuführen, ob eine unautorisierte Handlung tatsächlich zur Löschung des Sicherheits-Flags bzw. Codewortes führt, oder ob das Löschen durch Manipulation verhindert worden ist.

[0072] Bei autorisierter Bedienungshandlung wird in dem - in der Figur 2 gezeigten - Schritt 217 erkannt, daß kein verbotener Seiteneinstieg durchgeführt wurde. Ein erlaubter Seiteneinstieg, der für eine andere Eingabe durchgeführt wurde, ist in der Figur 2 nicht näher dargestellt worden. Jedoch ist ein solches Abtragekriterium ebenfalls vorgesehen, um beispielsweise im Schritt 212 zu erkennen, ob eine Bedienhandlung vorgenommen wurde, um in einen Testmode zu gelangen. Beim erlaubten Seiteneinstieg, der nicht der richtige Seiteneinstieg für den Sondermodus einer negativen Fernwertvorgabe zwecks Fondsrückübertragung von der Frankiermaschine zur Datenzentrale ist, wird zum Punkt e der System-routine 200 verzweigt. Anderenfalls wird beim richtigen Seiteneinstieg zum Schritt 220 verzweigt, um ein Sonder-Flag für den Eintritt in den Sondermodus zu setzen. Es ist in weiterer Ausgestaltung eventuell ein weiterer Abfrageschritt 219 vor dem Schritt 220 vorgesehen, um mit einem weiteren Kriterium die Sicherheit gegen unautorisierten Aufruf des Sondermodus weiter zu erhöhen, wobei bei Nichterfüllung des Kriteriums auf den Punkt e der Systemroutine 200 verzweigt wird. Beispielsweise kann der im Figur 2 gezeigte Abfrageschritt 219 ein solches weiteres Kriterium abfragen, ob die Identifikationsnummer (ID-Nr. bzw. PIN) eingegeben wurde. Durch den Seiteneinstieg ist die Sicherheit bereits ausreichend hoch, so daß im Interesse einer einfacheren Bedienung auf solche zusätzlichen weiteren Kriterinabfragen auch verzichtet werden kann. Eine andere Möglichkeit in dem in der Figur 2 gezeigten Abfrageschritt 219 ein solches weiteres Kriterium abfragen, ob mindestens n-mal der gleiche vorbestimmte Vorgabewunsch gestellt und ein entsprechender Vorgabewert zum Guthabenrestwert addiert wurde, ist ebenfalls nur optional und deshalb gestrichelt in der Figur 2 gezeichnet. Hierbei kann es sich um einen NULL-Vorgabewunsch handeln, der zur Übertragung eines NULL-Vorgabewertes führt und zum Restwert addiert werden kann, ohne daß dadurch die Höhe des gespeicherten Guthabens verändert wird.

[0073] Um die Sicherheit gegen Manipulation weiter zu erhöhen, ist vorgesehen, daß das im Schritt 220 gesetzte Sonder-Flag N für den Sondermodus ebenfalls ein MAC-gesichertes Flag N ist.

[0074] Die Sicherheit wird zusätzlich durch eine Überprüfung in der Datenzentrale erhöht, ob ein vorbestimmter Vorgabewunsch von der Frankiermaschine übermittelt worden ist. Es ist vorgesehen, daß der übermittelte Vorgabewunsch in der Datenzentrale als Code gewertet wird, eine ganz bestimmte Transaktion durchzuführen. Der übermittelte Vorgabewunsch kann in der Datenzentrale als Code gewertet werden, um eine Fondsrückübertragung zu erlauben. Andernfalls kann der übermittelte Vorgabewunsch in der Datenzentrale als Code gewertet werden, eine Übertragung für ein Sicherheits-Flag X bzw. für ein X-Codewort zu erlauben.

[0075] In den Figuren 3a und 3b erfolgt eine Darstellung der Sicherheitsabläufe der im Kommunikationsmodus befindlichen Frankiermaschine einerseits und der Sicherheitsabläufe der im Kommunikationsmodus befindlichen Datenzentrale andererseits.

[0076] Wird der Punkt e, d.h. der Beginn des nachfolgend erläuterten Kommunikationsmodus 300 erreicht, wird in einem - in den Figuren 2 und 3a dargestellten - Schritt 301 abgefragt, ob ein Transaktionsersuchen vorliegt. Ein solches kann beispielsweise zur Guthabennachladung, Telefonnummernänderung u.a. gestellt werden.

[0077] Der Benutzer wählt den Kommunikations- bzw. Fernwertvorgabemodus der Frankiermaschine über die Eingabe der Identifikationsnummer (achtstelligen Portoabrufnummer) an. Es wird nun beispielsweise angenommen, es soll die Fondsrückübertragung in Höhe des in der Frankiermaschine verbliebenen Restwertes erfolgen. Hierbei erfolgt zuerst eine Registerabfrage des Descending-registers R1, welches den Restwert gespeichert enthält. Nach einem Ausschalten der Frankiermaschine wird beim Wiedereinschalten ein Seiteneinstieg in den Sondermodus vorgenommen. Nach der Eingabe der Identifikationsnummer wird die Eingabe mit der Teleset-Taste bestätigt und der Vorgabewunsch in Höhe des vorher abgefragten Restwertes eingegeben. Durch den Seiteneinstieg wird der Vorgabewunsch automatisch als zu subtrahierender Vorgabewert gewertet. Der Vorgabewunsch wird durch Betätigung der Teleset-Taste (T-Taste) bestätigt. Da bei jeder Kommunikation von der Datenzentrale auch der Restwert abgefragt wird, kann damit ein Vergleich in der Datenzentrale beider, d.h. von Restwert und Vorgabe-Wunsch erfolgen. Anderenfalls können im Sondermodus die vorgenannten Eingaben für eine bevorzugte Variante auch automatisch von der Frankiermaschine ausgeführt werden, um die Bedienung zu vereinfachen.

[0078] Anderenfalls soll beispielsweise eine Kommunikation erfolgen, um ein neues Sicherheits-Flag X' zu laden, der das alte Sicherheits-Flag X ersetzen kann. Wird nur ein solches Transaktionsersuchen gestellt,

muß der Vorgabebetrag geändert werden, denn in diesem Fall muß das Guthaben in der Frankiermaschine natürlich nicht aufgestockt werden. Andererseits kann auch ein anderer Wert außer Null vereinbart werden, insbesondere ein Wert, dem nur ein minimaler Betrag entspricht, um den der Descending-Registerwert aufgestockt werden müßte.

[0079] In der Figur 3a wird derjenige Teil der Kommunikation einer Transaktion dargestellt, der mit unverschlüsselten Meldungen vorgenommen wird. Dennoch können diese Meldungen Daten enthalten, welche MAC-abgesichert sind, beispielsweise die Identifikationsnummer der Frankiermaschine.

[0080] Im Schritt 302 kann eine Eingabe der Identifikations-Nummer (ID-Nr.) und der beabsichtigten Eingabeparameter auf folgende Weise erfolgen. Bei der ID-Nr. kann es sich um die Serien-Nummer der Frankiermaschine, um eine PIN bzw. PAN (Portoabrufnummer) handeln, die durch Betätigung mittels vorbestimmter T-Taste des Eingabemittels 2 quittiert wird. In der Anzeigeeinheit 3 erscheint der bei der letzten Fernwertvorgabe(Nachladung) benutzte Eingabeparameter-(Vorgabewert), der nun durch die Eingabe des gewünschten Eingabeparameters überschrieben oder beibehalten wird. Beim Eingabeparameter handelt es sich um eine Zahlenkombination, welche in der Datenzentrale als Aufforderung verstanden wird, beispielsweise ein neues Sicherheits-Flag bzw. Codewort X' zu übermitteln, wenn zuvor eine Eingriffsbefugnis eingeholt worden ist. Bei Falscheingabe des vorgenannten Eingabeparameters kann die Anzeige durch Drücken einer C-Taste gelöscht werden.

[0081] Beispielsweise wird eine Änderung eingegeben, um bei einer Transaktion ein Guthaben mit dem Wert Null zu laden, aber es wird keine Eingriffsbefugnis zuvor eingeholt. Somit dient der Eingabeparameter nur als neuer Vorgabewert. Dabei wird aber weder das Guthaben für Frankierungen wertmäßig erhöht, wenn der Eingabeparameter den Wert Null hat, noch ein neues Sicherheitsflag geladen. Jedoch kann bei jeder Kommunikation eine Stückzahl S' übermittelt werden, wie ebenfalls der deutschen Anmeldung P 43 44 476.8, Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen, zu entnehmen ist.

[0082] Nur durch das vorhergehende Mitteilen, beispielsweise mittels eines separaten Anrufes bei der Datenzentrale oder einer anderen Kommunikationsform, wird der Datenzentrale mitgeteilt, daß ein neues Sicherheits-Flag X' zur Frankiermaschine übermittelt werden soll, wenn anschließend innerhalb einer vorbestimmten Zeitdauer seitens der Frankiermaschine eine Transaktion für den Wert Null gestartet wird. Das Eingriffsgesuch gilt nur dann als gestellt, wenn nach dem Anmelden eines autorisierten Eingriffs die Frankiermaschine in den so vereinbarten Kommunikationsmodus eintritt.

[0083] Wird aber zuvor ein beliebig anderer Eingabeparameter mit der Datenzentrale vereinbart, erfolgt bei Eingabe dieses Eingabeparameters außer der Übermittlung eines neuen Sicherheitsflags X' entsprechend des vorvereinbarten Codes der durch den vorbestimmten Vorgabewunsch gebildet wird auch noch eine Nachladung des Guthabens entsprechend des eingegebenen Vorgabewertes im Ergebnis einer zweiten Transaktion bewirkt.

[0084] Wird ein anderer Eingabeparameter als der vereinbarte eingegeben, führt dies im Ergebnis lediglich zur Nachladung in Höhe des gewählten neuen Vorgabebetrages, wo bei im Unterschied zu den anderen Transaktionsdaten jedoch der Vorgabebetrag nicht zur Frankiermaschine übermittelt werden braucht. Vielmehr ist die Tatsache, daß eine gültige Transaktion verifiziert wurde für die Frankiermaschine ausreichend, eine Aufstockung bzw. Minderung des Descendingregisterinhaltes um den Vorgabebetrag entsprechend dem gespeicherten Vorgabewunsch vorzunehmen.

[0085] Ist der gewünschte Eingabeparameter richtig angezeigt, wird dies durch erneutes Betätigen der vorbestimmten T-Taste des Eingabemittels 2 bestätigt. In der Anzeigeeinheit 3 erscheint dann eine Darstellung entsprechend einer Eingabeparameteränderung oder entsprechend der Nichtänderung (alter Vorgabewert).

[0086] Durch Betätigung der vorbestimmten T-Taste wird die Veränderung des Eingabeparameters über MODEM-Verbindung gestartet. Die Eingabe überprüft (Schritt 303) und der weitere Vorgang läuft automatisch ab, wobei der Ablauf durch eine entsprechende Anzeige begleitet wird.

[0087] Dazu prüft die Frankiermaschine, ob ein MODEM angeschlossen und betriebsbereit ist. Ist das nicht der Fall, wird auf den Schritt 310 verzweigt, um anzuzeigen, daß das Transaktionsersuchen wiederholt werden muß. Anderenfalls liest die Frankiermaschine die Wahlparameter, bestehend aus den Herauswahlparametern (Haupt-/Nebenstelle, usw.) und der Telefonnummer aus dem NVRAM-Speicherbereich F und sendet diese mit einem Wahlaufforderungskommando an das Modem 23. Anschließend erfolgt der für die Kommunikation erforderliche Verbindungsaufbau über das MODEM 23 mit der Datenzentrale in einem Schritt 304.

[0088] In der Figur 3a ist auf der linken Hälfte ebenfalls der parallel erfolgende Ablauf in der Datenzentrale dargestellt, welcher für die Kommunikation notwendig ist. Im Schritt 501 wird ständig geprüft, ob ein Anruf in der Datenzentrale erfolgt ist. Ist das der Fall, und das MODEM 23 hat die Gegenseite angewählt, erfolgt im Schritt 502 parallel der Verbindungsaufbau auch in der Datenzentrale. Und im Schritt 503 wird ständig überwacht, ob die Verbindung zur Datenzentrale gelöst wurde. Ist das der Fall, erfolgt nach einer Fehlermeldung im Schritt 513 eine Rückverzweigung zum Schritt 501.

[0089] Parallel dazu wird in der Frankiermaschine im Schritt 305 überwacht, ob Kommunikationsfehler aufgetreten sind und gegebenenfalls zum Schritt 304

zurückverzweigt, um seitens der Frankiermaschine die Verbindung erneut aufzubauen. Nach einer vorbestimmten Anzahl n ergebnisloser Wahlwiederholungen zwecks Verbindungsaufbau wird über einen Anzeigeschritt 310 auf den Punkt e zurückverzweigt. Lag kein im Schritt 305 ermittelbarer Fehler vor, wird im Schritt 306 seitens der Frankiermaschine festgestellt, daß die Verbindung aufgebaut ist und eine Transaktion erst noch erfolgen soll, wird auf den Schritt 307 verzweigt, um eine Eröffnungsnachricht bzw. um Identifikations-, Vorspann- bzw. Registerdaten zu senden. Im nachfolgenden Schritt 308 wird die gleiche Überprüfung, wie im Schritt 305 durchgeführt, d.h. bei einem aufgetretenen Kommunikationsfehler wird zum Schritt 304 zurückverzweigt. Anderenfalls wurde eine Eröffnungsnachricht von der Frankiermaschine an die Datenzentrale geschickt. Darin ist u.a. die Portoabrufnummer zur Bekanntmachung des Anrufenden, d.h. der Frankiermaschine, bei der Datenzentrale enthalten.

[0090] Diese Eröffnungsnachricht wird in der Datenzentrale im Schritt 504 auf Plausibilität überprüft und weiter ausgewertet, indem anschließend im Schritt 505 wieder überprüft wird, ob die Daten fehlerfrei übermittelt worden sind. Ist dies nicht der Fall, erfolgt eine Rückverzweigung zur Fehlermeldung auf den Schritt 513. Sind andererseits die Daten fehlerfrei und in der Datenzentrale wird erkannt, daß die Frankiermaschine ein Nachladeersuchen gestellt hat, so wird im Schritt 506 eine Erwiderungsnachricht zur Frankiermaschine als Vorspann gesendet. Im Schritt 507 wird überprüft, ob im Schritt 506 die Vorspannmeldung einschließlich Vorspann-Ende gesendet worden ist. Ist das aber nicht der Fall, dann wird auf den Schritt 513 zurückverzweigt.

[0091] In der Frankiermaschine wird im Schritt 309 geprüft, ob von der Datenzentrale inzwischen ein Vorspann als Erwiderungsnachricht gesendet bzw. empfangen wurde. Ist das nicht der Fall, wird zur Anzeige auf den Schritt 310 zurückverzweigt und danach erneut ein Transaktionsersuchen im Schritt 301 abgefragt. Wurde ein Vorspann empfangen und die Frankiermaschine hat eine OK-Meldung erhalten, erfolgt im Schritt 311 eine Überprüfung der Vorspannparameter hinsichtlich einer Telefonnummernänderung. Wenn ein verschlüsselter Parameter übermittelt wurde, liegt keine Telefonnummernänderung vor und es wird auf den Schritt 313 in der Figur 3b verzweigt.

[0092] In der Figur 3b erfolgt eine Darstellung der Sicherheitsabläufe der im Kommunikationsmodus befindlichen Frankiermaschine und parallel dazu derjenigen in der Datenzentrale.

[0093] Im Schritt 313 wird von der Frankiermaschine an die Datenzentrale eine Beginnmeldung verschlüsselt gesendet. Im Schritt 314 wird die Meldung auf Kommunikationsfehler überprüft. Liegt ein Kommunikationsfehler vor, wird zum Schritt 304 zurückverzweigt und es erfolgt erneut ein Versuch, die Verbindung zur Datenzentrale aufzubauen, um die Beginn-Meldung verschlüsselt zu senden.

[0094] Von der Datenzentrale wird diese verschlüsselte Beginn-Meldung empfangen, wenn im Schritt 506 die Vorspann-Meldung vollständig gesendet worden war und im Schritt 507 das Vorspann-Ende übermittelt worden ist. Im Schritt 508 wird in der Datenzentrale überprüft, ob diese die Beginn-Meldung erhalten hat und die Daten in Ordnung sind. Ist das nicht der Fall, wird im Schritt 509 überprüft, ob der Fehler behebbar ist. Ist der Fehler nicht behebbar, wird auf den Schritt 513 verzweigt nachdem eine Fehlermeldung von der Datenzentrale DZ an die Frankiermaschine FM im Schritt 511 übermittelt wurde. Anderenfalls wird im Schritt 510 eine Fehlerbehandlung durchgeführt und auf den Schritt 507 verzweigt. Wird im Schritt 508 der Empfang ordnungsgemäßer Daten festgestellt, beginnt die Datenzentrale im Schritt 511 eine Transaktion durchzuführen. Im vorgenannten Beispiel wird mindestens die Identifikationsnummer mittels einer verschlüsselten Meldung zur Frankiermaschine übertragen, welche im Schritt 315 die Transaktionsdaten empfängt.

[0095] Im nachfolgenden Schritt 316 werden die Daten geprüft. Liegt ein Fehler vor, wird auf den Schritt 310 zurückverzweigt. Anderenfalls erfolgt in der Datenzentrale im Schritt 512 eine Speicherung der gleiche vorgenannten Daten, wie in der Frankiermaschine. Im Schritt 318 wird also in der Frankiermaschine die Transaktion mit der Datenspeicherung abgeschlossen. Anschließend wird zum Schritt 305 zurückverzweigt. Soll keine weitere Transaktion erfolgen, wird zur Anzeige der Schritt 310 und danach Schritt 301 erreicht.

[0096] Wenn nun kein Transaktionsersuchen gestellt wird, wird im Schritt 211 gemäß Figur 2 überprüft, ob Daten übermittelt worden sind. Wurden Daten übermittelt, wird der Schritt 213 erreicht. Entsprechend des Eingabewunsches plaziert die Frankiermaschine den aktuellen Vorgabewunsch oder das neue Codewort Y' bzw. andere Transaktionsdaten beispielsweise im Speicherbereich E des nichtflüchtigen Speichers 5.

[0097] Wird als Eingabeparameter im Schritt 302 aber eine andere Zahlenkombination als Null eingegeben und die Eingabe war in Ordnung (Schritt 303), erfolgt ein Verbindungsaufbau (Schritt 304). Und wenn ohne Fehler (Schritt 305) eine Verbindung aufgebaut vorliegt (Schritt 306), wird eine Identifizierungs- und Vorspann-Meldung an die Datenzentrale gesendet. In dieser Eröffnungsnachricht ist wieder u.a. auch die Portoabrufnummer PAN zur Identifizierung der Frankiermaschine bei der Datenzentrale enthalten. Die Datenzentrale erkennt aus der eingegebenen Zahlenkombination, falls die Daten fehlerfrei sind (Schritt 505), daß in der Frankiermaschine beispielsweise ein Guthaben mit einem Vorgabewert aufgestockt werden soll.

[0098] Hat sich inzwischen die aktuelle Telefonnummer der Datenzentrale geändert, müssen Maßnahmen ergriffen werden, daß diese in der Frankiermaschine gespeichert wird. Im Schritt 506 wird dann von der Datenzentrale eine Erwiderungsnachricht

mit den Elementen Änderung der Telefonnummer und aktuelle Telefonnummer unverschlüsselt gesendet. Die Frankiermaschine, die diese Meldung erhält, erkennt im Schritt 311, daß die Telefonnummer geändert werden soll. Nun wird zum Schritt 312 verzweigt, um die aktuelle Telefonnummer zu speichern. Anschließend wird auf den Schritt 304 zurückverzweigt. Ist die Verbindung noch aufgebaut und ein Kommunikationsfehler liegt nicht vor (305), wird im Schritt 306 anschließend geprüft, ob eine weitere Transaktion erfolgen soll. Wenn das nicht der Fall ist, wird über den Schritt 310 zum Schritt 301 verzweigt. Die Übermittlung der Telefonnummer kann ebenfalls MAC-abgesichert erfolgen.

[0099] Nach erfolgter Abspeicherung der aktuellen Telefonnummer baut die Frankiermaschine automatisch eine neue Verbindung zur Datenzentrale unter Zuhilfenahme der neuen Telefonnummer auf. Die eigentliche, vom Benutzer beabsichtigte Transaktion, eine Fernwertvorgabe des neuen Sicherheits-Flag X' oder eine Übermittlung einer zur Verifizierung geeigneten verschlüsselten Meldung zur Nachladung des Restwertguthabens entsprechend einem Vorgabe-wunsch wird somit automatisch, d.h. ohne einen weiteren Eingriff durch den Benutzer der Frankiermaschine, durchgeführt. In der Anzeige erscheint eine entsprechende Mitteilung, daß aufgrund der Telefonnummernänderung die Verbindung automatisch neu aufgebaut wird.

[0100] Es ist vorgesehen, daß nach einem Eingriff, die Frankiermaschine in den Kommunikationsmodus 300 gesteuert wird. Der Berechtigte kann auch der Datenzentrale die beendete Überprüfung noch anschließend mitteilen. Eine Kommunikation kann eine Telefonnummernspeicherung, als auch eine Guthabennachladung bzw. Fondsrückübertragung umfassen. Ohne Unterbrechung der Kommunikation können so mehrere Transaktionen durchgeführt werden.

[0101] Soll die Höhe des nachzuladenden Guthabens in der gleichen Höhe verbleiben, wie bei der letzten Guthabennachladung, ist nur eine Transaktion notwendig.

[0102] Soll die Höhe des nachzuladenden Guthabens aber geändert werden, sind zwei Transaktionen erforderlich. Beide Transaktionen erfolgen auf vergleichbare Weise.

[0103] Eine gelungene Transaktion läuft dabei wie folgt ab: Die Frankiermaschine schickt ihre ID-Nummer und einen Vorgabewert für die Höhe des gewünschten Nachladeguthabens ggf. zusammen mit einem MAC an die Datenzentrale. Diese prüft eine derartige übermittelte Nachricht gegen den MAC, um dann eine ebenfalls MAC-gesicherte OK-Meldung an die Frankier-maschine zu senden. Die OK-Meldung enthält den Vorgabewert nicht mehr.

[0104] Es ist vorgesehen, daß die Übermittlung eines neuen Sicherheitsflags X' bzw. von relevanten Daten für eine Änderung der Guthabenhöhe in der Frankiermaschine in verschlüsselter Form, aber die Übermittlung von Telefonnummer in unverschlüsselter Form erfolgt. Jedoch ist eine MAC-Absicherung zusätzlich möglich. Wird in der Datenzentrale festgestellt, daß die Verbindung zur Frankiermaschine gelöst wurde (Schritt 503) oder fehlerhafte Daten (505) bzw. nicht behebbare Fehler (509) vorliegen oder kein Vorspannende gesendet wurde (507), ist die Kommunikation beendet. Nach einer Fehlermeldung erfolgt das Lösen der Kommunikationsverbindung, das Speichern der übermittelten Daten und deren Auswertung im Schritt 513 seitens der Datenzentrale.

[0105] Während einer ersten Transaktion wird mindestens eine verschlüsselte Nachricht zur Datenzentrale als auch zur Frankiermaschine übermittelt. Der Vorgabewunsch ist nur in der verschlüsselten Nachricht der ersten Transaktion enthalten. Jede übermittelte Nachricht, welche sicherheitsrelevante Transaktionsdaten enthält, ist verschlüsselt. Als Verschlüsselungsalgorithmus für die verschlüsselten Meldungen ist beispielsweise der DES-Algorithmus vorgesehen.

[0106] Ein Transaktionsersuchen führt in der Frankiermaschine zu einer speziell gesicherten Guthabennachladung. Vorzugsweise erfolgt ein Absichern der außerhalb des Prozessors im Kostenstellenspeicher 10 vorliegenden Postregister außerdem während der Guthabennachladung mittels einer Zeitsteuerung. Wird die Frankiermaschine beispielsweise mit einem Emulator/Debugger observiert, dann ist es wahrscheinlich, daß die Kommunikations- und Abrechnungsroutinen nicht innerhalb einer vorbestimmten Zeit ablaufen. Ist das der Fall, d.h. die Routinen benötigen erheblich mehr Zeit, wird ein Teil des DES-Schlüssels geändert. Das Datenzentrum, kann diesen modifizierten Schlüssel während einer Kommunkikationsroutine mit Registerabfrage feststellen und daraufhin die Frankiermaschine als suspekt melden, sobald gemäß Schritt 313 eine Beginn-Meldung verschlüsselt gesendet wird.

[0107] In der Datenzentrale wird im Schritt 509 festgestellt, daß der Fehler nicht behebbar ist. Die Datenzentrale kann dann keine Transaktion (Schritt 511) durchführen, weil zum Schritt 513 zurückverzweigt wurde. Da in der Frankiermaschine im Schritt 315 keine Daten empfangen wurden, war die Transaktion nicht fehlerfrei erfolgt (Schritt 316). Dann wird also über den Schritt 310 auf den Schritt 301 zurückverzweigt, um nach einer Anzeige erneut zu prüfen, ob ein Transaktionsersuchen weiterhin gestellt wird.

[0108] Ist das nicht der Fall, wird der Kommunikationsmodus 300 verlassen und der Punkt f, d.h. der Betriebsmodus 290 erreicht. Somit konnten im oben erörterten Fall, mit modifizierten DES-Schlüssel, keine Daten übermittelt werden (Schritt 211). Ebenfalls wird davon ausgegangen, daß weder eine Testanforderung (Schritt 212) noch ein Registerabruf (Schritt 214) veranlaßt wurde, um das Restguthaben zu prüfen. Dann aber wird der Frankiermodus 400 erreicht.

[0109] Die Sicherheit setzt bei einem autorisierten Eingriff voraus, die Zuverlässigkeit der berechtigten Person (Service, Inspektor) und die Möglichkeit deren

Anwesenheit zu überprüfen. Die Kontrolle des Siegels und die Kontrolle der Registerstände bei einer Inspektion der Frankiermaschine und unabhängig davon der Daten in der Datenzentrale ergibt dann die Überprüfungssicherheit. Die Kontrolle der frankierten Postgüter unter Einbeziehung eines Sicherheitsabdruckes liefert eine zusätzliche Überprüfungssicherheit.

[0110] Die Frankiermaschine führt regelmäßig und/oder beim Einschalten den Registercheck durch und kann somit die fehlende Information erkennen, falls in die Maschine unautorisiert eingegriffen bzw. falls diese unautorisiert bedient worden war. Die Frankiermaschine wird dann blockiert. Ohne die Erfindung in Verbindung mit einem Sicherheits-Flag X würde der Manipulator die Blockierung leicht überwinden. So geht aber das Sicherheits-Flag X verloren und es würde dem Manipulator zuviel Zeit und Aufwand kosten, das gültige MAC-gesicherte Sicherheits-Flag X bzw. Codewort durch Versuche zu ermitteln. In der Zwischenzeit wäre die Frankiermaschine längst in der Datenzentrale als suspekt registriert.

[0111] Andere Varianten bzw. eine Kombination mit anderen Varianten, wie beispielsweise das Löschen eines Teils des DES-Schlüssel oder der redundanten Registerstände bzw. Löschen anderer Daten oder Schlüssel, welche für die Datenzentrale bei einer Transaktion Bedeutung haben, sind durch den Erfindungsgedanken eingeschlossen. Dabei ist wesentlich, daß kritische Programmteile im OTP gespeichert vorliegen und die Programmlaufzeitüberwachungsmittel software- und/oder hardwaremäßige Bestandteile des OTP sind. Damit können mit diesen Programmteilen die extern vom OTP im Programmspeicher PSP 11 gespeicherten kritischen Programme überwacht werden. Der Vorteil besteht darin, daß das Überwachungsprogramm selbst nicht observiert oder manipuiert werden kann, da es ständig im OTP verbleibt und auch nicht ausgelesen werden kann.

[0112] Ein geeigneter Prozessortyp ist beispielsweise der TMS 370 C010 von Texas Instruments, welcher einen 256 Bytes E^2PROM aufweist. Damit können im Prozessor sicherheitsrelevante Daten (Schlüssel, Flags, u.a.) manipulationssicher gespeichert werden.

[0113] Nimmt ein Manipulator einen unautorisierten Eingriff vor, wird die Frankiermaschine durch das Überführen in den ersten Modus wirksam am Frankieren mit einem Portowert gehindert.

[0114] Der potentielle Manipulator einer Frankiermaschine muß mehrere Schwellen überwinden, was natürlich einen gewissen Zeitaufwand bedarf. Erfolgt in gewissen Zeitabständen keine Verbindungsaufnahme von der Frankiermaschine zur Datenzentrale, wird die Frankiermaschine bereits suspekt. Es ist dabei davon auszugehen, daß derjenige, der eine Manipulation an der Frankiermaschine begeht, sich kaum wieder bei der Datenzentrale melden wird.

[0115] Bei einer Inspektion werden zunächst das Siegel der Frankiermaschine auf Unversehrtheit und dann die Registerstände überprüft. Bei Bedarf kann ein Probeabdruck mit dem Wert 0 gemacht werden. Bei einer Reparatur durch den Service vor Ort muß eventuell in die Frankiermaschine eingegriffen werden. Die Fehlerregister sind beispielsweise mit Hilfe eines speziellen Service-EPROM auslesbar, welches an die Stelle des Advert-EPROM gesteckt wird. Wenn auf diesen EPROM-Steckplatz vom Prozessor nicht zugegriffen wird, wird gewöhnlich ein Zugriff auf die Datenleitungen durch spezielle - in der Figur 1 nicht dargestellte - Treiberschaltkreise verhindert. Die Datenleitungen, welche hier durch eine versiegelte Gehäusetür erreichbar sind, können somit nicht unbefugt kontaktiert werden. Eine andere Variante ist das Auslesen von Fehlerregisterdaten durch einen über eine Schnittstelle angeschlossenen Service-Computer. Zur Vorbereitung des Eingriffs werden die Register der Frankiermaschine abgefragt, um die Art des erforderlichen Eingriffs zu ermitteln. Bevor in die Frankiermaschine eingegriffen und das Gehäuse geöffnet wird, erfolgt ein separater Anruf bei der Datenzentrale. Wird dannach innerhalb einer vorbestimmten Zeitdauer der Vorgabewert auf Null geändert und zur Datenzentrale im Rahmen einer Transaktion übermittelt, d.h. die Art des Eingriffs und die Registerdaten wurden der Datenzentrale mitgeteilt, erfolgt ein Übermitteln von Daten von einer Datenzentrale zur Frankiermaschine entsprechend einem beantragten äutorisierten Eingriff in die Frankiermaschine, welcher als erlaubter Eingriff protokolliert wird.

[0116] Wird innerhalb einer vorbestimmten Zeitdauer aber der Vorgabewert auf einen Wert verschieden von Null geändert und zur Datenzentrale im Rahmen einer Transaktion übermittelt, bleibt ein zuvor erfolgter separater Anruf zur Datenzentrale folgenlos, d.h. ein Eingriffsgesuch gilt als nicht gestellt und eine Befugnis zum autorisierten Eingriff in die Frankiermaschine wird nicht erteilt und folglich kein neues Sicherheits-Flag bzw. Codewort X'übermittelt.

[0117] Die Frankiermaschine ist fähig, zu unterscheiden zwischen beantragten autorisierten und unautorisierten Eingriff in die Frankiermaschine mittels der Steuereinheit der Frankiermaschine in Verbindung mit den von der Datenzentrale übermittelten Daten,wobei bei unautorisierten Eingriff in die Frankiermaschine dieser Eingriff als Fehlerfall protokolliert wird, aber nach erfolgten autorisierten Eingriff in die Frankiermaschine der ursprüngliche Betriebszustand mittels den vorgenannten übermittelten Daten wiederhergestellt wird.

[0118] Die Erläuterung der Abläufe nach dem - in der Figur 4 gezeigten - Frankiermodus erfolgt in Verbindung mit dem - in der Figur 2 dargestellten - Ablaufplan. Es ist außerdem auch in Zeiten in welchen nicht gedruckt wird (Standby Modus) vorgesehen, daß eine Abfrage hinsichtlich Manipulationsversuchen erfolgt und/ oder die Checksumme der Registerstände und/oder über den Inhalt des Programmspeichers PSP 11 gebildet wird. Die vorgenannte Checksumme wird

vom Frankiermaschinen-Hersteller MAC-gesichert im nichtflüchtigen Speicher 5 (Speicherbereich E des NV-RAMs) abgelegt. Zur Überprüfung des Inhaltes des Programmspeichers PSP 11 wird die Checksumme erneut ermittelt und unter Verwendung eines gespeicherten unverändert gebliebenen Schlüssels ein MAC gebildet. Beim vorgenannten Schlüssel handelt es sich um einen manipulationsgesicherten (nichtauslesbaren) Teilschlüssel. Nun wird die alte MAC-gesicherte aus dem NV-RAM 5 geladen und mit der neu ermittelten MAC-gesicherten Checksumme im OTP verglichen. Zur Verbesserung der Manipulationssicherheit wird in einer anderen Variante für einen Kill-Mode 2 die Checksumme im Prozessor über den Inhalt des externen Programmspeichers PSP 11 gebildet und das Ergebnis mit einem im Prozessor gespeicherten vorbestimmten Wert verglichen. Dies erfolgt vorzugsweise im Schritt 101, wenn die Frankiermaschine gestartet wird, oder im Schritt 213, wenn die Frankiermaschine im Standby-Modus betrieben wird. Der Standby-Modus wird erreicht, wenn eine vorbestimmte Zeit keine Eingabe- bzw. Druckanforderung erfolgt. Letzteres ist der Fall, wenn ein ansich bekannter - nicht näher dargestellter - Briefsensor keinen nächsten Briefumschlag ermittelt, welcher frankiert werden soll. Der - in der Figur 4 gezeigte - Schritt 405 im Frankiermodus 400 umfaßt daher noch eine weitere Abfrage nach einem Zeitablauf oder nach der Anzahl an Durchläufen durch die Programmschleife, welche letztendlich wieder auf die Eingaberoutine gemäß Schritt 401 führt. Wird das Abfragekriterium erfüllt, wird im Schritt 408 ein Standby-Flag gesetzt und direkt auf den Punkt s zur Systemroutine 200 zurückverzweigt, ohne daß die Abrechnungs- und Druckroutine im Schritt 406 durchlaufen wird. Das Standby-Flag wird später im Schritt 211 abgefragt und nach der Checksummenprüfung im Schritt 213 zurückgesetzt, falls kein Manipulationsversuch erkannt wird.

[0119] Das Abfragekriterium in Schritt 211 wird dazu um die Frage erweitert, ob das Standby-Flag gesetzt ist, d.h. ob der Standby Modus erreicht ist. In diesem Fall wird ebenfalls auf den Schritt 213 verzweigt. Eine bevorzugte Variante besteht darin, in bereits beschriebenen Weise das Sicherheitsflag X zu löschen, wenn ein Manipulationsversuch im Standby Modus auf vorgenannte Weise im Schritt 213 festgestellt worden ist. Das besonders gesicherte Sonder-Flag N kann ebenfalls im Schritt 213 überprüft werden, insbesondere wenn es MAC-gesichert ist, indem der Flaginhalt mit dem MAC-Inhalt verglichen wird. Das Fehlen des Sicherheitsflags X wird im Abfrageschritt 409 erkannt und dann auf den Schritt 213 verzweigt. Der Vorteil dieses Verfahrens in Verbindung mit dem ersten Modus besteht darin, daß der Manipulationsversuch statistisch im Schritt 213 erfaßt wird.

[0120] Die Figur 4 zeigt den Ablaufplan für den Frankiermodus nach einer bevorzugten Variante. Die Erfindung geht davon aus, daß nach dem Einschalten automatisch der Postwert im Wertabdruck entsprechend der letzten Eingabe vor dem Ausschalten der Frankiermaschine und das Datum im Tagesstempel entsprechend dem aktuellem Datum vorgegeben werden, daß für den Abdruck die variablen Daten in die festen Daten für den Rahmen und für alle unverändert bleibenden zugehörigen Daten elektronisch eingebettet werden.

[0121] Die Zahlenketten (sTrings), die für die Erzeugung der Eingabedaten mit einer Tastatur 2 oder aber über eine an die Ein/Ausgabeeinrichtung 4 angeschlossene, den Portowert errechnende, elektronische Waage 22 eingegeben werden, werden automatisch im Speicherbereich D des nichtflüchtigen Arbeitsspeichers 5 gespeichert. Außerdem bleiben auch Datensätze der Subspeicherbereiche, zum Beispiel Bj, C usw., erhalten. Damit ist gesichert, daß die letzten Eingabegrößen auch beim Ausschalten der Frankiermaschine erhalten bleiben, so daß nach dem Einschalten automatisch der Portowert im Wertabdruck entsprechend der letzten Eingabe vor dem Ausschalten der Frankiermaschine und das Datum im Tagesstempel entsprechend dem aktuellem Datum vorgegeben wird. Ist eine Waage 22 angeschlossen, wird der Portowert aus dem Speicherbereich D entnommen. Im Schritt 404 wird gewartet, bis ein solcher aktuell gespeichert vorliegt. Bei einer erneuten Eingabeanforderung im Schritt 404 wird wieder auf den Schritt 401 zurückverzweigt. Anderenfalls wird auf den Schritt 405 verzweigt, um die Druckausgabeanforderung abzuwarten. Durch einen Briefsensor wird der zu frankierende Brief detektiert und damit eine Druckanforderung ausgelöst. Somit kann auf die Abrechnungs- und Druckroutine im Schritt 406 verzweigt werden. Liegt keine Druckausgabeanforderung (Schritt 405) vor, wird zum Schritt 301 (Punkt e) zurückverzweigt.

[0122] Da nach der - in der Figur 4 dargestellten - Variante zum Punkt e zurückverzweigt und der Schritt 301 erreicht wird, kann jederzeit ein Kommunikationsersuchen gestellt oder eine andere Eingabe gemäß den Schritten Testanforderung 212, Registercheck 214, Eingaberoutine 401 getätigt werden.

[0123] Ein weiteres Abfragekriterium kann im Schritt 405 abgefragt werden, um im Schritt 408 ein Standby-Flag zu setzen, wenn nach einer vorbestimmten Zeit noch keine Druckausgabeanforderung vorliegt. Wie bereits oben erläutert, kann das Standby-Flag im auf den Kommunikationsmodus 300 folgenden Schritt 211 abgefragt werden. Damit wird nicht auf den Frankiermodus 400 verzweigt, bevor nicht die Checksummenprüfung die Vollzähligkeit aller oder mindestens ausgewählter Programme ergeben hat.

[0124] Falls eine Druckausgabeanforderung im Schritt 405 erkannt wird, werden weitere Abfragen in den nachfolgenden Schritten 409 und 410 sowie im Schritt 406 getätigt. Beispielsweise werden im Schritt 409 das Vorhandensein eines gültigen Sicherheitsflags X bzw. eines entsprechenden MAC-abgesicherten Flags X, das Erreichen eines weiteren Stückzahlkrite-

rium und/oder im Schritt 406 die in bekannten Weise zur Abrechnung eingezogenen Registerdaten abgefragt. War die zum Frankieren vorbestimmte Stückzahl bei der vorhergehenden Frankierung verbraucht, d.h. Stückzahl gleich Null, wird automatisch zum Punkt e verzweigt, um in den Kommunikationsmodus 300 einzutreten, damit von der Datenzentrale eine neue vorbestimmte Stückzahl S wieder kreditiert wird. War jedoch die vorbestimmte Stückzahl noch nicht verbraucht, wird vom Schritt 410 auf die Abrechnungs- und Druckroutine im Schritt 406 verzweigt.

[0125] Die Anzahl von gedruckten Briefen, und die aktuellen Werte in den Postregistern werden entsprechend der eingegebenen Kostenstelle im nichtflüchtigen Speicher 10 der Frankiermaschine in einer Abrechnungsroutine 406 registriert und stehen für eine spätere Auswertung zur Verfügung. Ein spezieller Sleeping-Mode-Zähler wird während der unmittelbar vor dem Druck erfolgenden Abrechnungsroutine veranlaßt, einen Zählschritt weiterzuzählen.

[0126] Die Registerwerte können bei Bedarf im Anzeigemodus 215 abgefragt werden. Es ist ebenfalls vorgesehen, die Registerwerte mit dem Druckkopf der Frankiermaschine zu Abrechnungszwecken auszudrukken. Das kann beispielsweise ebenso erfolgen, wie das bereits in der deutschen Offenlegungsschrift P 42 24 955 A1 näher ausgeführt wird.

[0127] Es ist bei einer anderen Variante weiterhin vorgesehen, daß auch variable Pixelbilddaten während des Druckens in die übrigen Pixelbilddaten eingebettet werden. Entsprechend der vom Encoder 13 gelieferten Positionsmeldung über den Vorschub der Postgutes bzw. Papierstreifens in Relation zum Druckermodul 1 werden die komprimierten Daten aus dem Arbeitsspeicher 5 gelesen und mit Hilfe des Charakterspeichers 9 in ein binäre Pixeldaten aufweisendes Druckbild umgewandelt, welches ebenfalls in solcher dekomprimierten Form im flüchtigen Arbeitsspeicher 7 gespeichert wird. Nähere Ausführungen sind den europäischen Anmeldungen EP 576 113 A2 und EP 578 042 A2 entnehmbar.

[0128] Der Pixelspeicherbereich im Pixel-Speicher 7c ist also für die ausgewählten dekomprimierten Daten der festen Teile des Frankierbildes und für die ausgewählten dekomprimierten Daten der variablen Teile des Frankierbildes vorgesehen. Nach der Abrechnung erfolgt die eigentliche Druckroutine (im Schritt 406). Wie aus der Figur 1 hervorgeht, stehen der Arbeitsspeicher 7b und der Pixelspeicher 7c mit dem Druckermodul 1 über eine ein Druckregister (DR) 15 und eine Ausgabelogik aufweisende Druckersteuerung 14 in Verbindung. Der Pixelspeicher 7c ist ausgangsseitig an einen ersten Eingang der Druckersteuerung 14 geschaltet, an deren weiteren Steuereingängen Ausgangssignale der Mikroprozessorsteuereinrichtung 6 anliegen. Sind alle Spalten eines Druckbildes gedruckt worden, wird wieder zur Systemroutine 200 zurückverzweigt.

[0129] Die Übermittlung einer neuen Stückzahl S' kann dann auf die gleiche Art und Weise erfolgen, wie das im Zusammenhang mit der Übermittlung des neuen Sicherheits-Flags X' bereits erläutert wurde. Bei einer Kommunikation gemäß Figuren 3a und 3b wird dann eine neue vorbestimmte Stückzahl S' übermittelt und als Stückzahl S bei laufender Frankierung dekrementiert. Aus der neuen vorbestimmten Stückzahl S' wird intern die Vergleichsstückzahl S_{ref} errechnet (Schritt 213). Damit kann im Schritt 203 eine Warnung "CALL FP" vor Erreichen der Stückzahl Null abgegeben werden. Der Benutzer der Frankiermaschine wird damit aufgefordert in Kommunikation mit der Datenzentrale durchzuführen, um mindestens eine NULL-Fernwertvorgabe zur Nachkreditierung wenigstens der Stückzahl S vorzunehmen.

[0130] In der Figur 5 ist der Ablauf mit zwei Transaktionen für das Nachladen mit einem Guthabenwert, vorzugsweise mit einem Null-Guthabenwert vereinfacht dargestellt. Eine solche NULL-Fernwertvorgabe umfaßt immer zwei Transaktionen.

[0131] Die erste Transaktion einer Kommunikation mit der Datenzentrale DZ umfaßt die Mitteilung eines vorbestimmten Vorgabe-Wunsches. Um die Konsistenz der Registerstände zwischen der Datenzentrale DZ und der Frankiermaschine FM herzustellen, ist ein NULL-Vorgabe-Wunsch geeignet. Ein solcher führt während einer zweiten Transaktion zu einem NULL-Vorgabe-Wert der zum Descending-Register-Wert addiert werden kann, ohne den Wert der Restguthabens zu ändern.

[0132] Bei einem normalen Einstieg in den Kommunikationsmodus wird nach dem Start der Frankiermaschine im Schritt 218 der - in Figur 2 dargestellten - Systemroutine 200 abgefragt, ob vom Benutzer ein richtiger Seiteneinstieg durchgeführt wurde. Ist das nicht der Fall wird zum Punkt e der Systemroutine 200 verzweigt. Auf dem Display erscheint eine Meldung über eine Eröffnung der Kommunikation, wenn eine Eingabe der PIN und Drücken der Teleset-Taste (T-Taste) erfolgt. Zusätzlich wird der bisherige Vorgabewert angezeigt, der durch den neuen Vorgabe-Wunsch NULL überschrieben werden kann. Nach der Null-Eingabe wird wieder die T-Taste betätigt. Nun besteht ein Transaktionsersuchen und die Kommunikation kann durchgeführt werden.

[0133] Der erste Schritt während einer ersten Transaktion umfaßt nach dem Einstieg in den Kommunikationsmodus (positive Fernwertvorgabe bzw. Teleset-Modus) einen Subschritt 301 zur Überprüfung auf ein gestelltes Transaktionsersuchen und weitere Subschritte 302 bis 308 zur Eingabe der Identifizierungs- und anderer Daten, um die Kommunikationsverbindung aufzubauen und zur Kommunikation mit unverschlüsselten Daten, um mindestens Identifizierungs- und Transaktionstyp-Daten zur Datenzentrale zu übertragen.

[0134] Es ist vorgesehen, daß ein erster Schritt der ersten Transaktion Subschritte 301 bis 308 der Fran-

kiermaschine umfaßt, um die Verbindung aufzubauen, zur Kommunikation mit unverschlüsselten Daten und um mindestens Identifizierungs-, Transaktionstyp- und andere Daten zur Datenzentrale zu übertragen. Die Transaktionstyp-Daten (1 byte), umfaßt die Mitteilung an die Datenzentrale DZ nachfolgend den Teleset-Modus für eine gewünschte positive Fernwertvorgabe mit der identifizierten Frankiermaschine durchzuführen.

[0135] Ein zweiter Schritt der ersten Transaktion umfaßt Subschritte 501 bis 506 in der Datenzentrale, zum Empfang der Daten und zur Prüfung der Identifikation der Frankiermaschine sowie zur Übermittlung einer unverschlüsselten o.K. -Mitteilung zur Frankiermaschine. Der zweite Schritt der ersten Transaktion umfaßt auch Subschritte, um bei fehlerhaften unverschlüsselten Mitteilungen 505 über einen Subschritt 513 zur Fehlermeldung auf einen Ruhezustand Punkt q im Subschritt 501 in der Datenzentrale zu verzweigen, bis die Kommunikation seitens einer Frankiermaschine wieder aufgenommen wird.

[0136] Ein dritter Schritt der ersten Transaktion umfaßt Subschritte 309 bis 314 der Frankiermaschine, zur Bildung einer ersten verschlüsselten Mitteilung Crypto cv mittels einem in der Frankiermaschine gespeicherten ersten Schlüssel Kn und zur Übertragung von verschlüsselten Daten zur Datenzentrale, umfassend mindestens den Vorgabewunsch, Identifizierungs- und Postregister-Daten. In weiterer Ausgestaltung der Sicherheitsmaßnahmen umfaßt diese verschlüsselte Mitteilung auch Daten in Form von CRC-Daten (Cyclic Redundancey Check-Daten). Der Vorgabewunsch, die Identifizierungs-, Postregister- und andere Daten, wie beispielsweise eine Prüfsumme (CRC-Daten) werden in einer mit dem DES-Algorithmus verschlüsselten Mitteilung übertragen;

[0137] Ein vierter Schritt der ersten Transaktion, der Subschritte 507 bis 511 in der Datenzentrale umfaßt, ist zum Empfang und zur Decryptifizierung der ersten verschlüsselten Mitteilung vorgesehen. Eine Prüfung auf Decryptifizierbarkeit wird mittels eines in der Datenzentrale gespeicherten Schlüssels durchgeführt. Bei Erfolg wird in der datenzentrale eine Berechnung zum Bilden eines zweiten Schlüssels Kn+1 vorgenommen, entsprechend dem von der Frankiermaschine benutzten Schlüssel. Anschließend wird eine zweite verschlüsselten Mitteilung crypto Cv+1 gebildet, welche mindestens den vorgenannten zweiten Schlüssel Kn+1, die Identifizierungs- und die Transaktionsdaten enthält, wobei zur Verschlüsselung wieder der DES-Algorithmus genutzt wird. Abschließend ist ein Übertragen der zweiten verschlüsselten Mitteilung crypto Cv+1 zur Frankiermaschine vorgesehen.

[0138] Weitere Subschritte dienen dazu, um bei Feststellung von unbehebbar fehlerhaften verschlüsselten Mitteilungen im Subschritt 509 über einen Subschritt 513 zur Fehlermeldung auf einen Ruhezustand 501 in der Datenzentrale zu verzweigen, bis die Kommunikation seitens einer Frankiermaschine wieder aufgenommen wird. Es sind weiterhin Subschritte vorgesehen, um bei im Subschritt 509 festgestellten fehlerhaften verschlüsselten Mitteilungen aber mit behebbaren Fehler, auf einen Subschritt 510 zur Stornierung der vorherigen Transaktion und um danach auf den Subschritt 511 in der Datenzentrale zu verzweigen. Dieser Subschritt dient zum Bilden eines zweiten Schlüssels Kn+1, der zur Frankiermaschine verschlüsselt übermittelt werden soll, zum Bilden einer zweiten verschlüsselten Mitteilung crypto Cv+1 und zum Übertragen der verschlüsselten Mitteilung zur Frankiermaschine. Außerdem schließt der vierte Schritt der ersten Transaktion einen Subschritt 512 der Datenzentrale zum Speichern des Vorgabewunsches ein, von dem auf den ersten Subschritt 701 des zweiten Schrittes der zweiten Transaktion verzweigt wird, um den ersten Schlüssel Kn als Vorgängerschlüssel und den zweiten Schlüssel Kn+1 als Nachfolgerschlüssel zu speichern.

[0139] Ein fünfter Schritt der ersten Transaktion, der Subschritte 315 bis 318 der Frankiermaschine umfaßt, dient zum Empfang und zur Decryptifizierung der zweiten verschlüsselten Mitteilung, zum Extrahieren mindestens der Identifikationsdaten und des übertragenen zweiten Schlüssels $Kn+1_{Cv+1}$, sowie zum Verifizieren der empfangenen verschlüsselten Mitteilung anhand der extrahierten Identifizierungsdaten. Bei Verifizierung wird der übertragene zweite Schlüssel $Kn+1_{Cv+1}$ und der Vorgabewunsch in der Frankiermaschine gespeichert. Andernfalls bei Nichtverifizierung wird zum ersten Schritt der ersten Transaktion zurückverzweigt.

[0140] Nach dieser Vorsynchronisation der Datenzentrale durch die Frankiermaschine beginnt eine zweite Transaktion, welche vorzugsweise durch eine zusätzliche manuelle Eingabe im Schritt 602 ausgelöst wird. Im Ergebnis dieser zeitlich befristeten Eingabe erfolgt eine Auslösung der zweiten Transaktion oder ein Verlassen der zweiten Transaktion im Kommunikationsmodus, wenn die Eingabezeit überschritten ist. Vorzugsweise muß die T-Taste innerhalb von 30 sec betätigt werden oder die Eingabezeit ist überschritten und es wird zum ersten Schritt der ersten Transaktion zurückverzweigt. Die Kommunikation kann nun je nach Bedarf unterlassen oder wiederholt werden.

[0141] Ein erster Schritt der zweiten Transaktion umfaßt Subschritte 602 bis 608 der Frankiermaschine zur Kommunikation mit unverschlüsselten Daten, um die Verbindung aufzubauen und um mindestens Identifizierungs- und Transaktionstyp-Daten zur Datenzentrale zu übertragen.

[0142] Ein zweiter Schritt der zweiten Transaktion, der Subschritte 701 bis 706 der Datenzentrale umfaßt, ist zum Empfang der Daten und zur Prüfung der Identifikation der Frankiermaschine sowie zur Übermittlung einer unverschlüsselten o.K. -Mitteilung zur Frankiermaschine vorgesehen. Es ist weiterhin vorgesehen, daß der zweite Schritt der zweiten Transaktion Subschritte umfaßt, um bei fehlerhaften unverschlüsselten Mitteilungen 705 über einen Subschritt 513 zur Fehlermel-

dung auf einen Ruhezustand 501 in der Datenzentrale zu verzweigen, bis die Kommunikation seitens einer Frankiermaschine wieder aufgenommen wird.

[0143] Ein dritter Schritt der zweiten Transaktion umfaßt Subschritte 609 bis 614 der Frankiermaschine zur Bildung einer dritten verschlüsselten Mitteilung crypto cv+2 mittels des vorgenannten in der Frankiermaschine gespeicherten zweiten Schlüssels Kn+1 und zur Übertragung der dritten verschlüsselten Mitteilung crypto cv+2 zur Datenzentrale, umfassend mindestens Identifizierungs- und Postregister-Daten, jedoch ohne Daten für einen Vorgabewert.

[0144] Ein vierter Schritt der zweiten Transaktion, der Subschritte 707 bis 711 der Datenzentrale zum Empfang und zur Decryptifizierung der dritten verschlüsselten Mitteilung crypto Cv+2 enthält, führt deren Prüfung auf Decryptifizierbarkeit mittels eines in der Datenzentrale gespeicherten Schlüssels durch. Dann erfolgt ein Bilden eines dritten Schlüssels Kn+2, welcher zur Frankiermaschine verschlüsselt übermittelt werden soll, ein Bilden einer vierten verschlüsselten Mitteilung crypto Cv+3, welche mindestens den vorgenannten dritten Schlüssel Kn+2, die Identifizierungs- und die Transaktionsdaten enthält und das Übertragen der vierten verschlüsselten Mitteilung crypto Cv+3 zur Frankiermaschine.

[0145] Der vierte Schritt der zweiten Transaktion schließt Subschritte ein, um bei unbehebbar fehlerhaften verschlüsselten Mitteilungen (Subschritt 709) über einen Subschritt 513 zur Fehlermeldung auf einen Ruhezustand 501 in der Datenzentrale zu verzweigen, bis die Kommunikation seitens einer Frankiermaschine wieder aufgenommen wird. Bei in einem Schritt 709 festgestellten fehlerhaften verschlüsselten Mitteilungen mit behebbaren Fehler wird auf einen Schritt 710 zur Stornierung der vorherigen Transaktion verzweigt. Danach erfolgt in der Datenzentrale im Subschritt 711 ein Bilden eines dritten Schlüssels Kn+2, der zur Frankiermaschine verschlüsselt übermittelt werden soll. Zum Bilden einer vierten verschlüsselten Mitteilung crypto Cv+3 wird wieder der DES-Algorithmus eingesetzt. Anschließend erfolgt ein Übertragen der verschlüsselten Mitteilung zur Frankiermaschine.

[0146] Es ist außerdem vorgesehen, daß der vierte Schritt der zweiten Transaktion zum Speichern des Vorgabewertes einen Subschritt 712 der Datenzentrale umfaßt, der auf den ersten Subschritt 501 des zweiten Schrittes der ersten Transaktion verzweigt, um den zweiten Schlüssel Kn+1 als Vorgängerschlüssel Kn-1 und den dritten Schlüssel Kn+2 als Nachfolgerschlüssel Kn für weitere erste und zweite Transaktionen zu speichern.

[0147] Ein fünfter Schritt der zweiten Transaktion, der Subschritte 615 bis 618 der Frankiermaschine umfaßt, dient zum Empfang und zur Decryptifizierung der vierten verschlüsselten Mitteilung, zum Extrahieren mindestens der Identifizierungsdaten und des übertragenen dritten Schlüssels $Kn+2_{Cv+3}$ sowie der Transaktionsdaten, sowie zum Verifizieren der empfangenen verschlüsselten Mitteilung anhand der extrahierten Identifizierungsdaten. Bei Verifizierung wird der übertragene zweite Schlüssel $Kn+2_{Cv+3}$ und der Vorgabewert in der Frankiermaschine entsprechend zum Descendingregisterwert R1 addiert und das resultierende Guthaben gespeichert oder andernfalls bei Nichtverifizierung wird zum ersten Schritt der ersten Transaktion zurückverzweigt.

[0148] Entweder wird wieder zum ersten Schritt zurückgekehrt, um eine weitere Auslösung der Transaktionen zu bewirken, oder im fünften Schritt der zweiten Transaktion wird das vorgenannte Transaktionsersuchen wieder aufgehoben.

[0149] Von dieser NULL-Fernwertvorgabe im Kommunikationsmodus unterscheidet sich eine negative Fernwertvorgabe im Sondermodus vor allem durch spezielle manipulationssichere Flags und eine Zeitüberwachung. Solche manipulationssichere Flags sind insbesondere ein MAC-gesichertes Sicherheits-Flag X und ein MAC-gesichertes Sonder-Flag N.

[0150] In der Figur 6 ist der Ablauf mit zwei Transaktionen für das Nachladen mit einem Negativ-Guthabenwert, d.h. eine negative Fernwertvorgabe zur Fondsrückübertragung an die Datenzentrale dargestellt. Eine solche negative Fernwertvorgabe umfaßt mindestens zwei Transaktionen.

[0151] Die erste Transaktion einer Kommunikation mit der Datenzentrale DZ umfaßt die Mitteilung eines vorbestimmten Vorgabe-Wunsches, vorzugsweise eines NULL-Vorgabe-Wunsches, um die Konsistenz der Registerstände zwischen der Datenzentrale DZ und der Frankiermaschine FM herzustellen.

[0152] Der erste Schritt während einer ersten Transaktion umfaßt nach einen definierten Seiteneinstieg in den Sondermodus negative Fernwertvorgabe gegenüber einem normalen Einstieg in den Kommunikationsmodus (Teleset-Modus) nach dem Start der Frankiermaschine einen Subschritt 301 zur Überprüfung auf ein gestelltes Transaktionsersuchen und weitere Subschritte 302 bis 308 zur Eingabe der Identifizierungs- und anderer Daten, um die Kommunikationsverbindung aufzubauen und zur Kommunikation mit einer unverschlüsselten Mitteilung, um mindestens Identifizierungs- und Transaktionstyp-Daten zur Datenzentrale zu übertragen. Eine Absicherung einzelner Daten in der Mitteilung kann wieder durch einen MAC bzw. mittels CRC-Daten in der vorgenannten Weise erreicht werden.

[0153] Der definierte Seiteneinstieg wird durch Drücken einer geheimen vorbestimmten Tastenkombination während des Einschaltens der Frankiermaschine erreicht. Die Steuereinheit der Frankiermaschine kann erfindungsgemäß in Verbindung mit den von der Datenzentrale bereits früher übermittelten Daten und einem Eingabe-Vorgang zwischen autorisierten Handeln (Service-Techniker) und unautorisierten Handeln (Manipulationsabsicht) unterscheiden.

Beim autorisierten Handeln wird ein Sonder-Flag N im Schritt 220 gesetzt, denn falls die Frankiermaschine FM ausgeschaltet wird, muß die Weiterführung der Transaktionen nach dem Wiedereinschalten der Frankiermaschine gesichert sein. Als Schutz gegen eine eventuelle Manipulation wird das Sonder-Flag N ebenfalls MAC-gesichert nichtflüchtig gespeichert.

[0154] Erfolgt ein Fehlversuch oder wird eine andere Tastenkombination für den Seiteneinstieg eingegeben, wird dies als unautorisiertes Handeln bzw. als Manipulationsabsicht gewertet (Fehlermeldung) und gespeichert sowie ein Schritt 209 zur Verhinderung einer weiteren Frankierung ausgelöst.
Es ist vorgesehen, daß eine vorbestimmte Tastenkombination für jede Frankiermaschine in der Datenzentrale gespeichert wird und nur der autorisierten Person (Service-Techniker) mitgeteilt wird, um einen yorbestimmten Bedienablauf bei der Frankiermaschine zu erzielen. Der richtige Seiteneinstieg bewirkt eine Meldung auf dem Display über eine Eröffnung der Kommunikation.

[0155] Zur Überführung der Frankiermaschine in einen Sondermodus wird ein gegen Manipulation gesichertes Flag N im Schritt 220 gesetzt, wenn ein spezifisches Kriterium erfüllt vorliegt, wobei das spezifische Kriterium für den Sondermodus negative Fernwertvorgabe mindestens die Verwendung der vorbestimmten Tastenkombination zum Seiteneinstieg in den Sondermodus während des Einschaltens der Frankiermaschine umfaßt.

[0156] In einer Variante erfolgt, wie bei der positiven Fernwertvorgabe eine Eingabe der PIN und Drücken der Teleset-Taste (T-Taste), dann Null-Eingabe und Drücken der T-Taste, bevor die Kommunikation durchgeführt wird.

[0157] Die Kommunikation mit der Datenzentrale umfaßt mindestens zwei Transaktionen, welche im Fehlerfall wiederholt durchlaufen werden, wobei nach Unterbrechung die Kommunikation automatisch erneut wieder aufgenommen und/oder solange durchgeführt wird, wie das vorgenannte Sonder-Flag N für den Sondermodus gesetzt ist, durch das ein automatisches Transaktionsersuchen gestellt ist, um die Rückübertragung des Guthabens zu vollenden.

[0158] Es ist vorgesehen, daß ein erster Schritt der ersten Transaktion Subschritte 301 bis 308 der Frankiermaschine umfaßt, um die Verbindung aufzubauen, zur Kommunikation mit unverschlüsselten Daten und um mindestens Identifizierungs-, Transaktionstyp- und andere Daten zur Datenzentrale zu übertragen. Die Transaktionstyp-Daten (1 byte), umfaßt die Mitteilung an die Datenzentrale DZ nachfolgend den Sondermodus einer gewünschten negativen Fernwertvorgabe mit der identifizierten Frankiermaschine durchzuführen.

[0159] Ein zweiter Schritt der ersten Transaktion umfaßt Subschritte 501 bis 506 in der Datenzentrale, zum Empfang der Daten und zur Prüfung der Identifikation der Frankiermaschine sowie zur Übermittlung einer unverschlüsselten o.K.-Mitteilung zur Frankiermaschine. Der zweite Schritt der ersten Transaktion umfaßt auch Subschritte, um bei fehlerhaften unverschlüsselten Mitteilungen 505 über einen Subschritt 513 zur Fehlermeldung auf einen Ruhezustand 501 in der Datenzentrale zu verzweigen, bis die Kommunikation seitens einer Frankiermaschine wieder aufgenommen wird.

[0160] Ein dritter Schritt der ersten Transaktion umfaßt Subschritte 309 bis 314 der Frankiermaschine, zur Bildung einer ersten verschlüsselten Mitteilung Crypto cv mittels einem in der Frankiermaschine gespeicherten ersten Schlüssel Kn und zur Übertragung von verschlüsselten Daten zur Datenzentrale, umfassend mindestens den Vorgabewunsch, Identifizierungs- und Postregister-Daten. In weiterer Ausgestaltung der Sicherheitsmaßnahmen umfaßt diese verschlüsselte Mitteilung in Form von CRC-Daten (Cyclic Redundancey Check-Daten) die Mitteilung an die Datenzentrale DZ nachfolgend den Sondermodus einer gewünschten negativen Fernwertvorgabe durchzuführen. Bei dem zwei Byte umfassenden Cyclic Redundancey Check handelt es sich um eine Prüfsumme, die eine Manipulation an einzelnen der zur Prüfsumme verarbeiteten Daten erkennen läßt. Diese Prüfsumme kann einzelne Daten bzw. die Bestandteile aller Mitteilungen (Transaktionstyp) seitens der Frankiermaschine einschließen. Der Vorgabewunsch, die Identifizierungs-, Postregister- und die CRC-Daten werden in einer mit dem DES-Algorithmus verschlüsselten Mitteilung übertragen. Somit ist es nicht erforderlich, Daten im ersten Schritt MAC-gesichert bzw. verschlüsselt an die Datenzentrale zu übertragen.

[0161] Ein vierter Schritt der ersten Transaktion, der Subschritte 507 bis 511 in der Datenzentrale umfaßt, ist zum Empfang und zur Decryptifizierung der ersten verschlüsselten Mitteilung bzw. deren Prüfung auf Decryptifizierbarkeit mittels eines in der Datenzentrale gespeicherten Schlüssels, zum Bilden eines zweiten Schlüssels Kn+1 entsprechend dem von der Frankiermaschine benutzten Schlüssel, zum Bilden einer zweiten verschlüsselten Mitteilung crypto Cv+1, welche mindestens den vorgenannten zweiten Schlüssel Kn+1, die Identifizierungs- und die Transaktionsdaten enthält und zum Übertragen der zweiten verschlüsselten Mitteilung crypto Cv+1 zur Frankiermaschine vorgesehen.

[0162] Es ist vorgesehen, daß der vierte Schritt der ersten Transaktion auch Subschritte umfaßt, um bei unbehebbar fehlerhaften verschlüsselten Mitteilungen 509 über einen Subschritt 513 zur Fehlermeldung auf einen Ruhezustand 501 in der Datenzentrale zu verzweigen, bis die Kommunikation seitens einer Frankiermaschine wieder aufgenommen wird. Es sind weiterhin Subschritte vorgesehen, um bei fehlerhaften verschlüsselten Mitteilungen 509 mit behebbaren Fehler, auf einen Schritt 510 zur Stornierung der vorherigen Transaktion und um danach auf den Subschritt 511 in der Datenzentrale zu verzweigen. Dieser Subschritt dient zum Bilden eines zweiten bzw. dritten Schlüssels Kn+1,

der zur Frankiermaschine verschlüsselt übermittelt werden soll, zum Bilden einer zweiten verschlüsselten Mitteilung crypto Cv+1 und zum Übertragen der verschlüsselten Mitteilung zur Frankiermaschine. Außerdem schließt der vierte Schritt der ersten Transaktion einen Subschritt 512 der Datenzentrale zum Speichern des Vorgabewunsches ein, von dem den ersten Subschritt 701 des zweiten Schrittes der zweiten Transaktion verzweigt wird, um den ersten Schlüssel Kn als Vorgängerschlüssel und den zweiten Schlüssel Kn+1 als Nachfolgerschlüssel zu speichern.

[0163] Ein fünfter Schritt der ersten Transaktion, der Subschritte 315 bis 318 der Frankiermaschine umfaßt, dient zum Empfang und zur Decryptifizierung der zweiten verschlüsselten Mitteilung, zum Extrahieren mindestens der Identifikationsdaten und des übertragenen zweiten Schlüssels $Kn+1_{Cv+1}$, sowie zum Verifizieren der empfangenen verschlüsselten Mitteilung anhand der extrahierten Identifizierungsdaten. Bei Verifizierung wird der übertragene zweite Schlüssel $Kn+1_{Cv+1}$ und der Vorgabewunsch in der Frankiermaschine gespeichert. Andernfalls bei Nichtverifizierung wird zum ersten Schritt der ersten Transaktion zurückverzweigt.

[0164] Nach dieser Vorsynchronisation der Datenzentrale durch die Frankiermaschine erfolgt eine zweite Transaktion. Ein erster Schritt der zweiten Transaktion umfaßt Subschritte 602 bis 608 der Frankiermaschine zur Kommunikation mit unverschlüsselten Daten, um die Verbindung aufzubauen und um mindestens Identifizierungs- und Transaktionstyp-Daten zur Datenzentrale zu übertragen.

[0165] Ein zweiter Schritt der zweiten Transaktion, der Subschritte 701 bis 706 der Datenzentrale umfaßt, ist zum Empfang der Daten und zur Prüfung der Identifikation der Frankiermaschine sowie zur Übermittlung einer unverschlüsselten o.K.-Mitteilung zur Frankiermaschine vorgesehen. Es ist weiterhin vorgesehen, daß der zweite Schritt der zweiten Transaktion Subschritte umfaßt, um bei fehlerhaften unverschlüsselten Mitteilungen 705 über einen Subschritt 513 zur Fehlermeldung auf einen Ruhezustand 501 in der Datenzentrale zu verzweigen, bis die Kommunikation seitens einer Frankiermaschine wieder aufgenommen wird.

[0166] Ein dritter Schritt der zweiten Transaktion umfaßt Subschritte 609 bis 614 der Frankiermaschine zur Bildung einer dritten verschlüsselten Mitteilung crypto cv+2 mittels des vorgenannten in der Frankiermaschine gespeicherten zweiten Schlüssels Kn+1 und zur Übertragung der dritten verschlüsselten Mitteilung crypto cv+2 zur Datenzentrale, umfassend mindestens Identifizierungs- und Postregister-Daten, jedoch ohne Daten für einen Vorgabewert.

[0167] Ein vierter Schritt der zweiten Transaktion, der Subschritte 707 bis 711 der Datenzentrale zum Empfang und zur Decryptifizierung der dritten verschlüsselten Mitteilung crypto Cv+2 enthält, führt deren Prüfung auf Decryptifizierbarkeit mittels eines in der Datenzentrale gespeicherten Schlüssels durch. Dann erfolgt ein Bilden eines dritten Schlüssels Kn+2, welcher zur Frankiermaschine verschlüsselt übermittelt werden soll, ein Bilden einer vierten verschlüsselten Mitteilung crypto Cv+3, die mindestens den vorgenannten dritten Schlüssel Kn+2, die Identifizierungs- und die Transaktionsdaten enthält und das Übertragen der vierten verschlüsselten Mitteilung crypto Cv+3 zur Frankiermaschine.

[0168] Der vierte Schritt der zweiten Transaktion schließt Subschritte ein, um bei unbehebbar fehlerhaften verschlüsselten Mitteilungen 709 über einen Subschritt 513 zur Fehlermeldung auf einen Ruhezustand 501 in der Datenzentrale zu verzweigen, bis die Kommunikation seitens einer Frankiermaschine wieder aufgenommen wird. Bei in einem Schritt 709 festgestellten fehlerhaften verschlüsselten Mitteilungen mit behebbaren Fehler wird auf einen Schritt 710 zur Stornierung der vorherigen Transaktion verzweigt. Danach erfolgt in der Datenzentrale im Subschritt 711 ein Bilden eines dritten Schlüssels Kn+2, der zur Frankiermaschine verschlüsselt übermittelt werden soll. Zum Bilden einer vierten verschlüsselten Mitteilung crypto Cv+3 wird wieder der DES-Algorithmus eingesetzt. Anschließend erfolgt ein Übertragen der verschlüsselten Mitteilung zur Frankiermaschine.

[0169] Es ist außerdem vorgesehen, daß der vierte Schritt der zweiten Transaktion zum Speichern des Vorgabewertes einen Subschritt 712 der Datenzentrale umfaßt, der auf den ersten Subschritt 501 des zweiten Schrittes der ersten Transaktion verzweigt, um den zweiten Schlüssel Kn+1 als Vorgängerschlüssel Kn-1 und den dritten Schlüssel Kn+2 als Nachfolgerschlüssel Kn für weitere erste und zweite Transaktionen zu speichern.

[0170] Ein fünfter Schritt der zweiten Transaktion, der Subschritte 615 bis 618 der Frankiermaschine umfaßt, dient zum Empfang und zur Decryptifizierung der vierten verschlüsselten Mitteilung, zum Extrahieren mindestens der Identifizierungsdaten und des übertragenen dritten Schlüssels $Kn+2_{Cv+3}$ sowie der Transaktionsdaten, sowie zum Verifizieren der empfangenen verschlüsselten Mitteilung anhand der extrahierten Identifizierungsdaten. Der vorgenannte Schritt weist zur Identifikation der vollendeten Durchführung im Unterschied zur positiven Fernwertvorgabe ein weiteres Abfragekriterium auf. Innerhalb einer vorbestimmten Zeit, ab der Absendung der dritten Crypto-Mitteilung soll von der Frankiermaschine FM die vierte Crypto-Mitteilung empfangen werden. Bei Unterbrechungsfreiheit der Verbindung würde der Empfang in der vorbestimmten Zeit t1 erfolgen.

[0171] In der bevorzugten Ausführungsform wird also der letzte und besonders kritische Abschnitt der zweiten Transaktion auf Überschreiten der Zeit t1 überwacht. Damit ist die mögliche Manipulationszeit stark eingeschränkt. Hierzu wird während der vorletzten zu übertragenen Nachricht, ab Absendung der dritten Crypto-Mitteilung im Prozessor (Steuereinheit 6) der

Frankiermaschine eine Zeitzählung gestartet. Dies wird vorzugsweise so gelöst, daß der entsprechende Programmabschnitt eine Routine aktiviert, welche einen Zähler setzt, der seinerseits durch den Systemtakt oder dessen Vielfaches decrementiert wird. Um einen größeren Zeitabschnitt, beispielsweise in der Größenordnung von 10 sec, zu überwachen werden mehrere Zähler kaskadiert. Erreicht nun innerhalb des kritischen Zeitabschnittes die vierte Crypto-Mitteilung von der Datenzentrale die Frankiermaschine, wird der Zähler deaktiviert. Bleibt diese letzte Crypto-Mitteilung hingegen aus wird der gesetzte Zähler weiter decrementiert. Beim Nulldurchgang des Zählers wird ein Programmunterbrechungssignal (Interrupt) ausgelöst. Dieses Signal veranlaßt den Aufruf eines speziellen Unterprogrammes, welches eine erneute Transaktion vorbereitet und auslöst. Bestandteil dieser erneuten Transaktion ist wieder die Übermittlung der Postregisterinhalte. Eine in der Datenzentrale stattfindende Konsistenzprüfung führt dann zum Ergebnis, daß eine unvollendete Transaktion im Sondermodus negative Fernwertvorgabe vorausging. Die inkonsistenten Datensätze werden korrigiert und die negative Fernwertvorgabe wird vollendet.

[0172] Eine weitere Variante der Erfindung ergibt sich, wenn statt eines decrementalen Zählers ein incrementaler verwandt wird. Dabei muß nach jedem Zähltakt der Vergleich mit der Zahl durchgeführt werden, die dem überwachten Zeitabschnitt entspricht.

[0173] Ein Überschreiten der Zeit t1 ist ein sicheres Indiz für eine mißglückte Übertragung und bewirkt den Aufruf eines speziellen Unterprogrammms, welches eine erneute Durchführung des Sondermodus negative Fernwertvorgabe vorbereitet und automatisch auslöst. Die erste und zweite Transaktion werden in diesem Fall automatisch mit Schlüssel Kn+2 wiederholt.

[0174] Nach erfolgreicher Abfrage bzw. Verifizierung im fünften Schritt der zweiten Transaktion wird der übertragene zweite Schlüssel $Kn+2_{Cv+3}$ und der Vorgabewert in der Frankiermaschine entsprechend zum Descendingregisterwert R1 addiert und das resultierende Guthaben gespeichert oder andernfalls bei Nichtverifizierung oder Zeitüberschreitung wird zum ersten Schritt der ersten Transaktion zurückverzweigt.

[0175] Der fünfte Schritt der zweiten Transaktion schließt einen Subschritt (620) der Frankiermaschine zum Rücksetzen des vorgenannten Sonder-Flags N bzw. zur Rückkehr in den Normalmodus der Frankiermaschine ein, wodurch das vorgenannte automatische Transaktionsersuchen wieder aufgehoben wird, wenn die Durchführung der zweiten Transaktion vollendet worden ist.

[0176] Der anwesende Service-Techniker sichert den weiteren störungefreien Ablauf bis zur Vollendung der negativen Fernwertvorgabe.

[0177] Ist die Vollendung aufgrund einer längeren bzw. ständigen Unterbrechung der Verbindung zwischen Frankiermaschine und Datenzentrale nicht möglich, muß der Service-Techniker die Frankiermaschine in das Dealer-Büro mitnehmen und von dort die Vollendung weiterbetreiben. Anderenfalls würde sich ein Guthaben in der Frankiermaschine ergeben, welches nach Information in der Datenzentrale bereits als rückübertragen gilt. Die erfolgreiche Vollendung der negativen Fernwertvorgabe, d.h. der Fonds-Rückübertragung, ist durch eine Abfrage der Registerstände R1 = 0 bzw. R2 = R3 und R3 = R2 + R1 überprüfbar.

[0178] Die Frankiermaschine kann der Datenzentrale Registerwerte beispielsweise vor einer Nachladung mit einem NULL-Vorgabewert übermitteln. Dabei sind:

R1 (descending register) vorrätige Restbetrag in der Frankiermaschine,
R2 (ascending register) Verbrauchssummenbetrag in der Frankiermaschine,
R3 (total resetting) die bisherige Gesamtvorgabesumme aller Fernwertvorgaben,
R4 (piece count õprinting with value Ï O) Anzahl gültiger Drucke,
R8 (R4 + piece count õprinting with value = O) Anzahl aller Drucke

[0179] Bei jeder Fernwertvorgabe läßt sich mindestens R1 abfragen und statistisch auswerten.

[0180] Seitens der Datenzentrale wird am Tages-Ende über die Gültigkeit der Fondsrückübertragung im Ergebnis des Sondermodus negative Fernwertvorgabe entschieden. Wenn vom Service-Techniker kein Vorkommnis gemeldet wird, daß beispielsweise die negative Fernwertvorgabe nicht durchführbar war, bzw. wenn von derselben Frankiermaschine keine Anforderung zum Nachladen eines positiven Guthabens erfolgt, wird die Gültigkeit vorausgesetzt.

[0181] Das bei Eintritt in den Sondermodus negative Fernwertvorgabe gesetzte Sonder-Flag N wurde bei erfolgreicher Transaktion zurückgesetzt. Die Frankiermaschine verhindert alle Frankierungen mit Werten größer Null, weil kein mehr Guthaben geladen ist. Die Frankiermaschine ist weiterhin für Frankierungen mit Werten gleich Null und andere Betriebsarten betriebsbereit, solange diese kein Guthaben erfordern bzw. solange damit kein Porto frankiert und die Stückzahlgrenze nicht erreicht wird.

[0182] Entweder wird, wie bei der einen Variante, durch den vorbestimmten Seiteneinstieg eine Auslösung der Transaktionen im Sondermodus bewirkt oder es ist in einer anderen Variante mindestens ein manueller Schritt 302 im Sondermodus negative Fernwertvorgabe nach einem Seiteneinstieg zur Eingabe einer Identifizierungsnummer (PIN) und zur Eingabe des vorbestimmten Vorgabewunsches wie bei der positiven Fernwertvorgabe vorgesehen, welche im Schritt 303 abgefragt wird. Durch einen zusätzlichen manuellen Schritt zur zeitlich befristeten Eingabe, welche im Schritt 603 abgefragt wird, erfolgt eine Auslösung der zweiten Transaktion und ein Verlassen bzw. die Wieder-

holung der ersten Transaktion im Kommunikationsmodus bzw. im Sondermodus, wenn die Eingabezeit überschritten ist. Vorzugsweise muß die T-Taste innerhalb von 30 sec betätigt werden oder die Eingabezeit ist überschritten.

[0183] Es ist weiterhin eine Anzahl an Varianten mit unterschiedlichen Sicherheitsniveau realisierbar. So kann in der Datenzentrale eine Prüfung auf Übermittlung eines vorbestimmten Vorgabewunsches durchgeführt werden. Im einfachsten Fall muß der Vorgabewunsch - analog dem im Anzeigemodus 215 abfragbaren im Descendingregister noch vorrätigen Restbetrag R1 - eingegeben und zur Datenzentrale übermittelt werden. Da zur Datenzentrale automatisch bei jeder Transaktion die Postregisterinhalte, mindestens aber R1 übermittelt werden, wird eine negative Fernwertvorgabe zur Fondsrückübertragung bei Übereinstimmung des Vorgabebetrages mit dem Restbetrag erzielt.

[0184] In einer zweiten Variante wird mit der Datenzentrale ein beliebiger Vorgabewunsch als Code vereinbart. Vorzugsweise wird ein NULL-Vorgabewunsch vereinbart. Wird nun innerhalb einer bestimmten Zeit nach der Vereinbarung der Sondermodus negative Fernwertvorgabe aufgerufen und der NULL-Vorgabewunsch eingegeben bzw. als Vorgabewunsch bestätigt, wird in der Frankiermaschine automatisch der Restbetrag R1 auf NULL zurückgesetzt. Eine entsprechender Abfrageschritt 219 nach einem solchen weiteren spezifischen Kriterium für die Frankiermaschine wurde in der Figur 2 gestrichelt dargestellt. Von diesem wird auf den Schritt 220 zum Setzen des Sonder-Flags N verzweigt. In weiterer Ausgestaltung kann die Bedienung vereinfacht werden, wenn eine NULL-Fernwertvorgabe als letzte Transaktion bereits erfolgte. Dann ist lediglich noch die Bedienungshandlung für den Seiteneinstieg vorzunehmen, um die negative Fernwertvorgabe vollautomatisch durchzuführen bzw. um einen NULL-Restwert R1 = 0 zu erreichen.

[0185] Durch ein Starten einer Zeitüberwachung ab dem Subschritt 613 der Absendung der dritten Crypto-Mitteilung an die Datenzentrale bis zum Empfang der vierten Crypto-Mitteilung seitens der Frankiermaschine wird eine Manipulation zeitlich beschränkt. Wenn die vierte Crypto-Mitteilung nicht innerhalb einer vorbestimmten Zeit t1 empfangen werden konnte, wird ein spezielles Unterprogrammm aufgerufen, welches eine erneute Durchführung des Sondermodus negative Fernwertvorgabe vorbereitet und automatisch auslöst. Durch weitere Subschritte 615, 616, 301 zur automatischen Wiederaufnahme der Kommunikation nach Unterbrechung der Kommunikationsverbindung zwischen Datenzentrale und Frankiermaschine oder nach dem Aus- und Wiedereinschalten der Frankiermaschine wird solange, wie das vorgenannte Sonder-Flag N gesetzt ist, die Kommunikation weiter durchgeführt. Das als Transaktionsersuchen gewertete Sonder-Flag N ist nichtflüchtig und gegen Manipulation MAC-gesichert gespeichert. Erst nach Vollendung der Rückübertragung des Guthabens wird das Sonder-Flag N im Schritt 620 zurückgesetzt.

[0186] In einer dritten Variante wird die Sicherheit durch eine Kombination verschiedener Maßnahmen erhöht. Unabhängig von der Frankiermaschine wird eine erste Kommunikationsverbindung zwischen authorisierten Benutzer und der Datenzentrale zur Speicherung eines Codes für ein Anmelden einer autorisierten Handlung an der Frankiermaschine durch ein später übermittelten Vorgabewunsch hergestellt. Nun kann ein Einschalten der Frankiermaschine zur Vornahme eines autorisierten vorbestimmten Bedienablaufes erfolgen, um über einen Seiteneinstieg in einen Sondermodus negative Fernwertvorgabe einzutreten. Daraufhin wird eine zweite Kommunikationsverbindung zwischen Frankiermaschine und der Datenzentrale sowie Eingabe eines Vorgabewunsches hergestellt. In einer ersten Transaktion erfolgt ein unterscheidbares Anmelden bei der Datenzentrale, wenn der übermittelte Vorgabewunsch mit einem entsprechenden Code übereinstimmt. In der ersten Transaktion wird beispielsweise ein neues Codewort bzw. Sicherheits-Flag und/oder Bedienablauf zur Frankiermaschine übermittelt. Durch das Durchführen mindestens einer weiteren Transaktion und der automatischen Durchführung der vorgenannten Kommunikation werden die sicherheitsrelevanten Daten übertragen und deren Speicherung in der Frankiermaschine vollendet. Entsprechend des Vorgabewunsches wird der Vorgabewert im entsprechenden Speicher der Frankiermaschine und zwecks Überprüfung der Transaktion auch in einem entsprechenden Speicher der Datenzentrale zum Restguthaben addiert.

Anderenfalls ist eine Ausführung eines Schrittes 209 zur Löschung eines manipulationssicher gespeicherten Sicherheitsflags X im Ergebnis mindestens einer unerlaubten Abweichung vom vorbestimmten Bedienablauf bzw. weil in die Frankiermaschine eingegriffen wurde, vorgesehen. Damit wird die Frankiermaschine in einen ersten Modus überführt, um sie damit für ein Frankieren (Frankiermodus 400) wirksam außer Betrieb zu setzen (Schritt 409), im Gegensatz zur authorisierten Handlung bzw. Eingriff.

[0187] Eine Übertragung eines gültigen Bedienablaufes von der Datenzentrale zur Frankiermaschine wird überflüssig, wenn der Bedienablauf zeitabhängig geändert wird. In der Datenzentrale und in der Frankiermaschine wird der gleiche Berechnungsalgorithmus verwendet, um einen aktuellen Bedienablauf zu ermitteln. Eine andere Variante geht von der Einspeicherung des aktuellen Bedienablaufes in die Frankiermaschine mittels eines speziellen Reset-E^2PROMs durch den Service-Techniker aus.

[0188] In einer weiteren Variante wird die Sicherheit von einer autorisierten Person mittels einem zusätzlichen Eingabesicherheitsmittel erhöht, welches mit der Frankiermaschine in Kontakt gebracht wird, um ein

Restguthaben zurück zur Datenzentrale zu übertragen. Zunächst wird bei der Datenzentrale die Aktualität hergestellt, indem die Registerstände mittels einer Null-Fernwertvorgabe gemeldet werden. Anschließend wird als Eingabesicherheitsmittel vom Service-Techniker ein Rücksetz-Nurlese-Speicherbaustein in einen vorbestimmten Sockel der mindestens teilweise geöffneten Frankiermaschine eingesetzt. Nachdem Einschalten bzw. einem Seiteneinstieg in das Programm der Frankiermaschine wird geprüft, ob ein Rücksetz-Nurlese-Speicherbaustein (Refunds-EPROM) eingesetzt wurde. Die kann vorteilhaft im - in der Figur 2 gezeigten - Schritt 219 zur überprüfung eines weiteren Kriteriums erfolgen. Ein richtiger Seiteneinstieg bei nicht vorhandenen Refunds-EPROM führt zum Punkt e oder in einer nicht gezeigten Variante einen Schritt zum Abbruch der Routine. Beispielsweise kann auf einen Schritt 209 zum Löschen eines Flags X verzweigt werden, was im Schritt 409 des Frankiermodus (Figur 4) bemerkt würde und zur Statistik und Fehlerauswertung bzw. Registrierung im Schritt 213 führt. Anderenfalls, beim richtigen Seiteneinstieg und bei gestecktem Refunds-EPROM wird ein Sonder-Flag N gesetzt, was im Kommunikationsmodus automatisch das Rückübertragen des Restguthabens zur Datenzentrale auslöst.

[0189] In einer Subvariante können die Schritte 218 und 219 gemäß Figur 2 in ihrer Reihenfolge vertauscht ablaufen, so daß erst hinsichtlich des gesteckten Refunds-EPROM und erst danach nach dem richtigen Seiteneinstieg gefragt wird. Eine solche Subvariante hat den Vorteil, daß die Information über den richtigen Seiteneinstieg ebenfalls im Refunds-EPROM gespeichert werden kann, anstatt in der Frankiermaschine. Damit wird die Sicherheit vor einer Manipulation in Fälschungsabsicht weiter erhöht.

[0190] In der Datenzentrale wird der Zustand der Frankiermaschine (out of Service) gespeichert. Die autorisierte Person entfernt das Eingabesicherheitsmittel aus dem Sockel und schließt das Gehäuse der Frankiermaschine. In der Datenzentrale werden wie in der Frankiermaschine die Guthaben registrierenden Postregister für verfügbares Restguthaben R1, Verbrauchssummenbetrag R2 und Gesammtbetrag R3 auf Null gesetzt (R1 = 0; R2 = 0; R3 = R1 + R2 = 0).

[0191] Bei einer in der Frankiermaschine vorhandenen Chipkarten-Schreib/Leseeinheit kann das Eingabesicherheitsmittel natürlich auch als Chipkarte realisiert werden.

[0192] Die Erfindung ist nicht auf die vorliegenden Ausführungsformen beschränkt. Vielmehr ist eine Anzahl von Varianten im Rahmen der Ansprüche denkbar.

Patentansprüche

1. Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen gegen Manipulation mit einem Mikroprozessor in einer Steuereinheit der Frankiermaschine zur Ausführung von Schritten für eine Start- und Initialisierungsroutine und nachfolgender Systemroutine mit einer Möglichkeit in einen Kommunikationsmodus mit einer entfernten Datenzentrale einzutreten, um einen Guthabenwert zu laden oder an die Datenzentrale zurück zu übertragen sowie weiteren Eingabeschritten, um in einen Frankiermodus einzutreten von dem nach Ausführung einer Abrechnungs-und Druckroutine in die Systemroutine zurückverzweigtwird, **gekennzeichnet**, **durch** Unterscheiden zwischen nichtmanipuliertem und manipuliertem Betrieb einer Frankiermaschine mittels der Steuereinrichtung (6), indem während eines Betriebsmodus (290) eine Überwachung der Zeitdauer des Ablaufes von Programmen, Programmteilen bzw. sicherheitsrelevanter Routinen vorgenommen wird und durch einen nach Ablauf von Programmen, Programmteilen bzw. sicherheitsrelevanten Routinen anschließenden Vergleich der gemessenen Laufzeit mit einer vorgegebenen Laufzeit.

2. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet,** daß ein decrementaler Zähler oder ein incrementaler Zähler verwendet wird, um ein Überschreiten der Zeit t1 im Sondermodus als ein sicheres Indiz für eine mißglückte Übertragung zu detektieren und daß ein spezielles Unterprogrammm aufgerufen wird, welches eine erneute Durchführung des Sondermodus negative Fernwertvorgabe vorbereitet und automatisch auslöst, so daß die erste und zweite Transaktion automatisch wiederholt werden.

3. Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen gegen Manipulation mit einem Mikroprozessor in einer Steuereinheit der Frankiermaschine zur Ausführung von Schritten für eine Start- und Initialisierungsroutine und nachfolgender Systemroutine mit einer Möglichkeit in einen Kommunikationsmodus mit einer entfernten Datenzentrale einzutreten, um einen Guthabenwert zu laden oder an die Datenzentrale zurück zu übertragen sowie weiteren Eingabeschritten, um in einen Frankiermodus einzutreten von dem nach Ausführung einer Abrechnungs-und Druckroutine in die Systemroutine zurückverzweigt wird, **gekennzeichnet, durch** während einer Kommunikation im Kommunikationsmodus (300) vorgenommene Überwachung der Einhaltung eines bestimmten Zeitablaufes im Sondermodus negative Fernwertvorgabe, insbesondere der Zeitdauer vom Senden einer dritten verschlüsselten Mitteilung seitens der Frankiermaschine bis zum Empfang der von der Datenzentrale an die Frankiermaschine gesendeten vierten verschlüsselten Mitteilung in der Frankiermaschine, welche bei Verifizierung ein Null-Setzen des Guthabenwerts auslöst.

4. Verfahren, nach Anspruch 3, **dadurch gekennzeichnet,** daß ein decrementaler Zähler oder ein incrementaler Zähler verwendet wird, um ein Überschreiten der Zeit t1 im Sondermodus als ein sicheres Indiz für eine mißglückte Übertragung zu detektieren und daß ein spezielles Unterprogrammm aufgerufen wird, welches eine erneute Durchführung des Sondermodus negative Fernwertvorgabe vorbereitet und automatisch auslöst, so daß die erste und zweite Transaktion automatisch wiederholt werden.

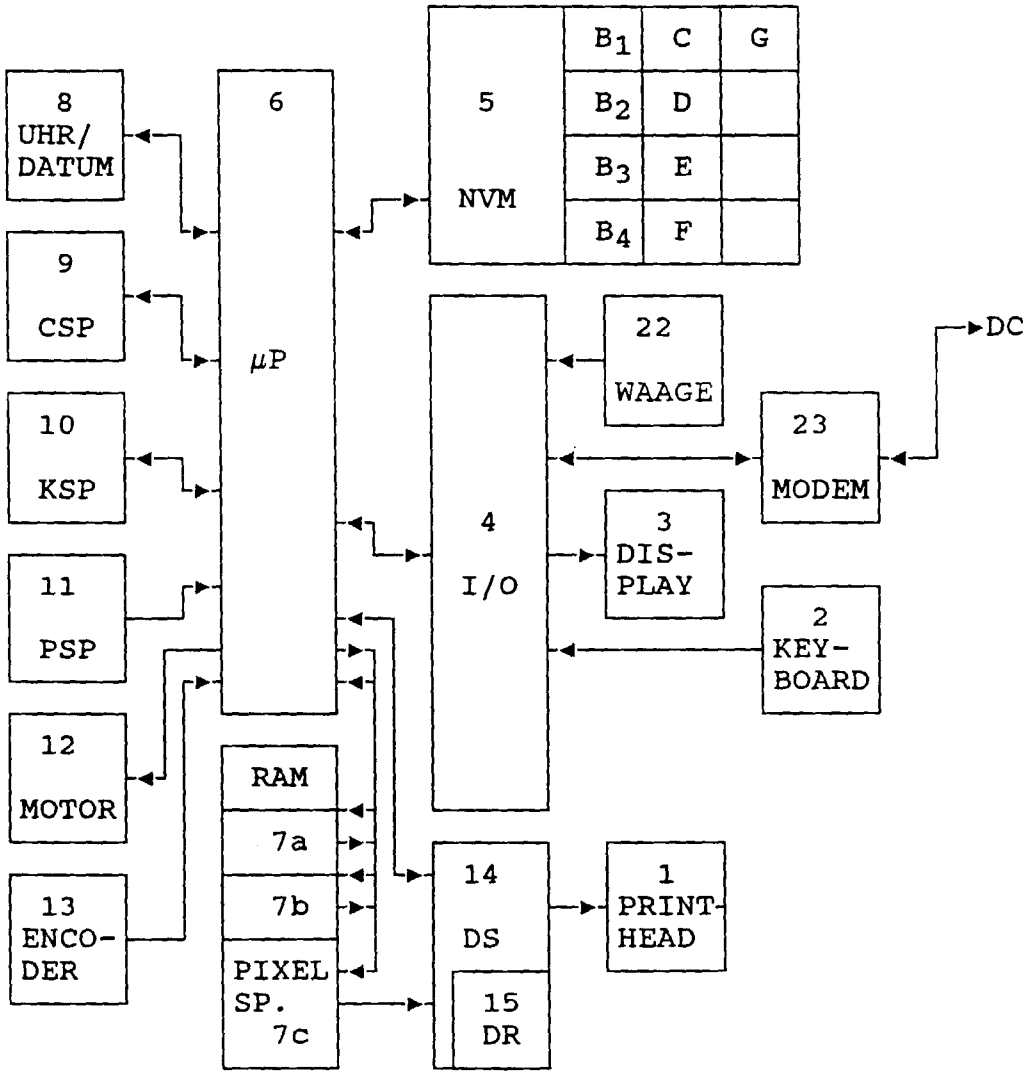
8
UHR/
DATUM
9
CSP
10
KSP
11
PSP
12
MOTOR
13
ENCO-
DER
6
µP
RAM
7a
7b
PIXEL
SP.
7c
5
NVM
B1
B2
B3
B4
C
D
E
F
G
4
I/O
22
WAAGE
23
MODEM
DC
3
DIS-
PLAY
2
KEY-
BOARD
14
DS
15
DR
1
PRINT-
HEAD

Fig. 1

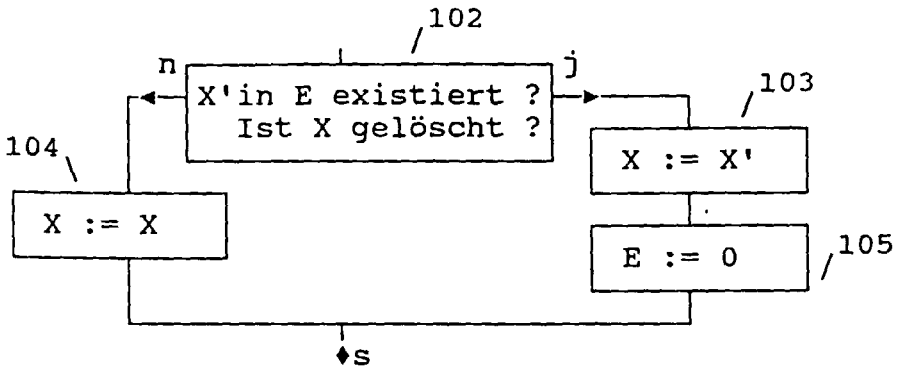
102
n
X'in E existiert ?
Ist X gelöscht ?
j
103
X := X'
104
X := X
E := 0
105
s

Fig. 7

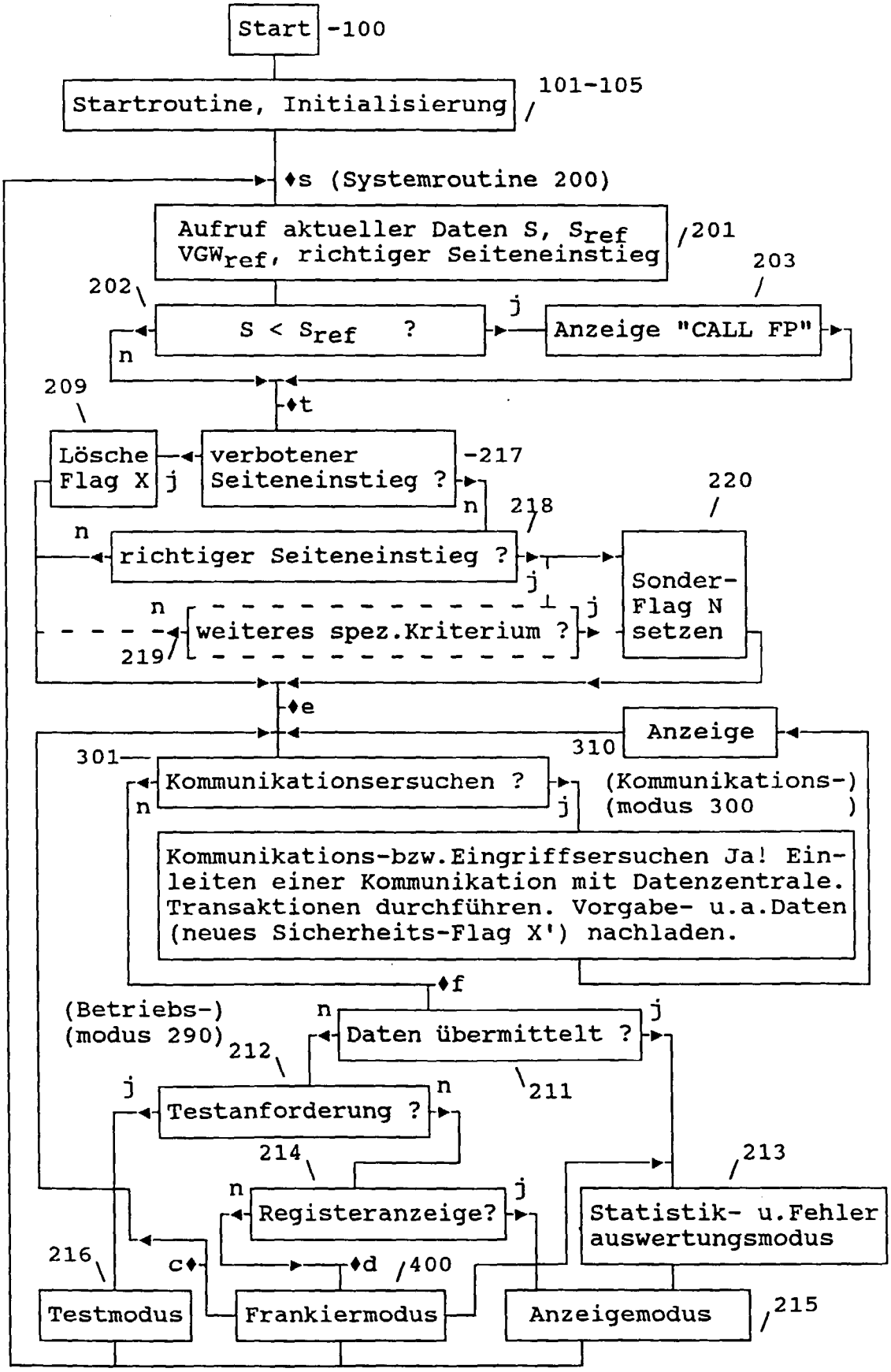
Start
-100
Startroutine, Initialisierung
101-105
♦s (Systemroutine 200)
Aufruf aktueller Daten S, S_{ref} VGW_{ref}, richtiger Seiteneinstieg
/201
202
S < S_{ref} ?
j
203
Anzeige "CALL FP"
n
209
♦t
Lösche Flag X
j
verbotener Seiteneinstieg ?
-217
n
218
220
n
richtiger Seiteneinstieg ?
j
Sonder-Flag N setzen
n
j
weiteres spez.Kriterium ?
219
♦e
Anzeige
310
301
Kommunikationsersuchen ?
n
j
(Kommunikations-) (modus 300)
Kommunikations-bzw.Eingriffsersuchen Ja! Einleiten einer Kommunikation mit Datenzentrale. Transaktionen durchführen. Vorgabe- u.a.Daten (neues Sicherheits-Flag X') nachladen.
♦f
(Betriebs-) (modus 290)
n
Daten übermittelt ?
j
212
211
j
Testanforderung ?
n
214
213
n
Registeranzeige?
j
Statistik- u.Fehler auswertungsmodus
216
c♦
♦d
/400
Testmodus
Frankiermodus
Anzeigemodus
/215

Fig. 2

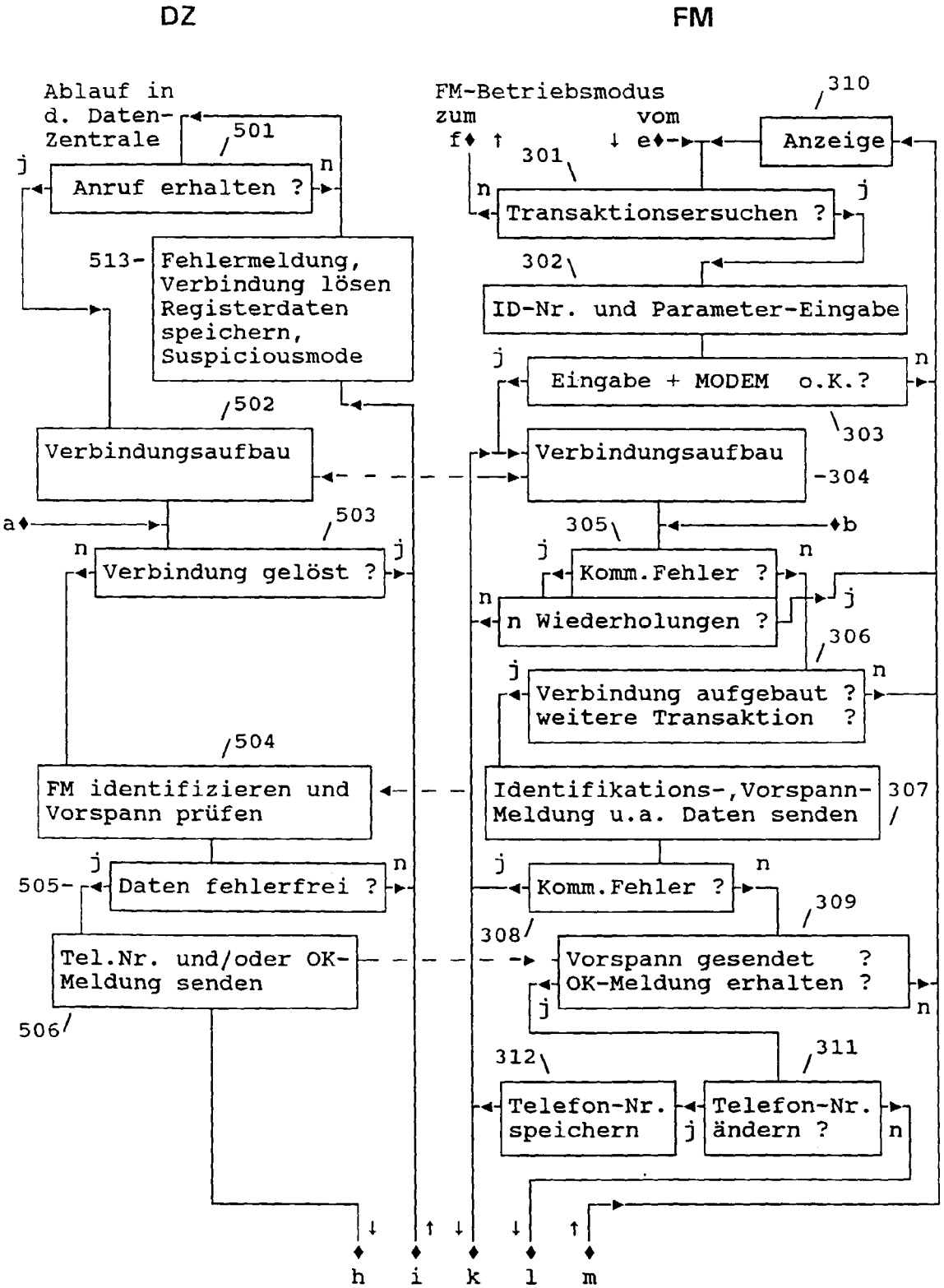
DZ
FM
Ablauf in d. Daten-Zentrale
501
Anruf erhalten ?
j
n
513-
Fehlermeldung, Verbindung lösen Registerdaten speichern, Suspiciousmode
502
Verbindungsaufbau
a
503
Verbindung gelöst ?
n
j
504
FM identifizieren und Vorspann prüfen
505-
Daten fehlerfrei ?
j
n
Tel.Nr. und/oder OK-Meldung senden
506
FM-Betriebsmodus zum
vom
f
e
310
Anzeige
301
Transaktionsersuchen ?
n
j
302
ID-Nr. und Parameter-Eingabe
Eingabe + MODEM o.K.?
j
n
303
Verbindungsaufbau
-304
305
b
Komm.Fehler ?
j
n
n Wiederholungen ?
n
j
306
Verbindung aufgebaut ? weitere Transaktion ?
j
n
Identifikations-,Vorspann-Meldung u.a. Daten senden
307
Komm.Fehler ?
j
n
308
309
Vorspann gesendet ? OK-Meldung erhalten ?
j
n
312
311
Telefon-Nr. speichern
Telefon-Nr. ändern ?
j
n
h
i
k
l
m

Fig. 3a

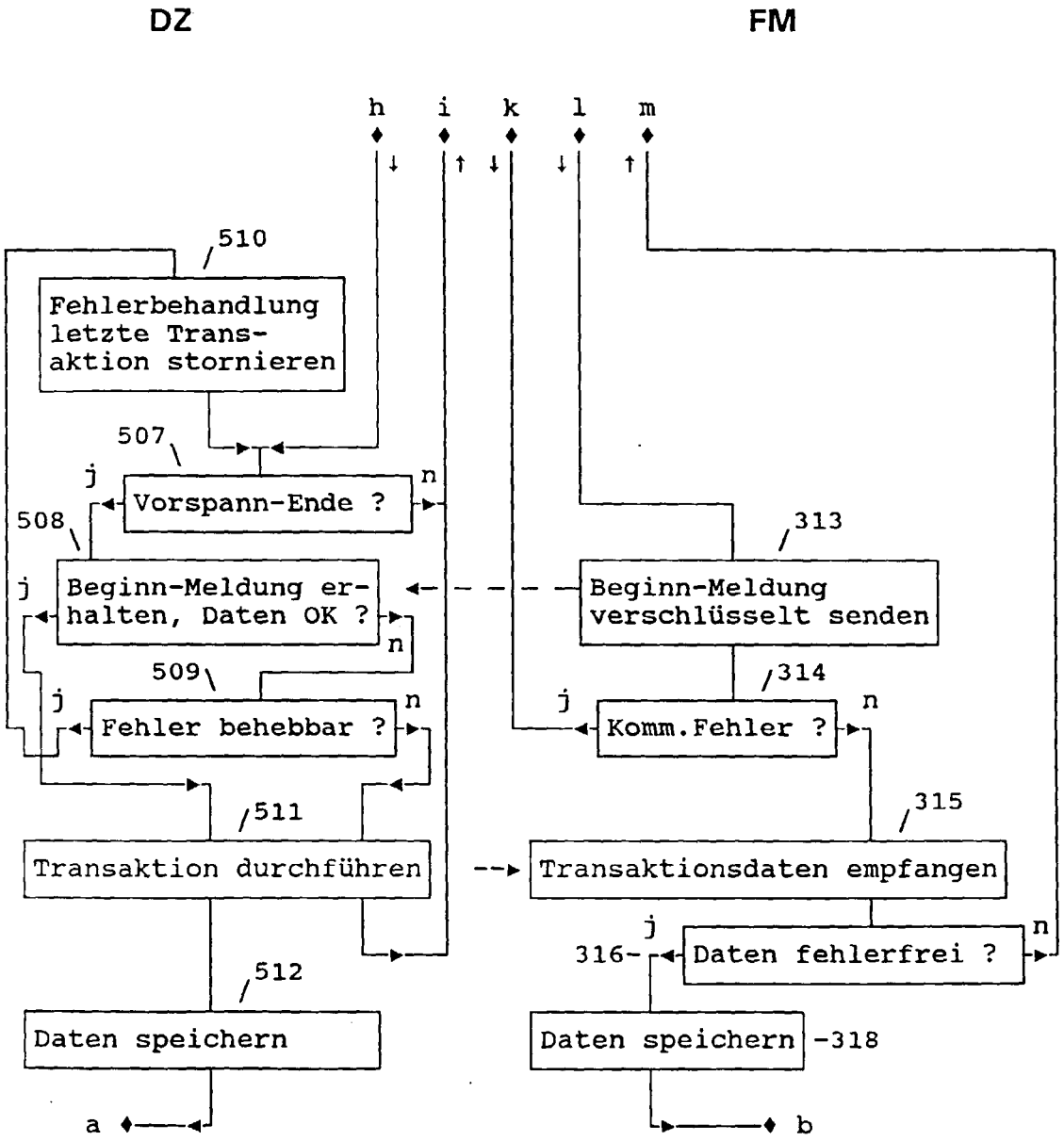
DZ
FM
h
i
k
l
m
510
Fehlerbehandlung letzte Trans-aktion stornieren
507
j
n
Vorspann-Ende ?
508
313
j
Beginn-Meldung er-halten, Daten OK ?
n
Beginn-Meldung verschlüsselt senden
509
314
j
Fehler behebbar ?
n
j
Komm.Fehler ?
n
511
315
Transaktion durchführen
Transaktionsdaten empfangen
j
n
316
Daten fehlerfrei ?
512
Daten speichern
Daten speichern
318
a
b

Fig. 3b

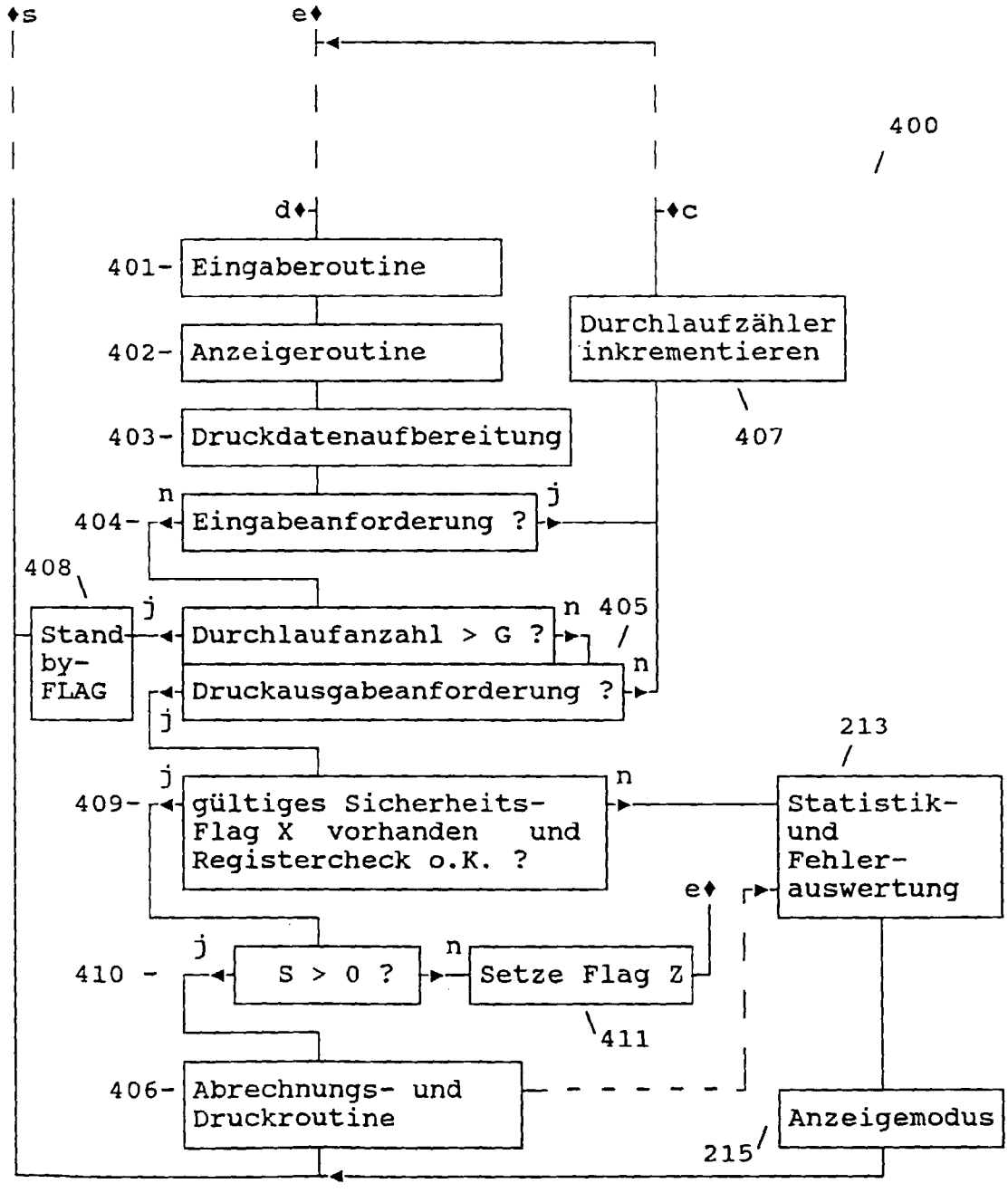
♦s
e♦
400
d♦
♦c
401-
Eingaberoutine
402-
Anzeigeroutine
403-
Druckdatenaufbereitung
Durchlaufzähler inkrementieren
407
n
j
404-
Eingabeanforderung ?
408
Stand by- FLAG
j
n
405
Durchlaufanzahl > G ?
n
Druckausgabeanforderung ?
j
213
j
n
409-
gültiges Sicherheits- Flag X vorhanden und Registercheck o.K. ?
Statistik- und Fehler- auswertung
e♦
j
n
410 -
S > 0 ?
Setze Flag Z
411
406-
Abrechnungs- und Druckroutine
Anzeigemodus
215

Fig. 4

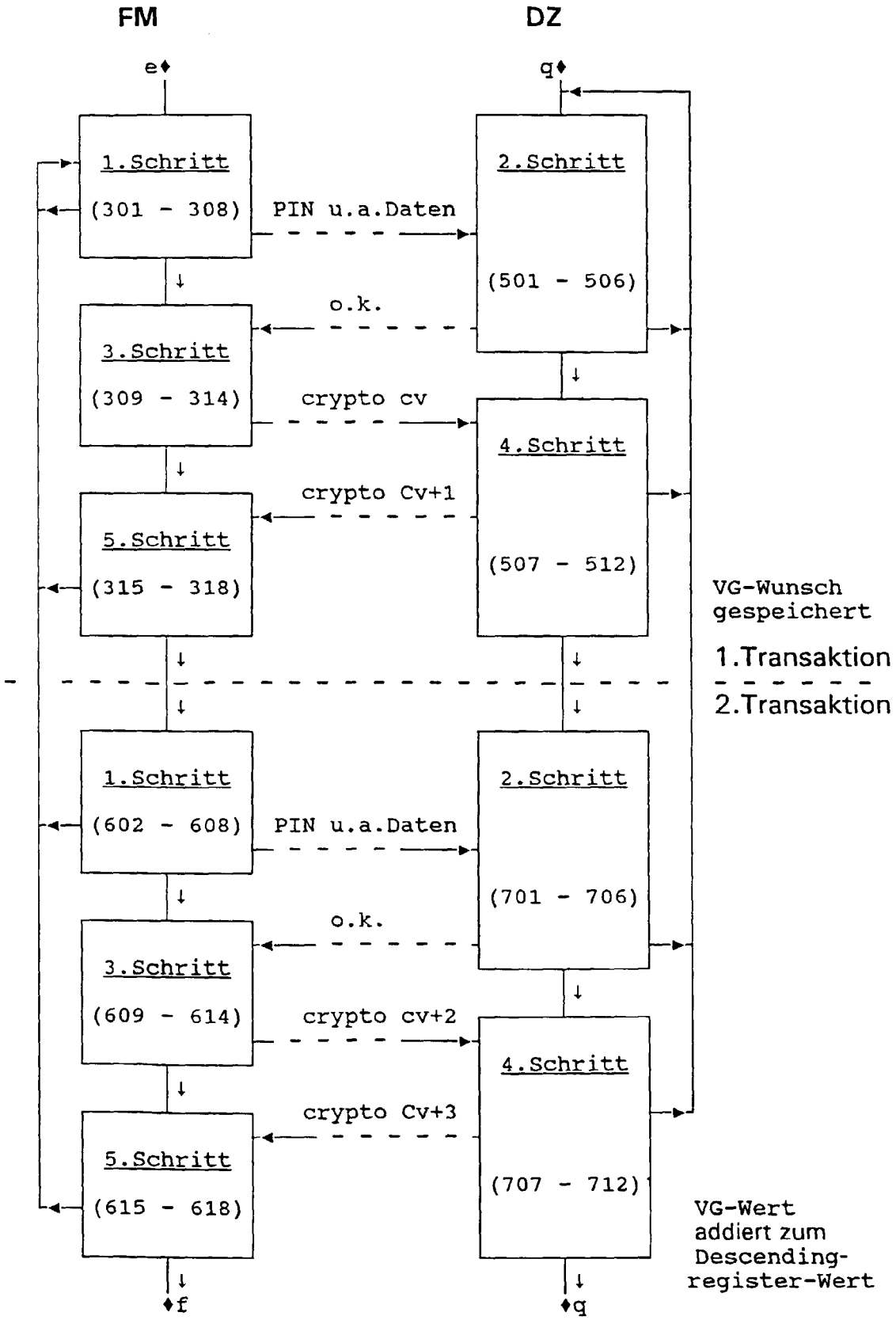
FM
DZ
e♦
q♦
1.Schritt
(301 - 308)
PIN u.a.Daten
2.Schritt
(501 - 506)
o.k.
3.Schritt
(309 - 314)
crypto cv
4.Schritt
(507 - 512)
crypto Cv+1
5.Schritt
(315 - 318)
VG-Wunsch gespeichert
1.Transaktion
2.Transaktion
1.Schritt
(602 - 608)
PIN u.a.Daten
2.Schritt
(701 - 706)
o.k.
3.Schritt
(609 - 614)
crypto cv+2
4.Schritt
(707 - 712)
crypto Cv+3
5.Schritt
(615 - 618)
VG-Wert addiert zum Descending-register-Wert
♦f
♦q

Fig.5

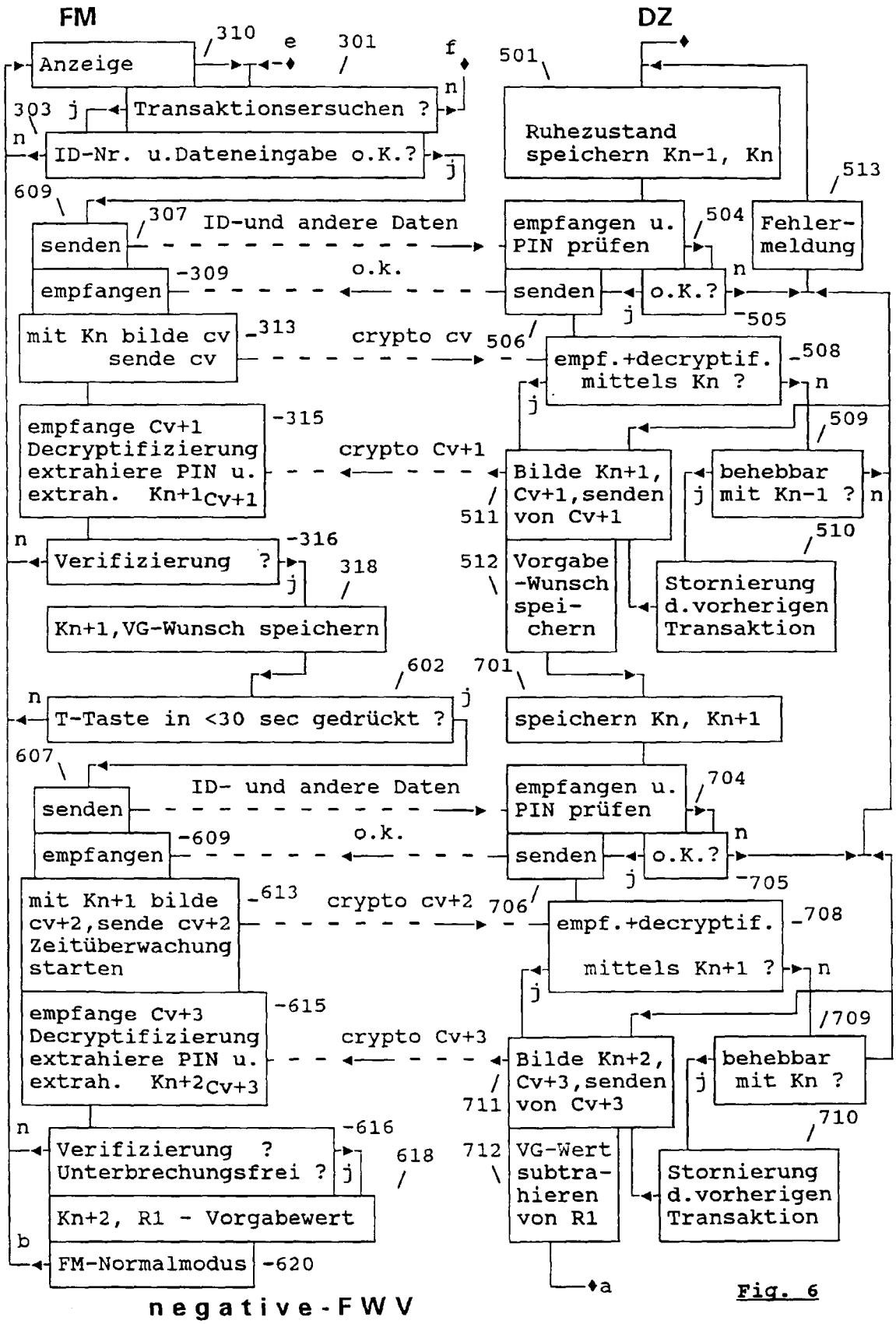
FM
DZ
Anzeige
310
e
301
f
501
Transaktionsersuchen ?
303
j
n
ID-Nr. u.Dateneingabe o.K.?
Ruhezustand speichern Kn-1, Kn
513
609
senden
307
ID-und andere Daten
empfangen u. PIN prüfen
504
Fehler-meldung
empfangen
-309
o.k.
senden
o.K.?
-505
mit Kn bilde cv sende cv
-313
crypto cv
506
empf.+decryptif. mittels Kn ?
-508
empfange Cv+1 Decryptifizierung extrahiere PIN u. extrah. Kn+1Cv+1
-315
crypto Cv+1
Bilde Kn+1, Cv+1,senden von Cv+1
511
behebbar mit Kn-1 ?
509
Verifizierung ?
-316
318
Vorgabe -Wunsch spei-chern
512
Stornierung d.vorherigen Transaktion
510
Kn+1,VG-Wunsch speichern
602
701
T-Taste in <30 sec gedrückt ?
speichern Kn, Kn+1
607
ID- und andere Daten
704
-609
-705
mit Kn+1 bilde cv+2,sende cv+2 Zeitüberwachung starten
-613
crypto cv+2
706
empf.+decryptif. mittels Kn+1 ?
-708
empfange Cv+3 Decryptifizierung extrahiere PIN u. extrah. Kn+2Cv+3
-615
crypto Cv+3
Bilde Kn+2, Cv+3,senden von Cv+3
711
behebbar mit Kn ?
709
710
Verifizierung ? Unterbrechungsfrei ?
-616
618
712
VG-Wert subtra-hieren von R1
Stornierung d.vorherigen Transaktion
Kn+2, R1 - Vorgabewert
b
FM-Normalmodus
-620
a
negative-FWV

Fig. 6