(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 199 28 058 B4** 2005.10.20

(12) **Patentschrift**

(21) Aktenzeichen: **199 28 058.4**
(22) Anmeldetag: **15.06.1999**
(43) Offenlegungstag: **28.12.2000**
(45) Veröffentlichungstag der Patenterteilung: **20.10.2005**

(51) Int Cl.[7]: **G07B 17/02**
**G07B 17/04**

Innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zur erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten(§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 2 Patentkostengesetz).

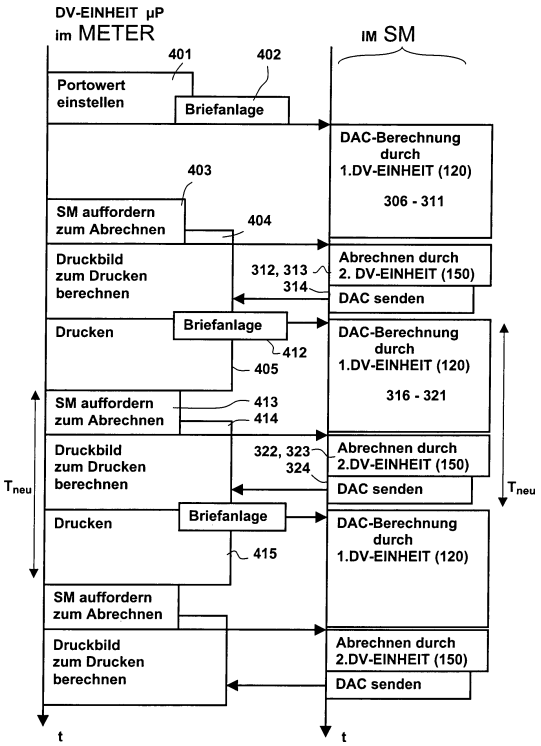
(73) Patentinhaber:
**Francotyp-Postalia AG & Co. KG, 16547 Birkenwerder, DE**

(72) Erfinder:
**Rosenau, Dirk, 13469 Berlin, DE; Wagner, Andreas, 13503 Berlin, DE**

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
**US 48 31 555**
**US 47 25 718**
**EP 6 47 925 A2**
**SCHÖNLEBER, C.: Die Suche nach dem Schlüssel, mc extra, 4/95, S. 30-33;**
**LUCKHARDT, N.: Qnf jne rvasnpu, tryy?, c't, H. 12, 1996, S. 110-113;**

(54) Bezeichnung: **Anordnung und Verfahren zur Generierung eines Sicherheitsabdruckes**

(57) Hauptanspruch: Anordnung zur Generierung eines Sicherheitsabdruckes, mit einem Sicherheitsmodul, der einen Programmspeicher (128), mindestens eine erste Datenverarbeitungseinheit (120) und nichtflüchtige Speicher (114, 116) einschließt, wobei die erste Datenverarbeitungseinheit (120) zur Generierung eines Sicherheitscodes programmiert ist und mit einer separaten Datenverarbeitungseinheit extern des Sicherheitsmoduls, die durch ein Programm in ihrem Programmspeicher (92) zu einer Druckdatenaufbereitung und zur Berechnung eines Druckbildes programmiert ist, das den Sicherheitscode enthält, gekennzeichnet dadurch, dass die erste Datenverarbeitungseinheit (120) durch ein Programm im Programmspeicher (128) programmiert ist,
– bei jeder Nachricht für neue Systemdaten sofort eine Neuberechnung des Sicherheitscodes zu starten, sofern die neuen Systemdaten vom Sicherheitsmodul als gültig erkannt und für den Sicherheitscode benötigt werden, wobei der Sicherheitscode ein Datenautorisierungscode (DAC) ist,
– die ersten n Bytes des Datenautorisierungscode (DAC) nach einem Algorithmus in einer ersten Runde für jeden Tag vorauszuberechnen, den Registerwert für das steigende Register (R2) mittels des eingegebenen Portowertes in einer weiteren...



## Beschreibung

**[0001]** Die Erfindung betrifft eine Anordnung zur Generierung eines Sicherheitsabdruckes, gemäß der im Oberbegriff des Anspruchs 1 angegebenen Art und für ein Verfahren zur Generierung eines Sicherheitsabdruckes, gemäß der im Oberbegriff des Anspruchs 9 angegebenen Art. Ein solcher postalischer Sicherheitsmodul ist ein Teil einer solchen Anordnung, die sich insbesondere für den Einsatz in einer Frankiermaschine bzw. Postbearbeitungsmaschine oder Computer mit Postbearbeitungsfunktion eignet. Das Verfahren dient der Sicherung vor einer Manipulation mit nichtbezahlten Frankierungen auf Postgütern.

### Stand der Technik

**[0002]** In EP 862 143 A2 wurde eine Frankiermaschine für die Erzeugung und Überprüfung eines Sicherheitsabdruckes vorgeschlagen. Ein Sicherheitsabdruck weist eine maschinenlesbare Markierung mit variablen Daten und einen Krypto- bzw. Authentisierungscode auf.

**[0003]** Zur Überprüfung des Sicherheitsabdruckes wird ein aus den variablen Daten gebildeter Kryto- bzw. Authentisierungscode mit dem aufgedruckten Kryto- bzw. Authentisierungscode verglichen. Die Frankiermaschine hat einen einzigen Mikroprozessor, der sowohl einen Krytocode bzw. einen DAC (DATA AUTHENTIFICATION CODE) zur Absicherung der Druckdaten, als auch das Druckbild selbst berechnet. Letzteres besteht aus festen Rahmenpixeldaten und den Fensterpixeldaten. Fensterpixeldaten sind variable und semivariable Druckdaten.

**[0004]** Dabei wurde vorgeschlagen, um die Rechenzeit optimal auszunutzen, die Druckdaten für den Krytocode bzw. einen DAC und diejenigen variablen Daten, die sich relativ häufig ändern, erst kurz vor dem Drucken in das berechnete Druckbild einzufügen. Bei Frankiermaschinen mit spaltenweisen Druck auf ein bewegtes Postgut, wobei die Druckzeile im Druckkopf orthogonal zur Transportrichtung des Briefes angeordnet ist, kann sich eine Möglichkeit ergeben, die vorgenannten variablen Daten direkt in das Druckregister der Drucksteuerung für den Druckkopf zu übertragen, wobei die Übertragung sequentiell mit den Rahmenpixeldaten erfolgt. Damit wird eine Möglichkeit geschaffen, erst spät fertigberechnete DAC-Druckdaten auch noch nachträglich während des Druckens einzubetten. Beispielsweise bei der Frankiermaschine T1000 der Anmelderin, welche nach einem Thermotransferdruckverfahren arbeitet, ergibt sich bei Lauflängencodierung der Druckdaten, eine solche Möglichkeit unter der Voraussetzung, daß bereits einige der festen Rahmenpixeldaten und der zuvor eingebetteten Fensterpixeldaten bereits gedruckt werden, so daß die DAC-Druckdaten erst spät eingebettet können, weil das entsprechende Fenster erst später gedruckt werden muß. Wenn jedoch seitens eines Postbeförderers die Forderung besteht, das betreffende Fenster zuerst zu drucken, muß die Einbettung der Druckdaten im Vorab erfolgen. Wenn die Änderungen sich über mehrere Druckspalten erstrecken, wobei mehr als die Hälfte der Druckspalten des gesamten Druckbildes verändert werden müssen, resultiert daraus eine entsprechende Verlängerung der Rechenzeit. Dann ist aber vor jedem Frankierbildausdrucken eine Neuberechnung des Druckbildes mit anderen variablen Fensterdaten und mit neuen DAC-Druckdaten nötig. Der Durchsatz beim Frankieren wird bei solchen Druckbildern für einen Sicherheitsabdruck deutlich verringert.

**[0005]** Aus der US 4.831.555 und US 4725718 sind offene Systeme mit einer Metereinheit, einem Personalcomputer und einem Drucker bekannt. Ein solches System bildet ein offenes System und wird auch PC-Frankierer genannt. Die Metereinheit liefert eine verschlüsselte Mitteilung mit Adresseninformationen und anderen Daten. Solche PC-Frankierer werden zur Einzelpostverarbeitung eingesetzt und sind für Massenpost ungeeignet. Dagegen werden für Massenpost Frankiermaschinen eingesetzt, welche geschlossene Systeme bilden.

**[0006]** Aus dem EP 647925 A2 ist ein Postgebührensystem mit nachprüfbarer Unversehrtheit bekannt, wobei ein Empfangen und Prüfen einer Information im Benutzergerät mittels einer aus den Dienstdaten generierten Vergleichsinformation erfolgt. Diese Lösung ist für die Übermittlung einer Portogebührenliste von einer Datenzentrale zum Benutzergerät vorgesehen und dabei für beide offene und geschlossene Systeme einsetzbar. Der Durchsatz beim Frankieren kann damit allerdings nicht erhöht werden.

**[0007]** Bekannte Möglichkeiten der Kryptographie erfordern einen erheblichen Rechenaufwand (Schönleber, C.: Die Suche nach dem Schlüssel; mc extra, 4/95, S. 30–33 bzw. Luckhardt, N.: Qnf jne rvasnpu, tryy ?; c't, H. 12, 1996, S. 110–113) zum Erzeugen eines Sicherheitsabdrucks.

### Aufgabenstellung

**[0008]** Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Anordnung zu entwickeln, um den

Durchsatz an Post beim Frankieren mit einem Sicherheitsabdruck zu erhöhen.

**[0009]** Bei Frankiermaschinen mit hohem Durchsatz (Systemtakt) ist eine Technik zu entwickeln, bei der nach jeder erfolgreichen Abrechnung der Frankierabdruck durch einen Sicherheitscodesigniert wird. Hierbei muß die Signatur schnell genug errechnet werden, um sie abhängig vom Systemtakt der Frankiermaschine schnell genug für die Druckbildberechnung zur Verfügung zu stellen. Auch wenn die Änderungen in den Druckdaten von Abdruck zu Abdruck maximal sind, soll dadurch der Durchsatz nicht verringert werden, daß ein Sicherheitsabdruck gedruckt wird.

**[0010]** Die Aufgabe wird mit den Merkmalen des Anspruchs 1 für eine Anordnung und mit den Merkmalen des Anspruchs 9 für ein Verfahren gelöst.

**[0011]** Eine Lösung des Problems wurde in der Durchführung von zwei zeitlich versetzten Berechnungen durch unterschiedliche Rechner gefunden. Die Berechnung des Sicherheitscodes wird erfindungsgemäß von einem separaten Sicherheitsmodul vorgenommen, während die Druckbilddatenaufbereitung vom Frankiermaschinen-Prozessor vorgenommen wird. Durch geschicktes Verschachteln der beiden Aufgaben und spezielle Auswahl von Algorithmen und Datenstrukturen wird eine hohe Systemtaktleistung erzielt.

**[0012]** Das Sicherheitsmodul wird so implementiert, daß alle für den Sicherheitscode DAC benötigten Systemdaten über Nachrichten von der Frankiermaschine voreingestellt werden. Jede Nachricht, die solche Systemdaten verändert, startet sofort, sofern die neuen Systemdaten vom Sicherheitsmodul als gültig erkannt werden, eine Neuberechnung des Sicherheitscodes. Eine über eine separate Nachricht an das Sicherheitsmodul gemeldete Aufforderung zur Abrechnung startet die Abrechnung. Das Sicherheitsmodul sendet den Sicherheitscode an die Frankiermaschine FM, wobei letztere die Druckdatenaufbereitung und Berechnung des Druckbildet vornimmt. Für Massenfrankierungen mit hohem Systemtakt ergibt sich folgende zeitliche Verschachtelung der Operationen beider Datenverarbeitungseinheiten, die zu einer hohen Systemleistung führt. Die zeitliche Verschachtelung läßt sich nur durch folgende zwei Maßnahmen ermöglichen:

1. Zwei Verarbeitungseinheiten (FM/FPSM)
2. Vorberechnung des Sicherheitscodes aufgrund voreingestellter Werte.

**[0013]** Das Verfahren findet beispielsweise in Frankiermaschinen Anwendung, für die besondere Sicherheitsforderungen bezüglich der Postregisterdaten und des Abdruckes gelten, da insbesondere die geldwerten Abrechnungsdaten unmanipulierbar sein müssen.

Ausführungsbeispiel

**[0014]** 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:

**[0015]** Fig. 1a, Zeit/Steuerungsdiagramm für eine Frankiermaschine bekannter Art mit einem Mikroprozessor,

**[0016]** Fig. 1b, Zeit/Steuerungsdiagramm für eine Frankiermaschine nach der Erfindung mit einem Mikroprozessor im Meter für die Druckaufgaben und einem Sicherheitsmodul für die Sicherheitsaufgaben,

**[0017]** Fig. 2, Blockschaltbild einer Frankiermaschine mit Sicherheitsmodul,

**[0018]** Fig. 3, Perspektivische Ansicht der Frankiermaschine von hinten,

**[0019]** Fig. 4, Darstellung eines Sicherheitsabdrucks,

**[0020]** Fig. 5, Blockschaltbild des Sicherheitsmoduls,

**[0021]** Fig. 6, Flußdiagramm für das Erzeugen von Sicherheitsabdrucken beim Frankieren.

**[0022]** In der Fig. 1a ist ein Zeit/Steuerungsdiagramm für eine Frankiermaschine dargestellt, die in bekannter Art mit einem Mikroprozessor ausgestattet ist, der für das Erzeugen von Sicherheitsabdrucken beim Frankieren folgende Schritte ausführt:

– Eingaberoutine **401**, um den Portowert einzustellen,

- Sensorroutine **402**, um die Briefanlage festzustellen, mit
- Subroutine **406**-**411** zur DAC-Berechnung,
- Aufforderungsroutine **403** zum Abrechnen, mit
- Subroutine **412**, **413** zum Abrechnen und mit
- Subroutine zum DAC bereitstellen,
- Berechnungsroutine **404** für das Druckbild sowie
- Druckroutine **405**.

**[0023]** Aufgrund der sequentiellen Verarbeitung der Daten bei der Durchführung der einzelnen Routinen und Subroutinen wird eine Datenverarbeitungszeitdauer $T_{alt}$ je Frankierung mit einem Sicherheitsabdruck benötigt.

**[0024]** Das erfindungsgemäße – in der Fig. 1b gezeigte – Zeit/Steuerungsdiagramm für eine Frankiermaschine benötigt eine Datenverarbeitungszeitdauer $T_{neu}$ je Frankierung mit einem Sicherheitsabdruck, welche kürzer ist, als die alte Datenverarbeitungszeitdauer $T_{alt}$ je Frankierung. Das ist nur möglich, weil bei der Erfindung eine Aufgabenteilung für zwei Datenverabeitungseinheiten stattfindet, wobei ein Mikroprozessor im Meter für die Druckaufgaben und ein Sicherheitsmodul für die Sicherheitsaufgaben vorgesehen ist.

**[0025]** Die Druckaufgaben umfassen eine Eingaberoutine **401**, um den Portowert einzustellen, eine Sensorroutine **402**, um die Briefanlage festzustellen, eine Aufforderungsroutine **403** zum Abrechnen, eine Berechnungsroutine **404** für das Druckbild sowie eine Druckroutine **405**.

**[0026]** Die Sicherheitsaufgaben umfassen eine Subroutine **406**–**411** zur DAC-Berechnung, eine Subroutine **412**, **413** zum Abrechnen und eine Subroutine zum DAC bereitstellen.

**[0027]** Die Berechnungsroutine **404** für das Druckbild ist besonders aufwendig für einen Sicherheitsabdruck, deshalb wird mit dem Druckbildaufbau schon vor dem Ende der Abrechnung begonnen. Außerdem führt der Mikroprozessor im Meter die Druckroutine **405** durch, während der Sicherheitsmodul bereits den Sicherheitscode das nächste Druckbild berechnet, sobald das Anlegen eines weiteren Briefes am Eingang des Transportweges von einem Briefsensor erfaßt wird.

**[0028]** Das ist besonders bei Massenfrankierungen von Poststücken, insbesondere von Briefen, mit dem gleichen Portowert sinnvoll. Das Anlegen eines weiteren Briefes, welches am Eingang des Transportweges von einem Briefsensor erfaßt wird, löst einen Interrupt für den Mikroprozessor im Meter aus, welcher die Briefanlage an das Sicherheitsmodul weitermeldet und dann die begonnenen Berechnungen zum Druckbildaufbau fortsetzt. In dem Patent US 5,710,721 wurde unter dem Titel: INTERNAL POSTAGE METER MACHINE INTERFACE CIRCUIT prinzipiell beschrieben, wie bei einem Sensorsignal ein Interrupt für den Mikroprozessor ausgelöst wird und wie die Drucksteuerung arbeitet.

**[0029]** Erfindungsgemäß arbeitet der Mikroprozessor noch am Druckbildaufbau (schritt **404**) oder ist mit der Durchführung der Druckroutine (Schritt **405**) beschäftigt, während die Weitermeldung **412** einer weiteren Briefanlage an das Sicherheitsmodul SM erfolgt, woraufhin letzteres bereits weiterer Berechnungen **316**–**321** für ein nächstes Poststück (Brief) durchführt.

**[0030]** Sobald der Mikroprozessor mit der Durchführung der Druckroutine (Schritt **405**) fertig ist, ergeht eine Aufforderung an das Sicherheitsmodul, eine Abrechnung durchzuführen. Das Sicherheitsmodul SM führt nun die Abrechnung (Schritte **322**, **323**) durch und sendet (Schritt **324**) den Sicherheitscode DAC an den Mikroprozessor **91** des Meters, welches nun in der Lage ist den Druckbildaufbau für das weitere Druckbild zuende zu führen (Schritt **414**).

**[0031]** Die Fig. 2 zeigt ein Blockschaltbild einer Frankiermaschine. Die Steuereinrichtung **1** weist ein mit einem Mikroprozessor **91** mit zugehörigen Speichern **92**, **93**, **94**, **95** ausgestattetes Motherboard **9** auf.

**[0032]** Der Programmspeicher **92** enthält ein Betriebsprogramm mindestens zum Drucken und wenigstens sicherheitsrelevante Bestandteile des Programms für eine vorbestimmte Format-Änderung eines Teils der Nutzdaten.

**[0033]** Der Arbeitsspeicher RAM **93** dient zur flüchtigen Zwischenspeicherung von Zwischenergebnissen. Der nichtflüchtige Speicher NVM **94** dient zur nichtflüchtigen Zwischenspeicherung von Daten, beispielsweise von statistischen Daten, die nach Kostenstellen geordnet sind. Der Kalender/Uhrenbaustein **95** enthält ebenfalls adressierbare aber nichtflüchtige Speicherbereiche zur nichtflüchtigen Zwischenspeicherung von Zwischener-

gebnissen oder auch bekannten Programmteilen. Es ist vorgesehen, daß die Steuereinrichtung **1** mit einer Chipkarten-Schreib/Leseeinheit **70** verbunden ist, wobei der Mikroprozessor **91** der Steuereinrichtung **1** beispielsweise dazu programmiert ist, die Nutzdaten N aus dem Speicherbereich einer Chipkarte **49** zu deren Anwendung in entsprechende Speicherbereiche der Frankiermaschine zu laden. Eine in einen Einsteckschlitz **72** der Chipkarten-Schreib/Leseeinheit **70** eingesteckte erste Chipkarte **49** gestattet ein Nachladen eines Datensatzes in die Frankiermaschine für mindestens eine Anwendung. Die Chipkarte **49** enthält beispielsweise die Portogebühren für alle üblichen Postbeförderleistungen entsprechend des Tarifs der Postbehörde und ein Postbefördererkennzeichen, um mit der Frankiermaschine ein Stempelbild zugenerieren und entsprechend des Tarifs der Postbehörde die Poststücke freizustempeln.

**[0034]** Die Steuereinrichtung **1** bildet das eigentliche Meter mit den Mitteln **91** bis **95** der vorgenannten Hauptplatine **9** und umfaßt auch eine Tastatur **88**, eine Anzeigeeinheit **89** sowie einen anwendungsspezifischen Schaltkreis ASIC **90** und das Interface **8** für das postalische Sicherheitsmodul PSM **100**. Das Sicherheitsmodul PSM **100** ist über einen Steuerbus mit dem vorgenannten ASIC **90** und dem Mikroprozessor **91** sowie über den parallelen µC-Bus mindestens mit den Mitteln **91** bis **95** der Hauptplatine **9** und der mit Anzeigeeinheit **89** verbunden. Der Steuerbus führt Leitungen für die Signale CE, RD und WR zwischen dem Sicherheitsmodul PSM **100** und dem vorgenannten ASIC **90**. Der Mikroprozessor **91** weist vorzugsweise einen Pin für ein vom Sicherheitsmodul PSM **100** abgegebenes Interruptsignal i, weitere Anschlüsse für die Tastatur **88**, eine serielle Schnittstelle SI-1 für den Anschluß der Chipkarten-Schreib/Lese-Einheit **70** und eine serielle Schnittstelle SI-2 für den optionalen Anschluß eines MODEMs auf. Mittels des MODEMs kann beispielsweise das im nichtflüchtigen Speicher des postalischen Sicherheitsmittels PSM **100** gespeicherte Guthaben erhöht werden.

**[0035]** Das postalische Sicherheitsmittel PSM **100** wird von einem gesicherten Gehäuse umschlossen. Vor jedem Frankierabdruck wird im postalischen Sicherheitsmodul PSM **100** eine hardwaremäßige Abrechnung durchgeführt. Die Abrechnung erfolgt unabhängig von Kostenstellen.

**[0036]** Es ist vorgesehen, daß der ASIC **90** eine serielle Schnittstellenschaltung **98** zu einem im Poststrom vorschalteten Gerät, eine serielle Schnittstellenschaltung **96** zu den Sensoren und Aktoren der Druckeinrichtung **2**, eine serielle Schnittstellenschaltung **97** zur Drucksteuerelektronik **16** für den Druckkopf **4** und eine serielle Schnittstellenschaltung **99** zu einem der Druckeinrichtung **20** im Poststrom nachgeschalteten Gerät aufweist. Der DE 197 11 997 ist eine Ausführungsvariante für die Peripherieschnittstelle entnehmbar, welche für mehrere Peripheriegeräte (Stationen) geeignet ist. Sie trägt den Titel: Anordnung zur Kommunikation zwischen einer Basisstation und weiteren Stationen einer Postbearbeitungsmaschine und zu deren Notabschaltung.

**[0037]** Die Schnittstellenschaltung **96** gekoppelt mit der in der Maschinenbasis befindlichen Schnittstellenschaltung **14** stellt mindestens eine Verbindung zu den Sensoren **6**, **7**, **17** und zu den Aktoren, beispielsweise zum Antriebsmotor **15** für die Walze **11** und zu einer Reinigungs- und Dichtstation RDS **40** für den Tintenstrahldruckkopf **4**, sowie zum Labelgeber **50** in der Maschinenbasis her. Die prinzipielle Anordnung und das Zusammenspiel zwischen Tintenstrahldruckkopf **4** und der RDS **40** sind der DE 197 26 642 C2 entnehmbar, mit dem Titel: Anordnung zur Positionierung eines Tintenstrahldruckkopfes und einer Reinigungs- und Dichtvorrichtung.

**[0038]** Einer der in der Führungsplatte **20** angeordneten Sensoren **7**, **17** ist der Sensor **17** und dient zur Vorbereitung der Druckauslösung beim Brieftransport. Der Sensor **7** dient zur Briefanfangserkennung zwecks Druckauslösung beim Brieftransport. Die Transporteinrichtung besteht aus einem Transportband **10** und zwei Walzen **11**, **11'**. Eine der Walzen ist die mit einem Motor **15** ausgestattete Antriebswalze **11**, eine andere ist die mitlaufende Spannwalze **11'**. Vorzugsweise ist die Antriebswalze **11** als Zahnwalze ausgeführt, entsprechend ist auch das Transportband **10** als Zahnriemen ausgeführt, was die eindeutige Kraftübertragung sichert. Ein Encoder **5**, **6** ist mit einer der Walzen **11**, **11'** gekoppelt. Vorzugsweise sitzt die Antriebswalze **11** mit einem Inkrementalgeber **5** fest auf einer Achse. Der Inkrementalgeber **5** ist beispielsweise als Schlitzscheibe ausgeführt, die mit einer Lichtschranke **6** zusammen wirkt, und gibt über die Leitung **19** ein Encodersignal an das Motherboard **9** ab.

**[0039]** Es ist vorgesehen, daß die einzelnen Druckelemente des Druckkopfes innerhalb seines Gehäuses mit einer Druckkopfelektronik verbunden sind und daß der Druckkopf für einen rein elektronischen Druck ansteuerbar ist. Die Drucksteuerung erfolgt auf Basis der Wegsteuerung, wobei der gewählte Stempelversatz berücksichtigt wird, welcher per Tastatur **88** oder bei Bedarf per Chipkarte eingegeben und im Speicher NVM **94** nichtflüchtig gespeichert wird. Ein geplanter Abdruck ergibt sich somit aus Stempelversatz (ohne Drucken), dem Frankierdruckbild und gegebenfalls weiteren Druckbildern für Werbeklischee, Versandinformationen (Wahldrucke) und zusätzlichen editierbaren Mitteilungen. Der nichtflüchtige Speicher NVM **94** weist eine Vielzahl an Speicherbereichen auf. Darunter sind solche, welche die geladenen Portogebührentabellen nichtflüchtig spei-

chern.

**[0040]** Die Chipkarten-Schreib/Leseeinheit **70** besteht aus einem zugehörigen mechanischen Träger für die Mikroprozessorkarte und Kontaktiereinheit **74**. Letztere gestattet eine sichere mechanische Halterung der Chipkarte in Lese-Position und eindeutige Signalisierung des Erreichens der Leseposition der Chipkarte in der Kontaktierungseinheit. Die Mikroprozessorkarte mit dem Mikroprozessor **75** besitzt eine einprogrammierte Lesefähigkeit für alle Arten von Speicherkarten bzw. Chipkarten. Das Interface zur Frankiermaschine ist eine serielle Schnittstelle gemäß RS232-Standard. Die Datenübertragungsrate beträgt min. 1,2 K Baud. Das Einschalten der Stromversorgung erfolgt mittels einem an der Hauptplatine angeschlossenen Schalter **71**. Nach Einschalten der Stromversorgung erfolgt eine Selbsttestfunktion mit Bereitschaftsmeldung.

**[0041]** In der Fig. 3 ist eine perspektivische Ansicht der Frankiermaschine von hinten dargestellt. Die Frankiermaschine besteht aus einem Meter **1** und einer Base **2**. Letztere ist mit einer Chipkarten-Schreib/Leseeinheit **70** ausgestattet, die hinter der Führungsplatte **20** angeordnet und von der Gehäuseoberkante **22** zugänglich ist. Nach dem Einschalten der Frankiermaschine mittels dem Schalter **71** wird eine Chipkarte **49** von oben nach unten in den Einsteckschlitz **72** eingesteckt. Ein zugeführter auf der Kante stehender Brief **3**, der mit seiner zu bedruckenden Oberfläche an der Führungsplatte anliegt, wird dann entsprechend der Eingabedaten mit einem Sicherheitabdruck **31** bedruckt. Die Briefzuführöffnung wird durch eine Klarsichtplatte **21** und die Führungsplatte **20** seitlich begrenzt. Die Statusanzeige des auf die Hauptplatine **9** des Meters **1** gesteckten Sicherheitsmoduls **100** ist von außen durch eine Öffnung **109** sichtbar.

**[0042]** Die Fig. 4 zeigt eine Darstellung eines Sicherheitsabdrucks, wie er von der amerikanischen USPS gefordert wird. Der Sicherheitsabdruck ist rechts vom Werbeklischee angeordnet und weist in der oberen Hälfte ein Beförderer-Logo und den Portowert und in der unteren Hälfte das Datum, den Portowert, einen Key-Indicator und einen Datenauthentisierungscode DAC in einer ersten Zeile und eine Hersteller-ID, eine Maschinen-ID, eine Modell-ID und den Ascendungregisterwert in einer zweiten Zeile auf, wobei beide Zeilen maschinenlesbar sind. Beide maschinenlesbare Zeilen sind durch Markierungsbalken seitlich begrenzt, welche die Erkennung und Auswertung der Zeichen nach dem OCR-Verfahren verbessern. Ein entsprechendes Auswerteverfahren für die vorgenannten Daten, die die Zeichen wiedergeben, wurde bereits in der europäischen Anmeldung EP 862 143 A2 zur Überprüfung eines Sicherheitsabdruckes vorgeschlagen.

**[0043]** Erfindungsgemäß wird die Berechnung des DAC für den Sicherheitsabdruck im Sicherheitsmodul durchgeführt. Eine weitere Beschleunigung der Berechnung des Sicherheitscodes wird durch die Wahl eines eigens für die DES-Berechnung gewählten und zertifizierten Assembler-Algorithmus erziehlt.

**[0044]** Um auch Druckdaten, die lediglich Teile eines Datums angeben, durch eine OCR-Lesestation authentifizieren zu können, wird für diese speziellen Datums-Werte ein Left out-Wert definiert. Dieser wird anstelle des Datumeintrages verwendet. Beispielsweise wird der Wert 0 verwendet, wenn die entsprechende Datumsteile nicht vorliegen.

**[0045]** Um das Druckdatum auf Gültigkeit zu prüfen, ist die Speicherung des aktuellen Datums in zwei unterschiedlichen Formaten und Speicherplätzen notwendig, da das Format der SM-internen Echtzeituhr RTC sich vom Format des im Druckbild verwendeten Datums unterscheidet und ein Vergleich zum Zeitpunkt der Abrechnung entsprechend Zeit benötigt.

**[0046]** Der Aufbau und die Interpretation der Systemdaten, die in den Sicherheitscode eingehen, sowie die Systemdaten, die von der FM für den Druck genutzt werden ermöglicht eine weitere Beschleunigung.

**[0047]** Da bei Massenfrankierungen das Druckdatum in der Regel konstant bleibt, lassen sich die ersten 8 Bytes des Sicherheitscodes in einer ersten 3DES-Runde für jeden Tag vorabrechnen.

**[0048]** In der Tafel 1 wird ein weiteres Beispiel für die Daten aus einem Sicherheitsabdruck hervorgehen gezeigt.

Tafel 1:

| # | Information | | Value range | | Left out | Leading zeroes |
|---|---|---|---|---|---|---|
| 1. | | | **Lower** | **Upper** | | |
| 2. | Date of mailing | Month: | JAN | DEC | '---' | |
| 3. | | Day: | 01 | 31 | '--' | YES |
| 4. | | Year: | 1999 | | '----' | |
| 5. | Postage | | 00000 | 99999 | | YES |
| 6. | Key-Indicator | | 0 | 9 | | |
| 7. | Data Authentication Code | | 00000 | 65535 | | YES |
| 8. | Vendor ID | | FP | | | |
| 9. | Machine ID | | 0000001 | 9999999 | | YES |
| 10. | Model ID | | JMB01 | JMB99 | | |
| 11. | Ascending Register | | 00000000 | FFFFFFFF | | YES |

**[0049]** Die Tafel 2 verdeutlicht Systemdaten die in den Sicherheitscode eingehen und gibt die Länge der benötigten Bytes an und Tafel 3 zeigt ein Beispiel.

Tafel 2:

| | **Element** | **Byte-Länge** | **Wertebereich (dezimal)** |
|---|---|---|---|
| 1. | Maschinen- ID | 4 | 7 digit –Wertebereich für Francotyp-Postalia |
| 2. | OCR Key Indicator | 1 | 0..9 |
| 3. | Postdatum<br>Subelemente:<br>Jahr<br>Monat<br>Tag | Total: 3<br>Detail:<br>1<br>1<br>1 | <br><br>0..99 ,<br>0..12 ,<br>0..31 , |
| 4. | Portowert | 4 | 0..99999 (unit is 1/10 cents) |
| 5. | Ascending Register | 4 | 0..4294967295 (unit is 1/10 cents) |
| | **TOTAL:** | **16** | |

Tafel 3: Beispiel für den Aufbau eines Sicherheitscodes

| | Serien-Nummer | | | | KI | Postdatum | | | Portowert | | | | Ascending Register | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dezimale Daten | 0050010 | | | | 1 | Feb 17 1999 | | | $12.300 | | | | $129.300 | | | |
| Hex. Daten | 00 | 00 | C3 | 5A | 01 | 63 | 02 | 11 | 00 | 00 | 30 | 0C | 00 | 1F | 91 | 14 |

**[0050]** Die Fig. 5 zeigt ein Blockschaltbild des postalischen Sicherheitsmoduls PSM **100** in einer bevorzugten Variante. Der negative Pol der Batterie **134** ist auf Masse und einen Pin P23 der Kontaktgruppe **102** gelegt. Der positive Pol der Batterie **134** ist über die Leitung **193** mit dem einen Eingang des Spannungsumschalters **180** und die Systemspannung führende Leitung **191** ist mit dem anderen Eingang des Spannungsumschalters **180** verbunden. Als Batterie **134** eignet sich der Typ SL-389/P für eine Lebensdauer bis zu 3,5 Jahren oder der Typ SL-386/P für eine Lebensdauer bis zu 6 Jahren bei einem maximalen Stromverbrauch durch das PSM **100**. Als Spannungsumschalter **180** kann ein handelsüblicher Schaltkreis vom Typ ADM 8693ARN eingesetzt werden. Der Ausgang des Spannungsumschalters **180** liegt über die Leitung **136** an der Batterieüberwachungseinheit **12** und der Detektionseinheit **13** an. Die Batterieüberwachungseinheit **12** und die Detektionseinheit **13** stehen mit den Pins1, 2, 4 und 5 des Prozessors **120** über die Leitungen **135**, **164** und **137**, **139** in Kommunikationsverbindung. Der Ausgang des Spannungsumschalters **180** liegt über die Leitung **136** außerdem am Versorgungseingang eines ersten Speichers SRAM **116** an, der durch die vorhandene Batterie **134** zum nichtflüchtigen Speicher NVRAM einer ersten Technologie wird.

**[0051]** Das Sicherheitsmodul steht mit der Frankiermaschine über den Systembus **115**, **117**, **118** in Verbindung. Der Prozessor **120** kann über den Systembus und ein Modem **83** in Kommunikationsverbindung mit einer entfernten Datenzentrale eintreten. Die Abrechnung wird vom ASIC **150** vollzogen. Die postalischen Abrechnungsdaten werden in nichtflüchtigen Speichern unterschiedlicher Technologie gespeichert.

**[0052]** Am Versorgungseingang eines zweiten Speichers NV-RAM **114** liegt Systemspannung an. Hierbei handelt es sich um einen nichtflüchtigen Speicher NVRAM einer zweiten Technologie, (SHADOW-RAM). Diese zweiten Technologie umfaßt vorzugsweise ein RAM und ein EEPROM, wobei letzteres die Dateninhalte bei Systemspannungsausfall automatisch übernimmt. Der NVRAM **114** der zweiten Technologie ist mit den entsprechenden Adress- und Dateneingängen des ASIC's **150** über einen internen Adreß- und Datenbus **112**, **113** verbunden.

**[0053]** Der ASIC **150** enthält mindestens eine Hardware-Abrecheneinheit für die Berechnung der zu speichernden postalischen Daten. In der Programmable Array Logic (PAL) **160** ist eine Zugriffslogik auf den ASIC **150** untergebracht. Der ASIC **150** wird durch die Logik PAL **160** gesteuert. Ein Adreß- und Steuerbus **117**, **115** von der Hauptplatine **9** ist an entsprechenden Pins der Logik PAL **160** angeschlossen und die PAL **160** erzeugt mindestens ein Steuersignal für das ASIC **150** und ein Steuersignal **119** für den Programmspeicher FLASH **128**. Der Prozessor **120** arbeitet ein Programm ab, das im FLASH **128** gespeichert ist. Der Prozessor **120**, FLASH **28**, ASIC **150** und PAL **160** sind über einen modulinternen Systembus miteinander verbunden, der Leitungen **110**, **111**, **126**, **119** für Daten-, Adreß- und Steuersignale enthält.

**[0054]** Die RESET-Einheit **130** ist über die Leitung **131** mit dem Pin 3 des Prozessors **120** und mit einem Pin des ASIC's **150** verbunden. Der Prozessor **120** und das ASIC **150** werden bei Absinken der Versorgungsspannung durch eine Resetgenerierung in der RESET-Einheit **130** zurückgesetzt.

**[0055]** An den Pins 6 und 7 des Prozessors **120** sind Leitungen angeschlossen, welche nur bei einem an die Hauptplatine **9** gesteckten PSM **100** eine Leiterschleife **18** bilden.

**[0056]** Der Prozessor **120** weist intern eine Verarbeitungseinheit CPU **121**, eine Echtzeituhr RTC **122** eine RAM-Einheit **124** und eine Ein/Ausgabe-Einheit **125** auf. An den Pins 8 und 9 liegen I/O-Ports der Ein/Ausgabe-Einheit **125**, an welchen modulinterne Signalmittel angeschlossen sind, beispielsweise farbige Lichtemitterdioden LED's **107**, **108**, welche den Zustand des Sicherheitsmoduls **100** signalisieren. Die Sicherheitsmodule können in ihrem Lebenszyklus verschiedene Zustände einnehmen. So muß z.B. detektiert werden, ob das Modul gültige kryptografische Schlüssel enthält. Weiterhin ist es auch wichtig zu unterscheiden, ob das Modul funktioniert oder defekt ist. Die genaue Art und Anzahl der Modulzustände ist von den realisierten Funktionen im Modul und von der Implementierung abhängig.

**[0057]** Der Prozessor **120** des Sicherheitsmoduls **100** ist über einen modulinternen Datenbus **126** mit einem FLASH **128** und mit dem ASIC **150** verbunden. Der FLASH **128** dient als Programmspeicher und wird mit Systemspannung Us+ versorgt. Er ist beispielsweise ein 128 Kbyte-FLASH-Speicher vom Typ AM29F010-45EC. Der ASIC **150** des postalischen Sicherheitsmoduls **100** liefert über einen modulinternen Adreßbus **110** die Adressen 0 bis 7 an die entsprechenden Adreßeingänge des FLASH **128**. Der Prozessor **120** des Sicherheitsmoduls **100** liefert über einen internen Adreßbus **111** die Adressen 8 bis 15 an die entsprechenden Adresseingänge des FLASH **128**. Der ASIC **150** des Sicherheitsmoduls **100** steht über die Kontaktgruppe **101** des Interfaces **8** mit dem Datenbus **118**, mit dem Adreßbus **117** und dem Steuerbus **115** der Hauptplatine **9** in Kommunikationsverbindung.

**[0058]** Die Echtzeituhr RTC **122** und der Speicher RAM **124** werden von einer Betriebsspannung über die Leitung **138** versorgt. Diese Spannung wird von der Spannungsüberwachungseinheit (Battery Observer) **12** erzeugt. Letzterer liefert außerdem ein Statussignal **164** und reagiert auf ein Steuersignal **135**. Der Spannungsumschalter **180** gibt als Ausgangsspannung auf der Leitung **136** für die Spannungsüberwachungseinheit **12** und Speicher **116** diejenige seiner Eingangsspannungen weiter, die größer als die andere ist. Durch die Möglichkeit, die beschriebene Schaltung in Abhängigkeit von der Höhe der Spannungen Us+ und Ub+ automatisch mit der größeren von beiden zu speisen, kann während des Normalbetriebs die Batterie **134** ohne Datenverlust gewechselt werden.

**[0059]** Die Batterie der Frankiermaschine speist in den Ruhezeiten außerhalb des Normalbetriebes in vorerwähnter Weise die Echtzeituhr **122** mit Datums und/oder Uhrzeitregistern und/oder den statischen RAM (SRAM) **124**, der sicherheitsrelevante Daten hält. Sinkt die Spannung der Batterie während des Batteriebetriebs unter eine bestimmte Grenze, so wird von der im Ausführungsbeispiel beschriebenen Schaltung der

Speisepunkt für RTC und SRAM mit Masse verbunden. D.h. die Spannung an der RTC und am SRAM liegt dann bei 0 V. Das führt dazu, daß der SRAM **124**, der z.B. wichtige kryptografische Schlüssel enthält, sehr schnell gelöscht wird. Gleichzeitig werden auch die Register der RTC **122** gelöscht und die aktuelle Uhrzeit und das aktuelle Datum gehen verloren. Durch diese Aktion wird verhindert, daß ein möglicher Angreifer durch Manipulation der Batteriespannung die frankiermaschineninterne Uhr **122** anhält, ohne daß sicherheitsrelevante Daten verloren gehen. Somit wird verhindert, daß er Sicherheitsmaßnahmen, wie beispielsweise Long Time Watchdogs umgeht.

**[0060]** Gleichzeitig mit der Indikation der Unterspannung der Batterie wechselt die beschriebene Schaltung in einen Selbsthaltezustand, in dem sie auch bei nachträglicher Erhöhung der Spannung bleibt. Beim nächsten Einschalten des Moduls kann der Prozessor den Zustand der Schaltung abfragen (Statussignal) und damit und/oder über die Auswertung der Inhalte des gelöschten Speichers darauf schließen, daß die Batteriespannung zwischenzeitlich einen bestimmten Wert unterschritten hat. Der Prozessor kann die Überwachungsschaltung zurücksetzen, d.h. "scharf" machen.

**[0061]** Weitere Maßnahmen zum Schutz eines Sicherheitsmoduls vor einem Angriff auf die in ihm gespeicherten Daten wurden auch in den nicht vorveröffentlichten deutschen Anmeldungen 198 16 572.2 8 mit dem Titel: Anordnung für ein Sicherheitsmodul und 198 16 571.4 mit dem Titel: Anordnung für den Zugriffsschutz für Sicherheitsmodule, sowie 199 12 780. 8 mit dem Titel: Anordnung für ein Sicherheitsmodul, 199 12 781.6 mit dem Titel: Verfahren zum Schutz eines Sicherheitsmoduls und Anordnung zur Durchführung des Verfahrens und die deutsche Gebrauchsmusteranmeldung 299 05 219.2 mit dem Titel: Sicherheitsmodul mit Statussignalisierung vorgeschlagen. Ein steckbares Sicherheitsmodul kann in seinem Lebenszyklus verschiedene Zustände einnehmen. Es kann nun unterschieden werden, ob das Sicherheitsmodul funktioniert oder defekt ist. Dabei wird auf die Nichtmanipulierbarkeit der hardwaremäßigen Abrechnung vertraut, ohne dies noch einmal zu kontrollieren. Jede andere softwaregesteuerte Arbeitsweise gilt nur mit den Orginalprogrammen als fehlerfrei, welche deshalb vor einer Manipulation geschützt werden müssen.

**[0062]** Die erste Datenverarbeitungseinheit **120** ist erfindungsgemäß durch ein im Programmspeicher **128** des Sicherheitsmoduls gespeichertes Programm programmiert, den Datenauthorisierungscode DAC vorauszuberechnen und an die separate Datenverarbeitungseinheit µP, **91** zu übermitteln, die parallel und annähernd zeitgleich zur Operation der Vorausberechnung durch ein Programm in ihrem Programmspeicher **92** zu einer Druckdatenaufbereitung und zur Berechnung eines Druckbildes programmiert ist. Es ist vorgesehen, daß die erste Datenverarbeitungseinheit **120** des Sicherheitsmoduls **100** einen internen nichtflüchtigen Speicher **124** aufweist, in welchem mindestens ein Schlüssel für die Berechnung des Datenauthorisierungscodes (DAC) vor einem Zugriff geschützt gespeichert ist. Im Sicherheitsmodul **100** ist eine zweite Datenverarbeitungseinheit **150** für eine Abrechnung der Postregister vorgesehen, so daß die vom Sicherheitsmodul **100** separate Datenverarbeitungseinheit im Meter eine dritte Datenverarbeitungseinheit µP, **91** insbesondere für die Bearbeitung der Druckaufgaben bildet.

**[0063]** In der zweiten Datenverarbeitungseinheit ASIC **150** ist eine Hardwareabrechnungseinheit zur Durchführung der Abrechnung enthalten, welche den neuen Postregistersatz mit den Abrechnungsdaten in den nichtflüchtigen Speicher **114**, **116** einspeichert.

**[0064]** Die erste Datenverarbeitungseinheit ist ein Modulprozessor **120** des Sicherheitsmoduls, welcher vorzugsweise programmiert ist, die ersten 8 Bytes des Datenauthorisierungscode (DAC) nach einem Algorithmus in einer ersten Runde für jeden Tag vorauszuberechnen. Der Algorithmus für den Datenauthorisierungscode (DAC) schließt einen DES-Algorithmus, insbesondere einen Tripel-DES-Algorithmus (3DES) ein.

**[0065]** Der Modulprozessor **120** des Sicherheitsmoduls ist programmiert, bei Einzelpostverarbeitung nach Eingabe eines Portowertes den Datenauthorisierungscode (DAC) vorauszuberechnen bzw. bei Massenpostverarbeitung nach Abrechnung des vorhergehenden Portowertes den nächstfolgenden Datenauthorisierungscode (DAC) vorauszuberechnen, wenn der Portowert nicht geändert wird und nach Vorausberechnung den Datenauthorisierungscode (DAC) an die dritte Datenverarbeitungseinheit µP, **91** sofort zu übermitteln.

**[0066]** Der interne nichtflüchtigen Speicher **124** ist ein durch eine Batterie **134** gestützter SRAM-Speicher des Modulprozessors **120** und ist mit Bereichen zur geschützten Speicherung von mindestens einen Teil der Daten eines Postregistersatzes ausgebildet, welcher bei einer Vorausabrechnung entsteht. In einem der Speicherbereiche ist der für die Berechnung eines Datenauthorisierungscodes (DAC) erforderliche mindestens eine Schlüssel geschützt gespeichert.

**[0067]** Der Modulprozessor **120** des Sicherheitsmoduls **100** ist programmiert, mit dem Portowert den steigenden Registerwert R2 (ascending register) im Voraus zu bestimmen und unter Einbeziehung des ermittelten Wertes den Datenauthorisierungscode (DAC) für die Daten des Sicherheitsabdruckes vorauszuberechnen. Beispielsweise unter Einbeziehung folgender Daten des Sicherheitsabdruckes kann der Datenauthorisierungscode (DAC) vorausberechnet werden: Maschinen-Identifikation, OCR-Key-Indikator, Datum, Postwert und Registerwertes R2 für das steigende Register, der bei der Vorausabrechnung ermittelt wurde.

**[0068]** Das Verfahren zur Generierung eines Sicherheitsabdruckes besteht im Wesentlichen in den Schritten:
- Vorausberechnung des aufsteigenden Registerwertes R2,
- Vorausberechnung des Datenauthorisierungscodes,
- Übermittlung des Datenauthorisierungscodes an eine separate Datenverarbeitungseinheit µP, **91**, welche ausgebildet ist, die Druckdaten extern des Sicherheitsmoduls **100** aufzubereiten, daß Druckbild zu berechnen und auszudrucken.

**[0069]** Anhand des – in der Fig. 6 dargestellten – Flußdiagramms werden nun die Routinen näher erläutert, welche im System vor dem Frankieren ablaufen. Der Mikroprozessor CPU **121** ist durch ein entsprechendes im Flash **128** gespeichertes Programm programmiert, solche vorgenannten Selbsttests auszuführen, wobei nach dem Start **299**, in einem ersten Schritt **300** ein Power on-Selbsttest durchgeführt und dann im Schritt **301** gefragt wird, ob der Power on-Selbsttest ein OK ergeben hat. Ist das der Fall, so wird im Schritt **302** die grüne LED **107** vom Mikroprozessor CPU **121** über ein I/O-Port **125** leuchtend gesteuert. Anderenfalls wird im Schritt **303** die rote LED **108** vom Mikroprozessor CPU **121** über ein I/O-Port **125** leuchtend gesteuert.

**[0070]** Vom Schritt **302** wird auf die Abfrage **304** verzweigt, in welcher geprüft wird, ob eine weitere statische Prüfung verlangt wird. Ist das der Fall, so wird zum Schritt **300** zurückverzweigt. Anderenfalls wird auf die Abfrage **305** verzweigt, in welcher geprüft wird, ob durch einen Briefsensor eine Briefanlage festgestellt bzw. vom Modulprozessor **120** eine Eingabe einen neuen Portowertes erkannt wird. Ist dies beides nicht der Fall, dann wird auf den Schritt **302** zurückverzweigt und somit eine Warteschleife solange durchlaufen, bis eine Briefanlage/Neueingabe festgestellt worden ist. Im letzteren Fall wird auf den Schritt **306** verzweigt, um das Eingeben der Daten zu beenden. Gleichzeitig oder kurz nach dem Zeitpunkt $t_0$ beginnend, wird ein Schritt **307** zur MAC-Berechnung auf der Grundlage der zum Zeitpunkt $t_0$ verfügbaren Postregisterdaten $P'_{to}$ gestartet. Ein vom Modulprozessor **120** bereits früher gebildeter MAC($P_{to}$) ist zum Zeitpunkt $t_0$ gültig. Die MAC-Berechnung ist zum Zeitpunkt $t_1$ abgeschlossen. Der berechnete MAC($P'_{to}$) wird mit dem alten zum Zeitpunkt $t_0$ gültigen (vom Modulprozessor **120** bereits früher gebildeten) MAC($P_{to}$) zum Zeitpunkt $t_1$ im Schritt **308** verglichen. Bei Nichtübereinstimmung wird zum Schritt **315** verzweigt, um die LED's **107**, **108** orange leuchtend zu steuern. Anderenfalls wird zum Schritt **309** verzweigt. Dort erfolgt zum Zeitpunkt $t_2$ im Modulprozessor **120** eine Vorausberechnung des aufsteigenden Registerwertes $R2_{t2}$ und eine $DAC_{neu}$-Berechnung. Anschließend erfolgt im Schritt **310** eine Vorausberechnung des Postregistersatzes $P_{t2}$ eine $MAC_{neu}$-Bildung, ggf. mit Speicherung im NVRAM_P **124**. Die Vorausberechnung des Datenauthorisierungscodes (DAC) bezieht den aufsteigenden Registenrwert R2 und weitere Daten ab einem Zeitpunkt $t_{i+1}$ ein, der nach dem Dateneingabe-Ende und/oder bei Massenfrankierungen ab Anlage eines weiteren Poststücks und vor der eigentlichen Abrechnung (**312**) liegt. Von den weiteren Daten, die mindestens den Portowert p und das Datum einschließen, kann mindestens die Maschinen-ID und ggf. das Datum in die DAC-Vorausberechnung ab Anlage eines weiteren Poststücks (Zeitpunkt $t_0$) einbezogen werden, wenn es für den jeweiligen zu frankierenden Briefstapel unverändert bleibt. Bis zum Zeitpunkt $t_5$ ist die Generierung im Sicherheitsmodul abgeschlossen.

**[0071]** Zum Zeitpunkt $t_3$, wenn im Schritt **311** die Speicherung des MAC($P_{t2}$) im NVRAM_P von der einen Datenverarbeitungseinheit **120** abgeschlossen worden ist, wird von der anderen Datenverarbeitungseinheit, nämlich von der – in der Fig. 5 gezeigten – Hardware-Abrecheneinheit im ASIC **150** im Schritt **312** eine Berechnung des neuen Postregistersatzes durchgeführt.

**[0072]** In einem abschließenden Schritt **313** erfolgt eine Abspeicherung der Ergebnisse $P'_{t3}$ und MAC($P_{t2}$) im NVRAM_A. In Vorbereitung eines Frankierens können dann noch eine Anzahl von weiteren Schritten seriell oder parallel zu den vorgenannten Schritten durchlaufen werden, die mindestens einen Subschritt zum Generieren eines Sicherheitscodes DAC einschließen und die mit einem Schritt **314** zur Druckdatenbereitstellung zum Frankieren des Briefes abschließen. Letzterer beinhaltet mindestens jedoch das Senden des Sicherheitscodes DAC an den Mikroprozessor **91** des Meters. Anschließend wird zum Schritt **302** zurückverzweigt.

**[0073]** Zum Generieren eines DAC-Sicherheitscodes wird zwar ebenfalls eine prinzipiell gleiche MAC-Bildungsprozedure genutzt, der DAC setzt sich aber aus dem Ascending-Registerwert R2 und aus weiteren Daten zusammen (Maschinen-ID, OCR-Key-Indikator, Datum, Portowert p) und das Generieren erfolgt zu einem

anderem Zeitpunkt $t_{i+1}$ zum Beispiel ab Dateneingabe-Ende. Bei Massenfrankierungen ist im Anschluß der Übermittlung des Datenauthorisierungscodes an die separate Datenverarbeitungseinheit µP **91** vorgesehen, daß vom Modulprozessor **120** der nächstfolgende Datenauthorisierungscode (DAC) vorausberechnet wird.

**[0074]** Der Modulprozessor **120** arbeitet mit dem – in der Fig. 5 gezeigten – Steuerungsprozessor µP **91** des Meters zusammen, wobei letzterer mindestens den Sicherheitscode DAC($R2_{t(i+1)}$, weitere Daten) empfängt, die Druckdaten zusammenstellt und zum Druckkopf übermittelt.

**[0075]** Erdindungsgemäß ist das Sicherheitsmodul zum Einsatz in postalischen Geräten bestimmt, insbesondere zum Einsatz in einer Frankiermaschine. Jedoch kann das Sicherheitsmodul auch eine andere Bauform aufweisen, die es ermöglicht, daß es mit einem Personalcomputer zusammenarbeiten kann, der als dritte Datebverarbeitungseinheit fungiert. Es kann beispielsweise mit die Hauptplatine eines Personalcomputers verbunden werden, der als PC-Frankierer einen handelsüblichen Drucker ansteuert.

## Patentansprüche

1. Anordnung zur Generierung eines Sicherheitsabdruckes, mit einem Sicherheitsmodul, der einen Programmspeicher (**128**), mindestens eine erste Datenverarbeitungseinheit (**120**) und nichtflüchtige Speicher (**114**, **116**) einschließt, wobei die erste Datenverarbeitungseinheit (**120**) zur Generierung eines Sicherheitscodes programmiert ist und mit einer separaten Datenverarbeitungseinheit extern des Sicherheitsmoduls, die durch ein Programm in ihrem Programmspeicher (**92**) zu einer Druckdatenaufbereitung und zur Berechnung eines Druckbildes programmiert ist, das den Sicherheitscode enthält, gekennzeichnet dadurch, dass die erste Datenverarbeitungseinheit (**120**) durch ein Programm im Programmspeicher (**128**) programmiert ist,
– bei jeder Nachricht für neue Systemdaten sofort eine Neuberechnung des Sicherheitscodes zu starten, sofern die neuen Systemdaten vom Sicherheitsmodul als gültig erkannt und für den Sicherheitscode benötigt werden, wobei der Sicherheitscode ein Datenautorisierungscode (DAC) ist,
– die ersten n Bytes des Datenautorisierungscode (DAC) nach einem Algorithmus in einer ersten Runde für jeden Tag vorauszuberechnen, den Registerwert für das steigende Register (R2) mittels des eingegebenen Portowertes in einer weiteren Runde für mindestens ein Poststück vorauszuberechnen und den Datenautorisierungscode (DAC) für mindestens einen Sicherheitsabdruck fertig zu berechnen, sowie
– eine Abrechnung für das zu frankierende mindestens eine Poststück und eine Übermittlung des Datenautorisierungscodes (DAC) an die separate Datenverarbeitungseinheit (µP, **91**) zu veranlassen.

2. Anordnung, nach Anspruch 1, gekennzeichnet dadurch, dass die erste Datenverarbeitungseinheit (**120**) des Sicherheitsmoduls einen internen nichtflüchtigen Speicher (**124**) aufweist, in welchem mindestens ein Schlüssel für die Berechnung des Datenautorisierungscodes (DAC) vor einem Zugriff geschützt gespeichert ist und dass das Sicherheitsmodul eine zweite Datenverarbeitungseinheit (**150**) für eine Abrechnung der Postregister aufweist sowie dass die separate Datenverarbeitungseinheit eine dritte Datenverarbeitungseinheit (µP, **91**) bildet.

3. Anordnung, nach den Ansprüchen 1 bis 2, gekennzeichnet dadurch, dass die erste Datenverarbeitungseinheit ein Modulprozessor (**120**) des Sicherheitsmoduls (**100**) und dass die zweite Datenverarbeitungseinheit (**150**) eine Hardwareabrechnungseinheit zur Durchführung der Abrechnung ist, die den neuen Postregistersatz mit den Abrechnungsdaten in den nichtflüchtigen Speicher (**114**, **116**) einspeichert.

4. Anordnung, nach den Ansprüchen 1 bis 3, gekennzeichnet dadurch, dass der Algorithmus für den Datenautorisierungscode (DAC) einen DES-Algorithmus einschließt.

5. Anordnung, nach den Ansprüchen 1 bis 4, gekennzeichnet dadurch, dass der Algorithmus für den Datenautorisierungscode (DAC) einen Tripel-DES-Algorithmus (3DES) einschließt.

6. Anordnung, nach Anspruch 3, gekennzeichnet dadurch, dass der Modulprozessor (**120**) programmiert ist, bei Massenpostverarbeitung nach Abrechnung des vorhergehenden Portowertes den nächstfolgenden Datenautorisierungscode (DAC) vorauszuberechnen, wenn der Portowert nicht geändert wird und den Datenautorisierungscode (DAC) an die dritte Datenverarbeitungseinheit (µP, **91**) sofort zu übermitteln.

7. Anordnung, nach den Ansprüchen 2 und 3, gekennzeichnet dadurch, dass der interne nichtflüchtigen Speicher (**124**) ein durch eine Batterie (**134**) gestützter SRAM-Speicher des Modulprozessors (**120**) ist und mit Bereichen zur geschützten Speicherung von mindestens einen Teil der Daten eines Postregistersatzes ausgebildet ist, der bei einer Vorausabrechnung entsteht, dass in einem der Speicherbereiche der mindestens eine

Schlüssel für die Berechnung des Datenautorisierungscodes (DAC) geschützt gespeichert ist.

8. Anordnung, nach Anspruch 7, gekennzeichnet dadurch, dass der Modulprozessor (**120**) des Sicherheitsmoduls programmiert ist, unter Einbeziehung einer Maschinen-Identifikation, eines OCR-Schlüssel-Indikators, eines Datums, des Postwertes und eines bei der Vorausabrechnung ermittelten Registerwertes für das steigende Register R2 den Datenautorisierungscode (DAC) vorauszuberechnen.

9. Verfahren zur Generierung eines Sicherheitsabdruckes, mit einer Berechnung eines Sicherheitscode zur Sicherung der Postregister vor Manipulation durch eine erste Datenverarbeitungseinheit und mit einer Abrechnung durch eine zweite Datenverarbeitungseinheit im Sicherheitsmodul, gekennzeichnet durch die Schritte:
– Voreinstellung aller für den Sicherheitscode benötigten Systemdaten, wobei jede Nachricht, die solche Systemdaten verändert, eine Neuberechnung des Sicherheitscodes sofort startet, sofern die neuen Systemdaten vom Sicherheitsmodul als gültig erkannt werden,
– Vorausberechnung des aufsteigenden Registerwertes R2,
– Vorausberechnung eines Datenautorisierungscodes (DAC),
– Übermittlung des Datenautorisierungscodes an eine separate Datenverarbeitungseinheit (µP, **91**), welche ausgebildet ist, die Druckdaten extern des Sicherheitsmoduls (**100**) aufzubereiten, dass Druckbild zu berechnen und auszudrucken.

10. Verfahren, nach Anspruch 9, gekennzeichnet dadurch, dass die Vorausberechnung des Datenautorisierungscodes (DAC), den aufsteigenden Registerwert R2 und weitere Daten einbezieht und dass das Generieren eines Sicherheitsabdruckes zu einem Zeitpunkt $t_{i+1}$ ab Dateneingabe-Ende und/oder bei Massenfrankierungen ab Anlage eines weiteren Poststücks und vor der eigentlichen Abrechnung erfolgt.

11. Verfahren, nach Anspruch 10, gekennzeichnet dadurch, dass die weiteren Daten mindestens die Maschinen-ID, den Portowert p und das Datum einschließen, wobei mindestens die Maschinen-ID und optional das Datum in die Vorausberechnung einbezogen wird, wenn es es für den jeweiligen zu frankierenden Briefstapel unverändert bleibt.

12. Verfahren, nach den Ansprüch 9 bis 11, gekennzeichnet dadurch, dass bei Massenfrankierungen im Anschluß der Übermittlung des Datenautorisierungscodes an die separate Datenverarbeitungseinheit (µP, **91**), vom Modulprozessor (**120**) der nächstfolgende Datenautorisierungscode (DAC) vorauszuberechnet wird.

Es folgen 6 Blatt Zeichnungen

**Anhängende Zeichnungen**

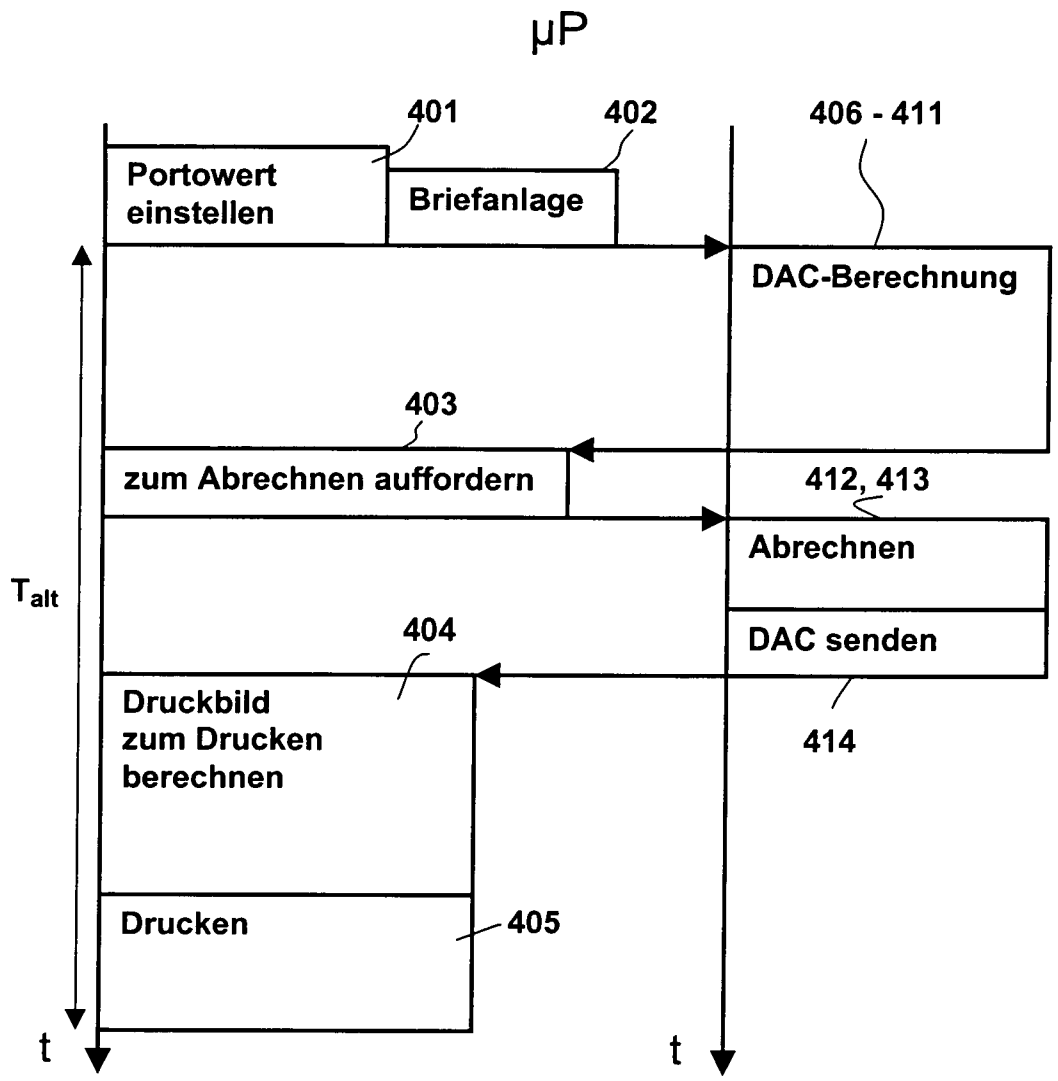



Fig. 1a

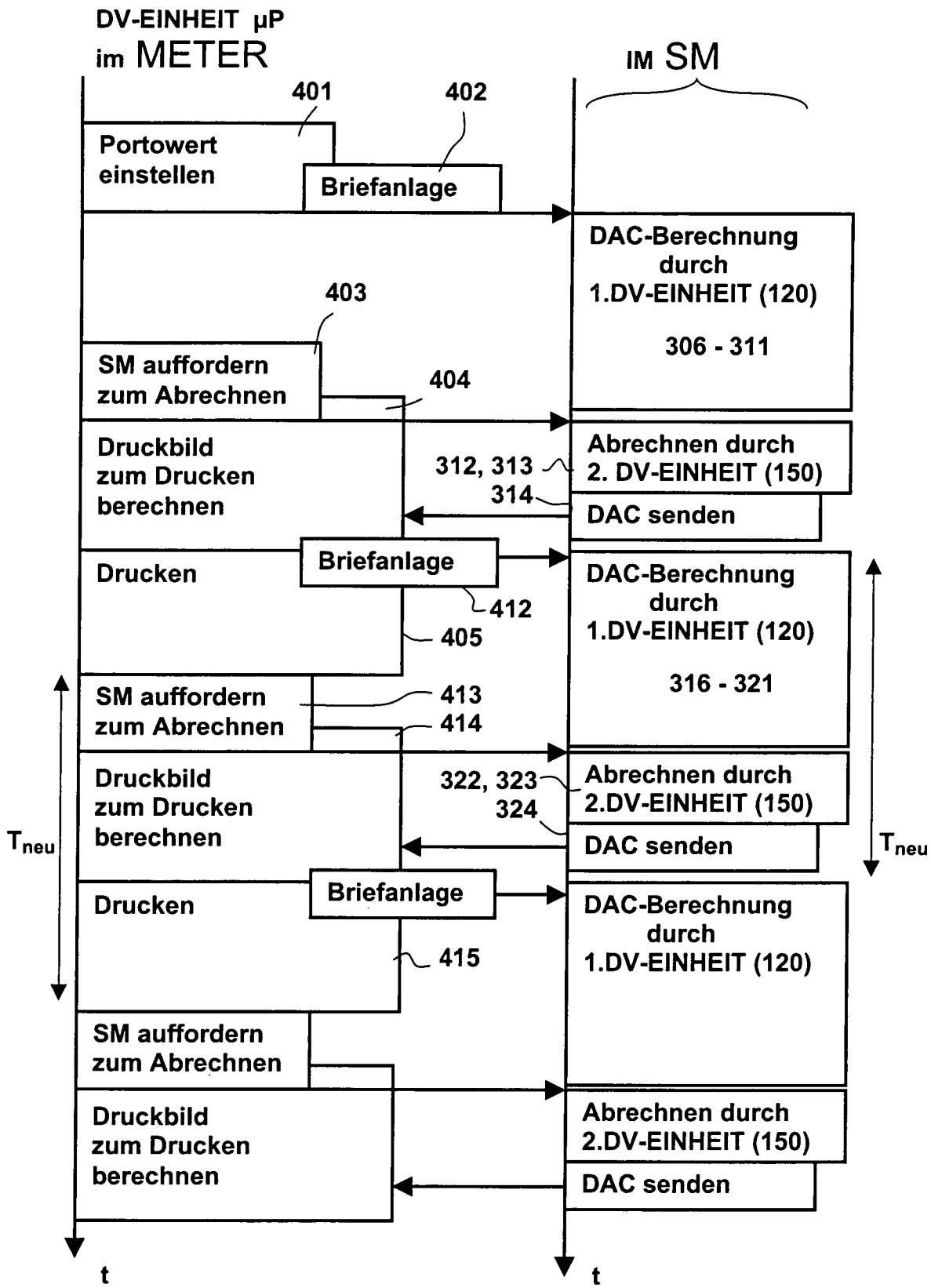

DV-EINHEIT µP
im METER
IM SM
401
402
Portowert einstellen
Briefanlage
DAC-Berechnung durch 1.DV-EINHEIT (120)
306 - 311
403
SM auffordern zum Abrechnen
404
Druckbild zum Drucken berechnen
312, 313
314
Abrechnen durch 2. DV-EINHEIT (150)
DAC senden
Drucken
Briefanlage
412
405
DAC-Berechnung durch 1.DV-EINHEIT (120)
316 - 321
SM auffordern zum Abrechnen
413
414
Druckbild zum Drucken berechnen
322, 323
324
Abrechnen durch 2.DV-EINHEIT (150)
DAC senden
Tneu
Tneu
Drucken
Briefanlage
415
DAC-Berechnung durch 1.DV-EINHEIT (120)
SM auffordern zum Abrechnen
Druckbild zum Drucken berechnen
Abrechnen durch 2.DV-EINHEIT (150)
DAC senden
t
t

Fig. 1b

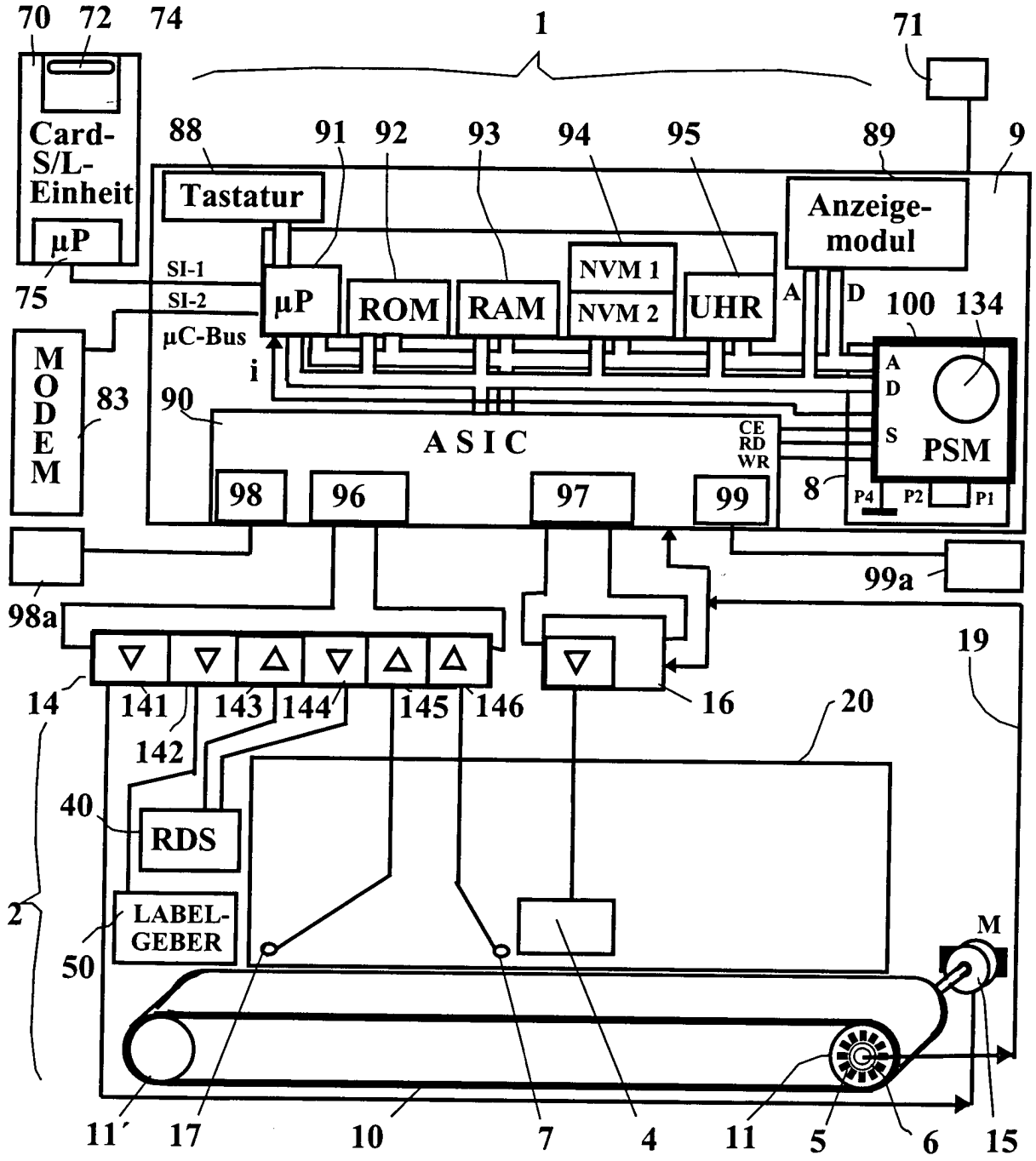

70
72
74
1
71
Card-
S/L-
Einheit
µP
75
88
91
92
93
94
95
89
9
Tastatur
Anzeige-
modul
SI-1
SI-2
µC-Bus
µP
ROM
RAM
NVM 1
NVM 2
UHR
A
D
100
134
MODEM
83
i
90
ASIC
CE
RD
WR
A
D
S
PSM
98
96
97
99
8
P4
P2
P1
98a
99a
19
14
141
142
143
144
145
146
16
20
40
RDS
LABEL-
GEBER
50
2
M
11´
17
10
7
4
11
5
6
15

Fig. 2

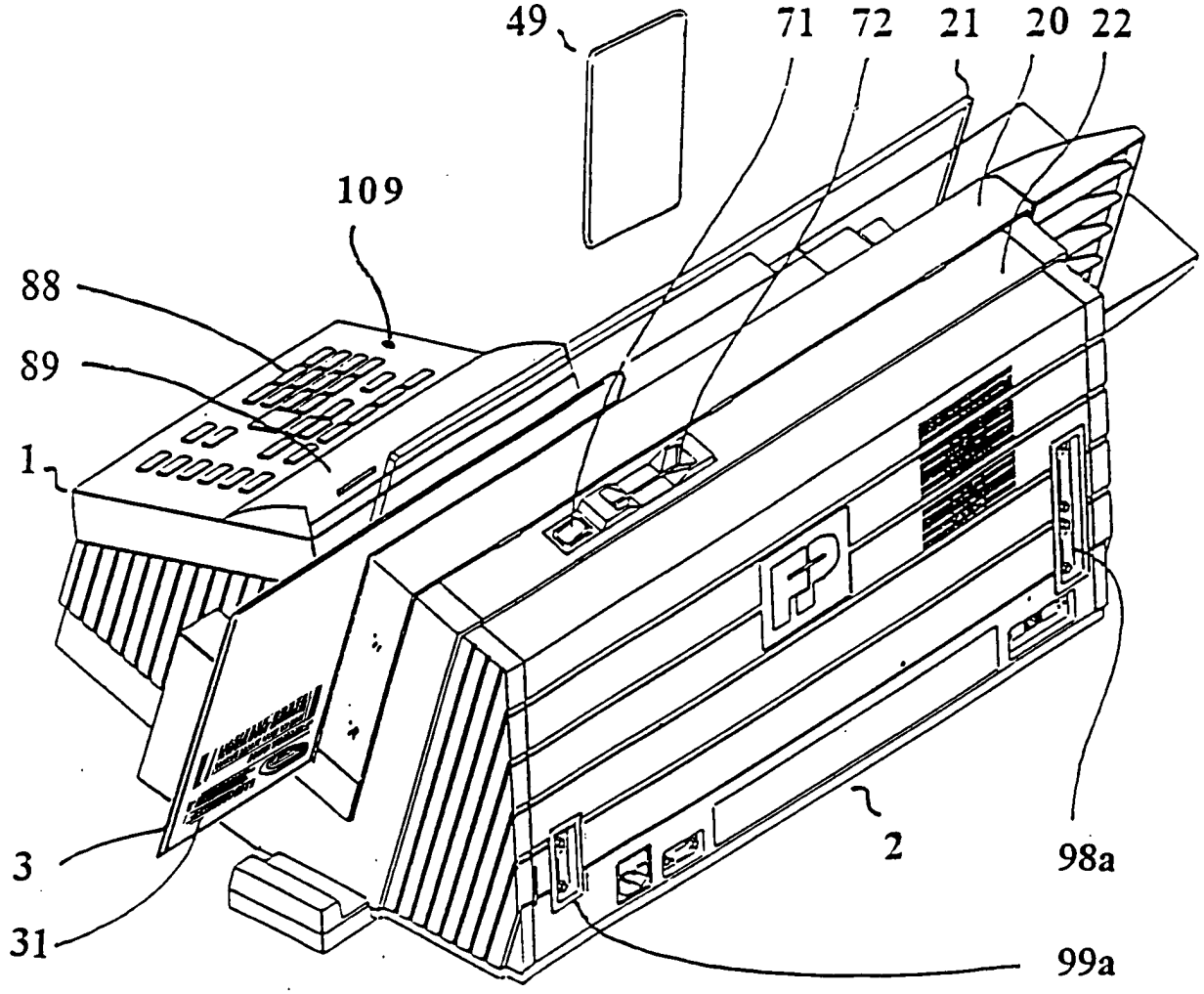

49
71
72
21
20
22
109
88
89
1
3
31
2
98a
99a

Fig. 3

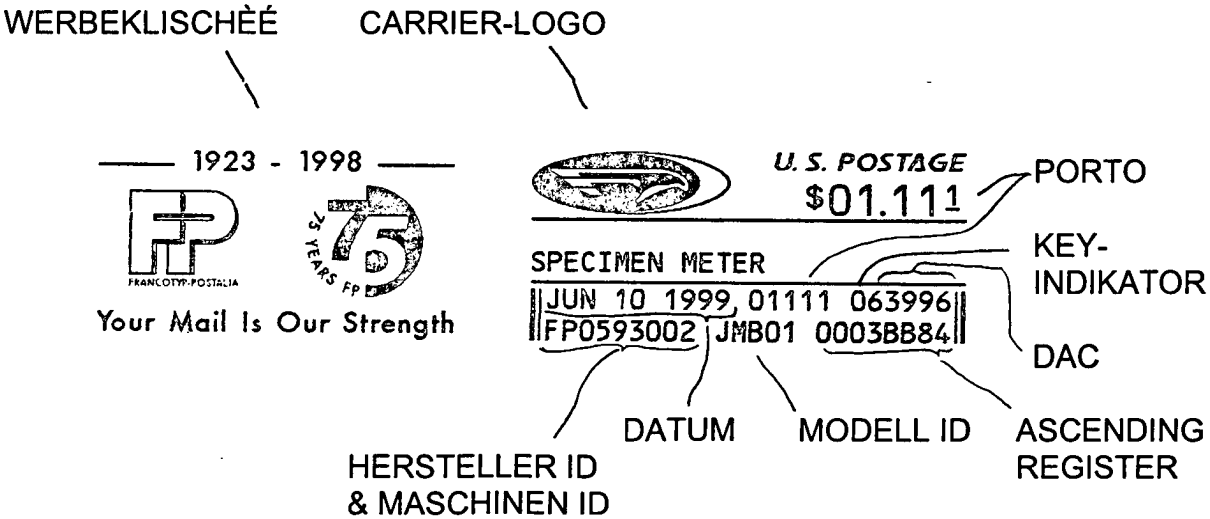

WERBEKLISCHÈÉ
CARRIER-LOGO
1923 - 1998
FRANCOTYP-POSTALIA
75 YEARS FP
Your Mail Is Our Strength
U.S. POSTAGE
$01.111
PORTO
SPECIMEN METER
JUN 10 1999 01111 063996
FP0593002 JMB01 0003BB84
KEY-
INDIKATOR
DAC
DATUM
MODELL ID
ASCENDING
REGISTER
HERSTELLER ID
& MASCHINEN ID

Fig. 4

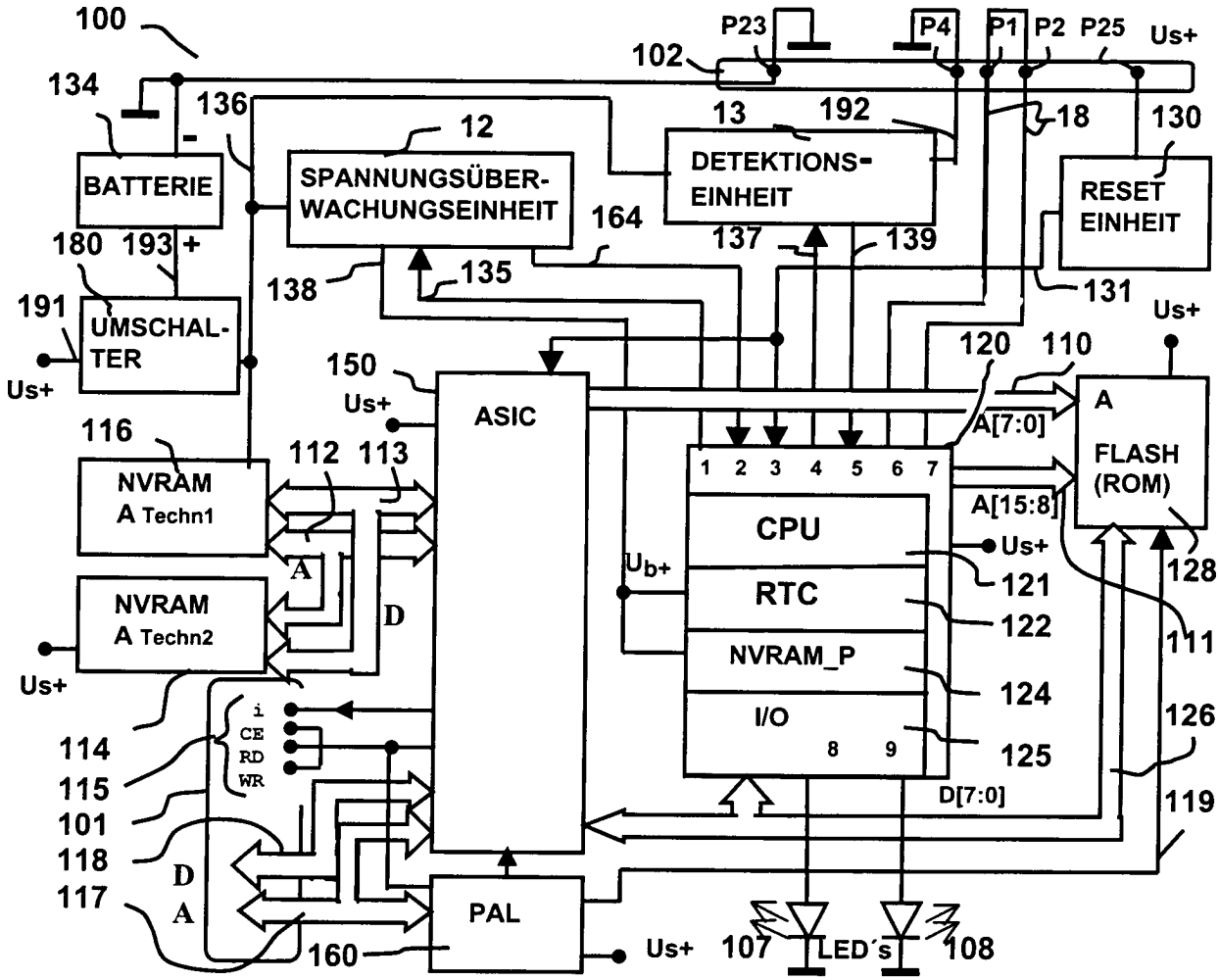

100
102
P23
P4
P1
P2
P25
Us+
134
136
12
13
192
18
130
BATTERIE
SPANNUNGSÜBER-
WACHUNGSEINHEIT
DETEKTIONS-
EINHEIT
RESET
EINHEIT
164
180
193
+
137
139
135
138
131
191
UMSCHAL-
TER
Us+
120
110
150
Us+
ASIC
A
FLASH
(ROM)
A[7:0]
116
112
113
1 2 3 4 5 6 7
NVRAM
A Techn1
A[15:8]
CPU
Us+
128
A
D
Ub+
121
RTC
122
NVRAM
A Techn2
111
NVRAM_P
124
Us+
i
CE
RD
WR
I/O
126
8 9
125
114
115
101
118
117
D[7:0]
119
D
A
PAL
160
Us+
107
LED´s
108

Fig. 5

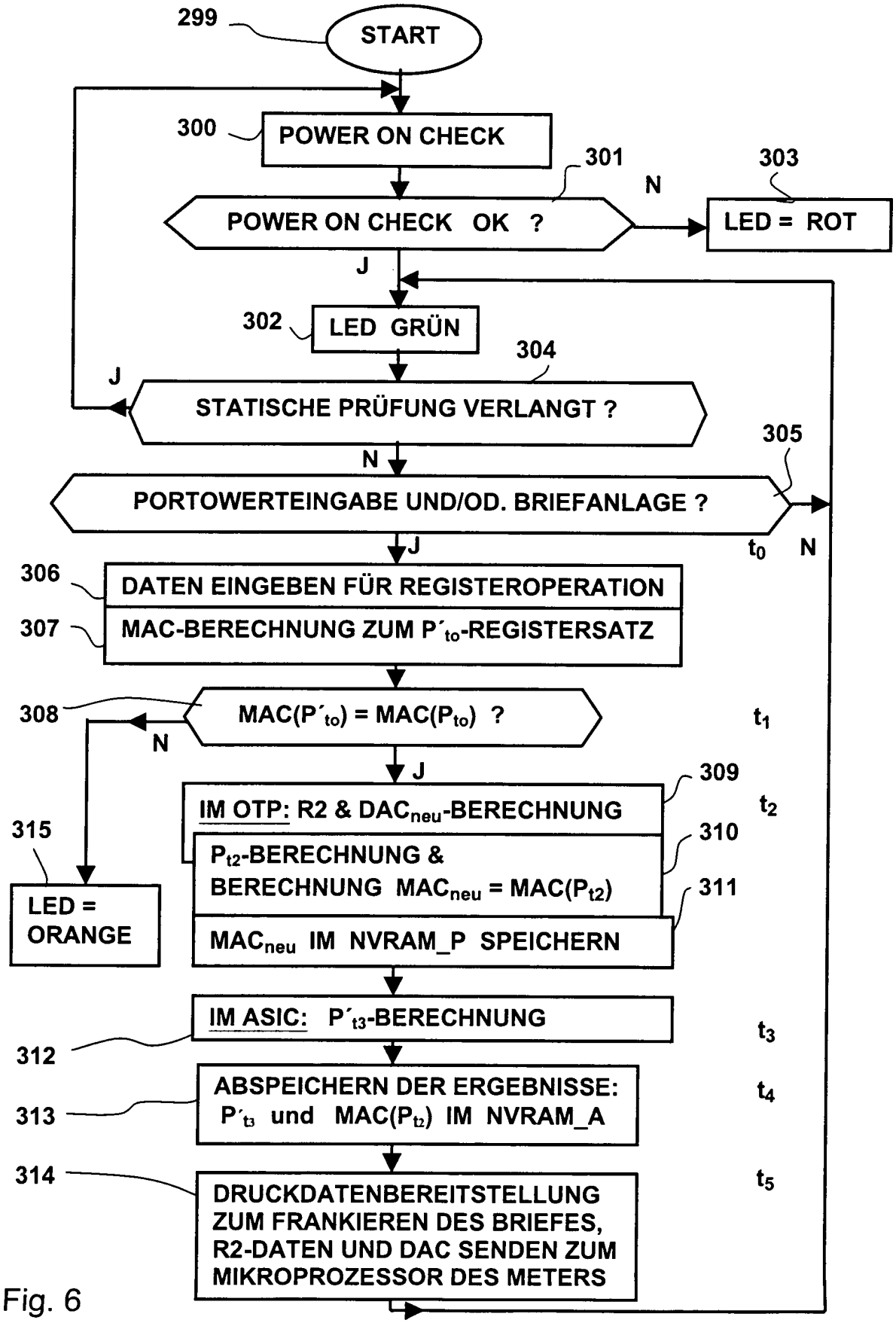

299
START
300
POWER ON CHECK
301
POWER ON CHECK OK ?
N
303
LED = ROT
J
302
LED GRÜN
304
J
STATISCHE PRÜFUNG VERLANGT ?
N
305
PORTOWERTEINGABE UND/OD. BRIEFANLAGE ?
J
$t_0$
N
306
DATEN EINGEBEN FÜR REGISTEROPERATION
307
MAC-BERECHNUNG ZUM P´$_{to}$-REGISTERSATZ
308
MAC(P´$_{to}$) = MAC(P$_{to}$) ?
$t_1$
N
J
309
IM OTP: R2 & DAC$_{neu}$-BERECHNUNG
$t_2$
315
LED = ORANGE
310
P$_{t2}$-BERECHNUNG & BERECHNUNG MAC$_{neu}$ = MAC(P$_{t2}$)
311
MAC$_{neu}$ IM NVRAM_P SPEICHERN
IM ASIC: P´$_{t3}$-BERECHNUNG
$t_3$
312
ABSPEICHERN DER ERGEBNISSE: P´$_{t3}$ und MAC(P$_{t2}$) IM NVRAM_A
$t_4$
313
314
DRUCKDATENBEREITSTELLUNG ZUM FRANKIEREN DES BRIEFES, R2-DATEN UND DAC SENDEN ZUM MIKROPROZESSOR DES METERS
$t_5$

Fig. 6