



(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
05.01.2000 Patentblatt 2000/01

(51) Int. Cl.⁷: G07B 17/00

(21) Anmeldenummer: 99250182.5

(22) Anmeldetag: 11.06.1999

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

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

(72) Erfinder: Reisinger, Frank
16515 Oranienburg (DE)

(30) Priorität: 29.06.1998 DE 19830055

(54) **Verfahren zur sicheren Übertragung von Dienstdaten an ein Endgerät und Anordnung zur Durchführung des Verfahrens**

(57) Das Verfahren zur sicheren Übertragung von Daten an ein Endgerät, insbesondere eine portoberechnende Waage oder Frankiermaschine, umfaßt die Schritte, Bereitstellen (210) von neuen Portotariftabellendaten in der Datenzentrale für eine zukünftige Portoberechnung, Bilden (110) von Anforderungsdaten für Portotariftabellendaten und Kommunikation (120, 220) des Endgerätes mit einer Datenzentrale, um die neuen Portotariftabellendaten von der Datenzentrale anzufordern, zu empfangen und zu speichern sowie einer Kommunikation (130, 230), um eine Information über die gespeicherten Portotariftabellendaten zur Datenzentrale zu übermitteln und dort zu prüfen, bevor ein Senden einer OK-Meldung an das Endgerät erfolgt.

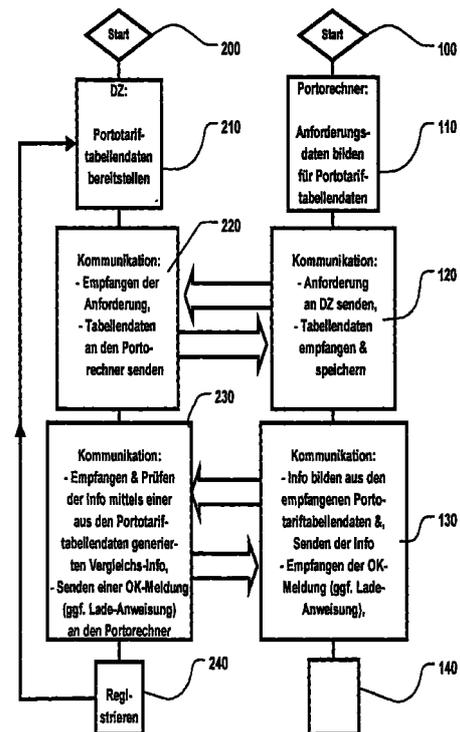


Fig. 2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur sicheren Übertragung von Dienstdaten an ein Endgerät, gemäß des Oberbegriffs der Ansprüche 1 und 18 sowie gemäß des Oberbegriffs des Anspruchs 12 eine Anordnung zur Durchführung des Verfahrens nach Anspruch 1. Die Lösung bezweckt insbesondere die Sicherheit zu liefern, daß die Übertragung und Speicherung von einer neuen Portogebührentabelle in einem Portorechner ordnungsgemäß durchgeführt wird. Das Verfahren ist sowohl für Anwender von Frankiermaschinen vorgesehen, als auch für Portorechnerwaagen geeignet.

[0002] Aus DE 38 23 719 C2 und US 41 38 735 ist bekannt, daß ein Nachladen einer Tariftabelle für Portogebühren von einer entfernten Datenzentrale zu bestimmten Zeitpunkten veranlaßt wird. Wenn der Datenaustausch vom Server der Datenzentrale initiiert wird, muß die Frankiermaschine ständig angeschaltet bleiben, was natürlich nachteilig ist.

[0003] Alternativ wurde im US 5,490,077 bzw. im US 5,606,508 vorgeschlagen, das Datenladen von der Frankiermaschine on demand zu initiieren, wobei nach dem Einschalten der Frankiermaschine der Datenbestand in Abhängigkeit von Bedingungen (wie z.B. Name, Datum) aktualisiert wird. Um rechtzeitig die Mehrheit der Postkunden mit einer Tariftabelle auszustatten, wird letztere weit vor ihrem Inkrafttreten in einem Speicher eines Übertragungsmittels (Chipkarte bzw. Zelle eines GSM-Netzes) separat von der Frankiermaschine gespeichert. Beim Einschalten der Frankiermaschine wird das Datum des Kalenderbausteins der Frankiermaschine verwendet bzw. mit weiteren eingegebenen Bedingungen verknüpft, um die Tabelle auszuwählen, die bei Inbetriebnahme der Frankiermaschine in deren Speicher geladen wird. Beim Laden aus einem Speicher des Übertragungsmittels in den Speicher der Frankiermaschine erfolgt ein Aktualisieren der bisherigen Tabelle.

[0004] Aus dem US 5,710,706 (EP 724 141 A1) ist eine Dateneingabe in eine Waage bekannt, welche mit einer Frankiermaschine schnittstellenmäßig verbunden ist, um Tariftabellendaten mit Daten zu aktualisieren. Das Laden der Daten erfolgt von einer entfernten Datenzentrale per Modem zur Frankiermaschine. Das Laden und Aktualisieren erfolgt unmittelbar aufeinanderfolgend. Wenn eine Information vorliegt, daß Tariftabellendaten zu aktualisieren sind, erfolgt ein Laden und ggf. unter Zwischenspeichern von Tariftabellendaten in der Frankiermaschine und ein sektorweises Löschen der alten Portotabelle im nichtflüchtigen Speicher der Waage vor dem Übertragen der neuen Tariftabellendaten aus dem Zwischenspeicher der Frankiermaschine zur Waage und dem Einschreiben der neuen Tariftabellendaten in den nichtflüchtigen Speicher der Waage. In der Waage können mehrere Tabellen gespeichert sein. Jedoch bezieht sich jede Tabelle auf einen separaten Postbeförderer (Carrier), welcher über Tastatur anwähl-

bar ist. Das Mindestgültigkeitsdatum einer zu einer Carrier-Identifikations-Nummer CIN zugeordneten Tariftabelle wird gespeichert und von der Frankiermaschine ausgewertet, um bei Bedarf Anforderungsdaten zu bilden zum Laden von neuen Tariftabellendaten bzw. zur Aktualisierung im Speicher der Waage entsprechend der CIN.

[0005] Aus der US 5,448,641 ist postalisches Gebührensystem mit Gültigkeitsprüfung im Endgerät auf der Benutzerseite bekannt. Die Portotariftabelle wird von der Datenzentrale zum Endgerät übertragen. Auch ein zur Portotariftabelle zugehöriger Code wird von der Datenzentrale zum Endgerät übertragen. Letzteres generiert einen Vergleichs-Code aus einer Information basierend auf der empfangenen Portotariftabelle. Anhand des Vergleiches des empfangenen Codes mit dem generierten Vergleichs-Code kann im Endgerät die Gültigkeit der empfangenen Portotariftabelle überprüft werden. Damit kann zwar das Endgerät die übermittelte Portotariftabelle verifizierbaren, jedoch kann seitens der Datenzentrale nicht überprüft werden, ob die aktuelle Portotariftabelle vom Endgerät wirklich ordnungsgemäß gespeichert wurde. Im Streitfall könnte der Benutzer die Bezahlung der Dienstleistung verzögern oder verweigern, weil kein Beleg über die im Endgerät erfolgte Speicherung der Portotariftabelle existiert. Dem Frankiermaschinenhersteller bliebe somit eine Inspektion der Maschine vor Ort nicht erspart.

[0006] Es war die Aufgabe zu lösen, die Nachteile des Standes der Technik zu überwinden und eine Anordnung und ein Verfahren zur sicheren Übertragung von Dienstdaten an ein Endgerät zu schaffen, um eine Überprüfung auf ordnungsgemäße Speicherung von Dienstdaten, insbesondere einer übermittelten Portotariftabelle, zu ermöglichen. Die Überprüfung soll automatisch möglichst ohne Zutun des Benutzers des Endgerätes erfolgen. Das Endgerät soll dabei nicht bzw. nicht unnötig lange blockiert werden.

[0007] Die Aufgabe wird mit den Merkmalen des Verfahrens nach den Ansprüchen 1 und 18 sowie mit den Merkmalen der Anordnung nach Anspruch 12 gelöst.

[0008] Die Erfindung geht von dem Bedürfnis einiger Postbeförderer aus, die Dienstdaten, insbesondere die Gebühren in Portotariftabellen, beliebig zu ändern. Die Dienstdaten werden in einem Verarbeitungsmodul im oder beim Endgerät benötigt. Die Dienstdaten schließen insbesondere die Gebühren in Portotariftabellen ein.

[0009] Das Verarbeitungsmodul ist ein elektronischer Portorechner. Beim Endgerät handelt es sich vorzugsweise um eine elektronische Frankiermaschine oder um eine Portorechnerwaage. Es ist vorgesehen, daß das Endgerät mit einem Portorechner verbunden ist und daß der Mikroprozessor das Endgerätes oder des Portorechners programmiert ist, eine Speicherung der neuen Portotariftabellendaten im Speicher des Endgerätes bzw. des Portorechners vorzunehmen und eine Prüfsumme über die gespeicherten neuen Portotarifa-

bellendaten zu bilden und zur Datenzentrale zu übermitteln, sowie eine empfangene (OK-)Meldung auszuführen und das Endgerät oder den Portorechner in einen Betriebsmodus umzuschalten.

[0010] Es ist alternativ vorgesehen, daß der Mikroprozessor des Endgerätes oder des Portorechners programmiert ist, eine Zwischenspeicherung der neuen Portotariftabellendaten im flüchtigen Arbeitsspeicher des Endgerätes bzw. des Portorechners vorzunehmen und eine Prüfsumme über die zwischengespeicherten neuen Portotariftabellendaten zu bilden und zur Datenzentrale zu übermitteln, sowie bei sowie beim Empfang einer OK-Meldung eine Lade-Anweisung der Datenzentrale an das Endgerät auszuführen, die neuen Portotariftabellendaten in einen nichtflüchtigen Speicher eines Portorechners zu laden und dannach das Endgerät oder den Portorechner in einen Betriebsmodus umzuschalten.

[0011] Werden Dienstdaten benötigt, insbesondere eine geänderte Portotariftabelle in einem elektronischen Portorechner, kann folglich eine Ferninstallation erfolgen. Die Postbeförderer beauftragen jeweils eine Datenzentrale mit der Dienstleistung zur Ferninstallation, auf Anforderung Dienstdaten, zum Endgerät zu übermitteln, um diese in entsprechende Speicher des Verarbeitungsmoduls laden zu können. Bei einer solchen Ferninstallation kommt das erfindungsgemäße Verfahren zur sicheren Übertragung von Dienstdaten an ein Endgerät mit folgenden Verfahrensschritten zum Einsatz:

- Bereitstellen von neuen Dienstdaten in der Datenzentrale für eine zukünftige Verarbeitung basierend auf den Dienstdaten,
- Bilden von Anforderungsdaten für Dienstdaten,
- erste Kommunikation des Endgerätes mit einer Datenzentrale, umfassend ein Senden der Anforderungsdaten, um die neuen Dienstdaten von der Datenzentrale anzufordern, und umfassend ein Empfangen und Zwischenspeichern der angeforderten Dienstdaten,
- erste Kommunikation der Datenzentrale mit dem Endgerät, umfassend ein Empfangen der Anforderungsdaten in der Datenzentrale und ein Senden der angeforderten Dienstdaten an das Endgerät,
- zweite Kommunikation des Endgerätes mit einer Datenzentrale, umfassend ein Bilden und Übermittlung einer Information vom Endgerät zur Datenzentrale, welche auf die zwischengespeicherten gültigen neuen Dienstdaten bezogen ist,
- zweite Kommunikation der Datenzentrale mit dem Endgerät, umfassend ein Empfangen und Prüfen der Information in der Datenzentrale mittels einer aus den Dienstdaten generierten Vergleichsinformation und umfassend ein Senden einer Meldung an das Endgerät, wobei in Verbindung mit dem Senden der Meldung in der Datenzentrale ein Registrieren der Dienstleistung erfolgt.

[0012] In vorteilhafter Weise kann die Kommunikation von der Datenzentrale per Modem direkt mit dem Verarbeitungsmodul im Endgerät oder indirekt über das Endgerät mit dem Verarbeitungsmodul erfolgen.

Die zunächst flüchtig zwischengespeicherten gültigen neuen Dienstdaten werden vom Verarbeitungsmodul zu einer Prüfsumme verarbeitet. Dann wird eine Information gebildet, in die die Prüfsumme eingeht. Die Kommunikation des Endgerätes mit einer Datenzentrale, umfaßt während einer zweiten Transaktion ein Bilden und Übermittlung einer Information vom Endgerät zur Datenzentrale. Die zur Datenzentrale übermittelte Information enthält vorzugsweise eine Identifikation des Endgerätes (z.B. eine PIN), eine Versionsnummer und die Prüfsumme über die Dienstdaten oder eine verschlüsselte Prüfsumme bzw. eine Signatur. Damit können in vorteilhafter Weise in der Datenzentrale die im Verarbeitungsmodul bzw. Endgerät (zwischen-)gespeicherten neuen Dienstdaten identifiziert und deren ordnungsgemäße bzw. fehlerfreie (Zwischen-)Speicherung verifiziert werden. Die von der Datenzentrale abschließend gesendete Meldung ist beispielsweise Ladeanweisung, die neuen Dienstdaten in einen nichtflüchtigem Speicher eines Verarbeitungsmoduls zu laden.

[0013] Es ist vorgesehen, daß der Portorechner im Endgerät integriert ist oder separat vom Endgerät angeordnet ist. Das Endgerät ist vorzugsweise eine Frankiermaschine, wobei ein symmetrischer Verschlüsselungs-Algorithmus zur Bildung einer verschlüsselten Prüfsumme und ein geheimer Schlüssel in der Frankiermaschine sicher gespeichert vorliegen.

[0014] Alternativ ist der Portorechner in eine Waage integriert. Es ist vorgesehen, daß ein unsymmetrischer Verschlüsselungs-Algorithmus zur Bildung einer verschlüsselte Prüfsumme und ein öffentlicher Schlüssel in der Waage gespeichert ist, wobei der öffentliche Schlüssel ungesichert gespeichert vorliegt.

[0015] 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:

- | | | |
|----|--------------|--|
| 45 | Figur 1a, | Blockschaltbild einer Frankiermaschine mit Portorechner, |
| | Figur 1b, | Blockschaltbild der Frankiermaschine für eine OTP-Variante, |
| 50 | Figur 1c, | Blockschaltbild einer Frankiermaschine mit einer Portorechner-Waage, |
| | Figur 2, | Flußplan für die sichere Übertragung von Daten. |
| 55 | Figur 3a, b, | Flußpläne für die Überprüfung der sicheren Übertragung von Daten. |

[0016] Die Figur 1a zeigt ein Blockschaltbild der erfindungsgemäßen Frankiermaschine mit einem Druckermodul 1 für ein vollelektronisch erzeugtes Frankierbild, mit mindestens einem mehrere Betätigungselemente aufweisenden Eingabemittel 2, einer Anzeigeeinheit 3, einem die Kommunikation mit einer Datenzentrale herstellenden MODEM 23, weitere Eingabemittel 21 bzw. Waage 22 welche über einen Ein/Ausgabe-Steuermodul 4 mit einer Steuereinrichtung 6 gekoppelt sind und mit nichtflüchtigen Speichern 5a, 5b bzw. 9, 10 und 11 für Daten, welche die variablen bzw. die konstanten Teile des Frankierbildes einschließen, und bzw. Programme zur Verarbeitung der Daten in Zusammenhang mit der Postbeförderungs- bzw. Dienstleistung, welche vom Carrier zu erbringen ist.

[0017] In der deutschen Patentanmeldung DE 19534530 A1 werden nähere Ausführungen zu einzelnen Funktionen der Mittel gemacht. Ein Charakterspeicher 9 liefert die nötigen Druckdaten für die variablen Teile des Frankierbildes zu einen flüchtigen Arbeitsspeicher 7. Die Steuereinrichtung 6 weist einen Mikroprozessor μ P auf, der mit dem Ein/Ausgabe-Steuermodul 4, mit dem Charakterspeicher 9, mit dem flüchtigen Arbeitsspeicher 7 und mit nichtflüchtigen Arbeitsspeichern 5a, 5b (mit internen nichtflüchtigen Tarifspeicher) bzw. (gestrichelt gezeichnet) mit einem zusätzlichen nichtflüchtigen Tarifspeicher 16, mit einem nichtflüchtigen Arbeitsspeicher 10 und 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. Derjenige Speicherbaustein, welcher den nichtflüchtigen Arbeitsspeicher 5b umfaßt, kann beispielsweise ein EEPROM sein, der durch mindestens eine zusätzliche Maßnahme, beispielsweise Aufkleben auf der Leiterplatte, Versiegeln oder Vergießen mit Epoxidharz, gegen Entnahme gesichert wird. Die Speicherung der Portotariftabellen kann separat oder beispielsweise innerhalb des nichtflüchtigen Speichers 5a realisiert werden, indem besondere Speicherbereiche bereitgestellt werden. Die einzelnen Speicher können in mehreren physikalisch getrennten oder in nicht gezeigter Weise in wenigen Bausteinen zusammengefaßt verwirklicht sein. Die zukünftig gültige Tariftabelle wird im entsprechend dafür eingerichteten vorgesehenen Speicherbereich 16-01 bzw. die bisher gültige Tariftabelle wird entsprechend im separat vorgesehenen Speicherbereich 16-02 gespeichert. Die verfügbare Speicherkapazität im nichtflüchtigen Speicher beträgt beispielsweise 20 kByte wird durch eine platzsparende Speicherplatzverwaltung optimal genutzt. Der nichtflüchtige Tarifspeicher ist vorzugsweise ein batteriegestützter C-MOS-RAM-Baustein. In einer bevorzugten Ausführungsvariante schließt er einen dritten Speicherbereich 16-03 ein, in welchem die zur jeweilig gewünschten Portotariftabelle gebildete Prüfsumme zugeordnet zu einer Versionsnummer gespeichert vorliegt.

[0018] Der Abruf der Portotariftabellendaten aus der Datenzentrale erfolgt bedarfsweise oder im Zusammenhang mit der Fernnachladung der Frankiermaschine mit einem Guthaben (Portoabruf zwecks Nachkreditierung), wobei die Sicherheitsmaßnahmen der Guthaben-Nachkreditierung mit genutzt werden. Die Portotariftabellendaten werden zunächst im Speicherbereich 7d des flüchtigen Arbeitsspeichers RAM 7 der Frankiermaschine zwischengespeichert. Der Mikroprozessor 6 kann nun über den Inhalt der Portotariftabellendaten eine Prüfsumme bilden und per Modem 23 zur Datenzentrale DC über ein Kommunikationsnetz bzw. per Funk übermitteln. Die Datenzentrale besitzt Modems 33, die mit einem Server 32 verbunden sind, welcher auf eine Datenbank 31 zugreift. Die anfordernde Frankiermaschine identifiziert sich bei der Datenzentrale mit ihrer PIN (Portoabruf Identifikation Nummer) und übermittelt die Versionsnummer zwecks Auffindung einer neuen Portotariftabelle in der Datenbank DB 31 der Datenzentrale, wobei eine Portotariftabelle der übermittelten Versionsnummer zugeordnet ist. Der Server 32 ist zur Überprüfung der ordnungsgemäßen Übertragung und fehlerfreien Zwischenspeicherung von Dienstdaten anhand der Prüfsumme programmiert, was anhand der Fig.3a und b noch näher erläutert wird.

[0019] In der Figur 1b sind Details des Blockschaltbildes der elektronischen Frankiermaschine für eine Variante mit OTP (One Time programmable Prozessor) in der Steuereinrichtung gezeigt, welche prinzipiell in der deutschen Patentanmeldung DE 19534530 A1 mit dem Titel: Verfahren zur Absicherung von Daten und Programmcode einer elektronischen Frankiermaschine, sowie näher in der deutschen Patentanmeldung DE 19731304.3-53 mit dem Titel: Verfahren zur Statistikmodusnachladung und zur statistischen Erfassung nach Statistikklassen bei der Speicherung eines Datensatzes, erläutert wurden. Die CPU 6a bildet die Prüfsumme aufgrund der übermittelten und flüchtig zwischengespeicherten Tabelle. Die Zwischenspeicherung der übermittelten Tabelle kann beispielsweise auch im internen Arbeitsspeicher iRAM 6b statt im flüchtigen Arbeitsspeicher RAM 7 oder unter Nutzung beider Arbeitsspeicher erfolgen.

[0020] In der Figur 1c ist ein Blockschaltbild der elektronischen Frankiermaschine für eine Variante mit portoberechnender Waage dargestellt. Der Tarifspeicher 16 und der Portorechner sind hier Bestandteil der portoberechnenden Waage 22a. Letztere nutzt das Modem 23 der Frankiermaschine zur Kommunikation mit der Datenzentrale.

[0021] Wird eine geänderte Portotariftabelle in einem elektronischen Portorechner benötigt, kann eine Ferninstallation an demand erfolgen. Auf Anforderung ist eine Portotariftabelle zum Endgerät zu übermitteln, um diese in entsprechende Speicher des Portorechners laden zu können. Bei einer solchen Ferninstallation ist das erfindungsgemäße Verfahren zur sicheren Übertragung von Dienstdaten an ein Endgerät in einer Ausführungsform

mit folgenden Verfahrensschritten vorgesehen:

- Bereitstellen 210 von neuen Portotariftabellendaten in der Datenzentrale für eine zukünftige Portoberechnung,
- Bilden 110 von Anforderungsdaten für Portotariftabellendaten,
- erste Kommunikation 120 des Endgerätes mit einer Datenzentrale, umfassend ein Senden der Anforderungsdaten, um die neuen Portotariftabellendaten von der Datenzentrale anzufordern, und umfassend ein Empfangen und Speichern der angeforderten Portotariftabellendaten,
- erste Kommunikation 220 der Datenzentrale mit dem Endgerät, umfassend ein Empfangen der Anforderungsdaten in der Datenzentrale und ein Senden der angeforderten Portotariftabellendaten an das Endgerät,
- zweite Kommunikation 130 des Endgerätes mit einer Datenzentrale, umfassend ein Bilden und Übermittlung einer Information vom Endgerät zur Datenzentrale, welche auf die gespeicherten gültigen neuen Portotariftabellendaten bezogen ist,
- zweite Kommunikation 230 der Datenzentrale mit dem Endgerät, umfassend ein Empfangen und Prüfen der Information in der Datenzentrale mittels einer aus den Portotariftabellendaten generierten Vergleichsinformation und umfassend ein Senden einer OK-Meldung an das Endgerät, wobei in Verbindung mit dem Senden einer OK-Meldung in der Datenzentrale ein Registrieren (Schritt 240) der Dienstleistung erfolgt.

[0022] Es ist vorgesehen, daß beim Empfang der OK-Meldung im Endgerät ein Markieren der gespeicherten Daten als gültig registriert erfolgt, als Vermerk, daß in der Datenzentrale ein Registrieren zur Bezahlung der Dienstleistung erfolgt. Im nichtflüchtigen Speicher des Portorechners wird zwecks Markierung entweder in einem gesicherten Bereich ein Bit gesetzt oder entsprechende MAC-gesicherte Daten gespeichert. Vom Mikroprozessor werden zur Portoberechnung nur gültig registrierte Daten genutzt.

[0023] Bei einer alternativen Ausführungsform sind folgende Verfahrensschritte vorgesehen:

- Bereitstellen 210 von neuen Portotariftabellendaten in der Datenzentrale für eine zukünftige Portoberechnung,
- Bilden 110 von Anforderungsdaten für Portotariftabellendaten,
- erste Kommunikation 120 des Endgerätes mit einer Datenzentrale, umfassend ein Senden der Anforderungsdaten, um die neuen Portotariftabellendaten von der Datenzentrale anzufordern, und umfassend ein Empfangen und Zwischenspeichern der angeforderten Portotariftabellendaten,
- erste Kommunikation 220 der Datenzentrale mit

dem Endgerät, umfassend ein Empfangen der Anforderungsdaten in der Datenzentrale und ein Senden der angeforderten Portotariftabellendaten an das Endgerät,

- 5 - zweite Kommunikation 130 des Endgerätes mit einer Datenzentrale, umfassend ein Bilden und Übermittlung einer Information vom Endgerät zur Datenzentrale, welche auf die zwischengespeicherten gültigen neuen Portotariftabellendaten bezogen ist,
- 10 - zweite Kommunikation 230 der Datenzentrale mit dem Endgerät, umfassend ein Empfangen und Prüfen der Information in der Datenzentrale mittels einer aus den Portotariftabellendaten generierten Vergleichsinformation und umfassend ein Senden einer Lade-Anweisung an das Endgerät, die neuen Portotariftabellendaten in einen nichtflüchtigen Speicher eines Portorechner zu laden.

20 **[0024]** Es ist vorgesehen, daß in der Datenzentrale ein Registrieren (Schritt 240) des Ladens erfolgt und daß nach Empfangen der Ladeanweisung ein Laden (Schritt 140) der Portotariftabellendaten in einen nichtflüchtigen Speicher des Portorechners erfolgt.

25 **[0025]** In vorteilhafter Weise kann die Kommunikation von der Datenzentrale per Modem direkt mit der Frankiermaschine bzw. portoberechnenden Waage oder indirekt über die Frankiermaschine zur portoberechnenden Waage, wie in US 5,606,508 und US 5,710,706 vorgeschlagen wurde, erfolgen.

30 Der Portorechner ist gemäß der US 5,606,508 innerhalb der elektronischen Frankiermaschine angeordnet und eine Waage ist nur zur Gewichtsübermittlung mit der elektronischen Frankiermaschine verbunden. Alternativ ist - in aus der US 5,710,706 bekannter Weise - eine portoberechnende Waage mit einem elektronischen Portorechner ausgerüstet. Somit kann bereits aufgrund des gemessenen Gewichtes der Portowert von der portoberechnende Waage bestimmt und in der Frankiermaschine eingegeben werden. Bei diesen bekannten Lösungen wird von einer nichtflüchtigen Zwischenspeicherung der Portotariftabelle, beispielsweise in einer Chipkarte oder im Speicher eines GSM-Netzes, ausgegangen, aus welchen die Datentabellen zum

45 Laden entnommen werden.
Im Unterschied dazu ist bei der alternativen Ausführungsform der erfindungsgemäßen Lösung zunächst eine flüchtige Zwischenspeicherung der übermittelten Tabelle in einem flüchtigen Arbeitsspeicher des Endgerätes bzw. des Portorechners ausreichend. Es ist vorgesehen, daß das Endgerät mit einem Portorechner verbunden ist, in welchem die Speicherung der neuen Portotariftabellendaten erfolgt.

50 **[0026]** Eine Variante sieht vor, daß der Portorechner im Endgerät integriert ist oder separat vom Endgerät angeordnet ist. Es ist vorgesehen, daß die Zwischenspeicherung im flüchtigen Arbeitsspeicher RAM 7 erfolgt, um mittels des Mikroprozessors 6 eine Prüf-

summe zu bilden. Die Prüfsumme wird vom Portorechner über den Inhalt der Tabelle nach einem bekannten Algorithmus gebildet, welcher im Programmspeicher 11 gespeichert ist.

Die zur Datenzentrale übermittelte Information enthält vorzugsweise die Versionsnummer und eine Prüfsumme über die Portotariftabellendaten in einer vorbestimmten mathematischen Verknüpfung oder eine verschlüsselte Prüfsumme bzw. eine Signatur. Zur Verschlüsselung werden bekannte symmetrische oder unsymmetrische Algorithmen eingesetzt.

[0027] Eine zweite Variante der Anordnung ist mit einem OTP-Prozessor ausgestattet und erlaubt die Bildung einer DES-verschlüsselten Prüfsumme, wobei der symmetrische DES-Algorithmus (Data Encryption Standard) und der geheime DES-Schlüssel in der Frankiermaschine sicher gespeichert sind. Alternativ kann eine Prüfsumme vom separaten Portorechner zur Frankiermaschine übermittelt werden, welche ein sicheres Gehäuse aufweist und durch besondere Maßnahmen vor einer Manipulation in Fälschungsabsicht geschützt ist. Die Frankiermaschine bildet dann eine DES-verschlüsselte Prüfsumme, wobei der dazu benötigte DES-Schlüssel in der Frankiermaschine in an sich bekannter Weise sicher gespeichert ist.

[0028] Die andere Variante zeichnet sich dadurch aus, daß der Portorechner in eine Waage integriert ist oder separat vom Endgerät angeordnet ist. Der Portorechner enthält einen Programmspeicher mit einem unsymmetrischen Verschlüsselungsalgorithmus und mit einem öffentlichen Schlüssel. Letzterer, welcher im Unterschied zu einem geheimen Schlüssel nicht besonders geschützt zu werden braucht, kann folglich ebenfalls in einem Speicher der Waage nichtflüchtig gespeichert werden.

[0029] Als unsymmetrischer Verschlüsselungsalgorithmus ist der nach seinen Erfindern (R.Rivest, A.Shamir, L.Adleman) benannte RSA-Algorithmus bekannt. Dieser ist dann vorteilhaft, wenn kein gesichertes Gehäuse zum Schutz der Schlüssel verfügbar ist. Beispielsweise wird in der Waage eine RSA-verschlüsselte Prüfsumme gebildet, wobei ein RSA-Schlüssel benutzt wird, welcher in der Waage als ein öffentlicher Schlüssel gespeichert ist, der nicht gesichert gespeichert werden muß.

[0030] In der Figur 2 ist ein Flußplan für die sichere Übertragung von Daten an ein Endgerät dargestellt. Die Datenzentrale startet im Schritt 200 und stellt im folgenden Schritt 210 neue Portotariftabellen bereit.

Das Endgerät ist beispielsweise eine Frankiermaschine, welche beim Einschalten gestartet wird (Schritt 100).

Die Frankiermaschine enthält einen Portorechner, welcher im Schritt 110 Anforderungsdaten für neue Portotariftabellendaten bildet. Es ist in einer Variante vorgesehen, daß eine Automatik Anforderungsdaten bildet, um auf aktuelle Tabellen zugreifen zu können, wenn der Zeitpunkt für neue Portotariftabellendaten

näher rückt. Diese Automatik arbeitet abhängig vom eingestellten Carrier und dem vom Uhren/Datumsbaustein 8 der Frankiermaschine gelieferten Datum. Die Automatik kann im Portorechner und/oder in den Speicherzellen des Uhren/Datumsbausteins 8 realisiert sein. Alternativ kann der Portorechner in eine portoberechnende Waage 22a integriert sein, welche schnittstellenmäßig mit der Frankiermaschine verbunden ist.

[0031] Die Kommunikation auf der Seite des Endgerätes, d.h. der Frankiermaschine mit einer Datenzentrale, umfaßt beispielsweise zwei Transaktionen. Die erste Transaktion 120 beginnt mit einem Senden der Anforderungsdaten, um die neuen Portotariftabellendaten von der Datenzentrale anzufordern und schließt mit einem Empfangen und Zwischenspeichern der angeforderten Portotariftabellendaten in einem flüchtigen Arbeitsspeicher RAM 7d. Parallel läuft auf der Seite der Datenzentrale eine Kommunikation (Schrill 220) der Datenzentrale mit dem Endgerät, umfassend ein Empfangen der Anforderungsdaten in der Datenzentrale und ein Senden der angeforderten Portotariftabellendaten an das Endgerät, d.h. an die Frankiermaschine.

[0032] Die zweite Transaktion 130 auf der Seite des Endgerätes beginnt mit einem Bilden einer Information im Endgerät, d.h. in der Frankiermaschine, wobei die Information auf die zwischengespeicherten gültigen neuen Portotariftabellendaten bezogen ist. Die Kommunikation des Endgerätes mit einer Datenzentrale wird mit der Übermittlung der Information vom Endgerät zur Datenzentrale und einem Empfangen der OK-Meldung, ggf. mit Ladeanweisung, fortgesetzt. Parallel läuft auf der Seite der Datenzentrale eine zweite Kommunikation (Schritt 230) der Datenzentrale mit dem Endgerät, umfassend ein Empfangen und Prüfen der Information in der Datenzentrale mittels einer aus den Portotariftabellendaten generierten Vergleichsinformation und umfassend ein Senden einer OK-Meldung, ggf. mit Lade-Anweisung an das Endgerät, die neuen Portotariftabellendaten in einen nichtflüchtigen Speicher des Portorechner zu laden. Im Schritt 140 wird die empfangene OK-Meldung ausgeführt, ggf. erfolgt ein Laden einer neuen Portotariftabellendaten, wenn eine gültige Lade-Anweisung empfangen wurde. Andernfalls wird die zweite Kommunikation wiederholt, wenn keine OK-Meldung empfangen wurde.

Parallel dazu wird auf der Seite der Datenzentrale eine Registrierung (Schritt 240) der Dienstleistung in einer Datenbank der Datenzentrale vorgenommen, zwecks Rechnungslegung und Abbuchung bzw. späterer Bezahlung. Dann wird auf den Schritt 210 zurückverzweigt.

[0033] Beim bevorzugten Beispiel mit dem Portorechner in der elektronischen Frankiermaschine, sendet die Frankiermaschine neben Ihrer PIN eine Versionsnummer und die Prüfsumme an die Datenzentrale, welche in der Datenzentrale gestatten, die übertragenen neuen Tariftabellendaten eindeutig zu identifizieren. Bevor die in der Frankiermaschine zwischengespeicherten Tarif-

tabellendaten als gültig anerkannt werden, wird noch eine Überprüfung einer Prüfsumme in der Datenzentrale durchgeführt.

Die Information beinhaltet vorzugsweise die Versionsnummer der Tabelle und eine verschlüsselte Prüfsumme, um eine Verifikation der ordnungsgemäß übermittelten und zwischengespeicherten Tabelle zu ermöglichen. Eine verschlüsselte Prüfsumme kann als digitale Signatur verwendet werden, welche auf die flüchtig zwischengespeicherten gültigen neuen Portotariftabellendaten bezogen ist. Es können jedoch weitere Daten in die Information eingehen bzw. mit verschlüsselt werden.

[0034] In den Figuren 3a und 3b werden eine erste und zweite Variante eines Flußplans für die Überprüfung der sicheren Übertragung von Daten an ein Endgerät dargestellt.

[0035] Es ist in einer - in der Fig.3a gezeigten - Variante vorgesehen, daß die verschlüsselte Prüfsumme vom Portorechner mittels eines unsymmetrischen Verschlüsselungs-Algorithmuses gebildet wird, in welchem ein öffentlicher Schlüssel gespeichert ist, sowie daß zur Prüfung in der Datenzentrale ein zugehöriger privater geheimer Schlüssel (PRIVET KEY) verwendet wird, welcher sicher gespeichert und vor einer dritten Partei geheim gehalten wird. Bei einer RSA-Signatur (R.Rivest, A.Shamir, L.Adleman), wird eine auf der Versionsnummer und der Prüfsumme basierende Nachricht mit einem öffentlichen Schreibschlüssel (PUBLIC KEY) zu einer digitalen Unterschrift verschlüsselt. Die digitale Unterschrift (SIGNATUR) wird zusammen mit der Identifikationsnummer PIN und der Versionsnummer (VERSION-Nr.) vom Endgerät zur Datenzentrale gesendet, welche mit einem geheimen Leseschlüssel (PRIVET KEY) nach dem dem unsymmetrischen Algorithmus (RSA) die Signatur entschlüsseln kann. Die Prüfsumme (CHECK SUM) über den Inhalt der Tariftabellendaten, welche in der Datenbank 31 zugeordnet zur Versionsnummer und ggf. auch zugeordnet zu PIN gespeichert sind, muß mit der entschlüsselten Nachricht übereinstimmen, wenn die im Portorechner bzw. in der Frankiermaschine zwischengespeicherten Tariftabellendaten als gültig anerkannt werden sollen. Diese Verifikation ist eine Voraussetzung, um einen entsprechenden Befehl zur Frankiermaschine zu übermitteln. Die RATE TABLE CHECK SUM-Bildung kann vor oder während der Kommunikation erfolgen. Eine vorherige Bildung hat den Vorteil, daß die Vergleichs-Prüfsumme RATE TABLE CHECK SUM in der Datenbank 31 zugeordnet zur Versionsnummer VERSION-NR. bzw. PIN gespeichert vorliegt und vom Server 31 zum Vergleich direkt aus der Datenbank 31 aufgerufen werden kann. Die eingesparte Rechenzeit des Servers 32 steht damit vorteilhaft dem Entschlüsselungsvorgang der SIGNATUR zur Verfügung. Die entschlüsselte Nachricht ist mit der Prüfsumme CHECK SUM identisch, welche im Portorechner bzw. Endgerät aus der flüchtig zwischengespeicherten Portotariftable gebildet wurde. Bei

ordnungsgemäßer Zwischenspeicherung ist die entschlüsselte Prüfsumme CHECK SUM identisch mit der gebildeten bzw. in der Datenbank 31 gespeicherten Vergleichsprüfsumme RATE TABLE CHECK SUM.

5 **[0036]** Zur RSA-Signatur (R.Rivest, A.Shamir, L.Adleman) ist auch der Digital Signatur Algorithmus (DSA) nach US 5,231,668 bekannt. Prinzipiell kann aber auch ein beliebig anderer unsymmetrischer Algorithmus, beispielsweise ELGamal-Algorithmus (ELGA) oder Elliptic
10 Curve Signatur Schema (ECSS), eingesetzt werden.

[0037] Alternativ ist in einer - in der Fig.3b gezeigten - Variante vorgesehen, daß die verschlüsselte Prüfsumme MAC (Message Authentication Code) mittels eines symmetrischen Verschlüsselungs-Algorithmuses von der Frankiermaschine gebildet wird, in welcher ein geheimer Schlüssel gespeichert ist. Die verschlüsselte Prüfsumme MAC wird zur Datenzentrale übermit-
15 telt. Im Unterschied zur in der Fig.3a gezeigten Variante, wird in der Datenzentrale keine Entschlüsselung durchgeführt, sondern eine Verschlüsselung, um eine eine aus der Portogebührentabelle abgeleitete Prüfsumme zu verschlüsseln zu einem Vergleichs MAC'. Die RATE TABLE CHECK SUM-Bildung kann vor oder während der Kommunikation erfolgen. Eine vorherige Bildung hat den Vorteil, daß die CHECK SUM ledig-
20 lich aus der Datenbank 31 aufgerufen werden muß, um aus dieser CHECK SUM durch Verschlüsselung mit einem Geheimschlüssel SECRET KEY unter Anwendung eines symmetrischen Algorithmus DES mit Hilfe des Servers 32 den Vergleichs MAC' zu erzeugen.

[0038] Bei der Prüfung in der Datenzentrale wird der gleiche geheime Schlüssel SECRET KEY verwendet, wie in der Frankiermaschine. Die Überprüfung in der Datenzentrale erfolgt vorzugsweise mittels beider
25 MAC's. Bei der MAC-Bildung wird vorzugsweise eine geeignete Variante des DES-Algorithmuses genutzt. Bei einer MAC-Bildung werden in der Datenzentrale und der Frankiermaschine der gleiche geheime DES-Schlüssel verwendet. Dazu muß der geheime DES-Schlüssel jener das Endgerät identifizierende PIN zugeordnet in der Datenbank 31 sicher gespeichert werden. Alternativ kann die RATE TABLE CHECK SUM-Bildung und die Verschlüsselung zu einem Vergleichs-MAC
30 gemeinsam vor der Kommunikation erfolgen. Die Vergleichs-MAC ist dann in der Datenbank 31 zugeordnet zur PIN und Versionsnummer gespeichert und kann vom Server zu Vergleichszwecken abgerufen werden.

[0039] Neuere Frankiermaschinen setzen digital arbeitende Druckwerke ein. Beispielsweise weisen die
35 Frankiermaschinen T1000 bzw. JetMail des Anmelders weltweit erstmals einen Thermotransferdrucker bzw. einen Tintenstrahldrucker auf. Damit ist es prinzipiell möglich, auf einen gefüllten Brief im Bereich des Frankierstempels andere Informationen bzw. beliebig
40 anders zu drucken, welche in einem entsprechenden Zusammenhang mit einer Dienstleistung eines Carriers stehen. Es ist also leicht möglich zwischen den privaten Postbeförderern und Ihren Dienstleistungen zu wech-

seln. Der Frankierstempelsabdruck enthält deshalb vorteilhaft einen Hinweis auf den Carrier und/oder die in Anspruch genommene oder noch geplante Dienstleistung.

[0040] Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die vom gleichen Grundgedanken der Erfindung ausgehend, die von den anliegenden Ansprüchen umfaßt werden.

Patentansprüche

1. Verfahren zur sicheren Übertragung von Dienstdaten an ein Endgerät, **gekennzeichnet durch** die Schritte,
 - Bereitstellen (210) von neuen Dienstdaten in der Datenzentrale für eine zukünftige Verarbeitung basierend auf den Dienstdaten,
 - Bilden (110) von Anforderungsdaten für Dienstdaten,
 - erste Kommunikation (120) des Endgerätes mit einer Datenzentrale, umfassend ein Senden der Anforderungsdaten, um die neuen Dienstdaten von der Datenzentrale anzufordern, und umfassend ein Empfangen und Speichern der angeforderten Dienstdaten,
 - erste Kommunikation (220) der Datenzentrale mit dem Endgerät, umfassend ein Empfangen der Anforderungsdaten in der Datenzentrale und ein Senden der angeforderten Dienstdaten an das Endgerät,
 - zweite Kommunikation (130) des Endgerätes mit einer Datenzentrale, umfassend ein Bilden und- Übermittlung einer Information vom Endgerät zur Datenzentrale, welche auf die gespeicherten gültigen neuen Dienstdaten bezogen ist,
 - zweite Kommunikation (230) der Datenzentrale mit dem Endgerät, umfassend ein Empfangen und Prüfen der Information in der Datenzentrale mittels einer aus den Dienstdaten generierten Vergleichsinformation und umfassend ein Senden einer Meldung an das Endgerät, wobei in Verbindung mit dem Senden der Meldung in der Datenzentrale ein Registrieren (Schritt 240) der Dienstleistung erfolgt.
2. Verfahren, nach Anspruch 1, **gekennzeichnet dadurch**, daß während der zweiten Kommunikation im Schritt (130) eine von der Datenzentrale gesendete OK-Meldung empfangen wird sowie daß im Endgerät die empfangene OK-Meldung im nachfolgenden Schritt (140) ausgeführt und das Endgerät oder der Portorechner in einen Betriebsmodus umgeschaltet wird.
3. Verfahren, nach den Ansprüchen 1 bis 2, **gekennzeichnet dadurch**, daß die erste Kommunikation mit Speichern der angeforderten Dienstdaten im Schritt (120) ein Zwischenspeichern der angeforderten Dienstdaten beinhaltet, daß die während der zweiten Kommunikation im Schritt (130) übermittelte Information vom Endgerät zur Datenzentrale auf die zwischengespeicherten gültigen neuen Dienstdaten bezogen ist und daß die während der zweiten Kommunikation (230) von der Seite der Datenzentrale gesendete OK-Meldung, eine Lade-Anweisung an das Endgerät einschließt, die neuen Dienstdaten in einen nichtflüchtigen Speicher eines Verarbeitungsmoduls zu laden und daß nach Empfangen der OK-Meldung mit Ladeanweisung im Endgerät ein Laden (Schritt 140) der Dienstdaten in einen nichtflüchtigen Speicher des Verarbeitungsmoduls erfolgt.
4. Verfahren, nach Anspruch 2, **gekennzeichnet dadurch**, daß die Ausführung der empfangenen OK-Meldung ein Markieren der gespeicherten Daten als gültig einschließt.
5. Verfahren, nach einem der vorherigen Ansprüche 1 oder 3, **gekennzeichnet dadurch**, daß die gebildete Information eine Versionsnummer und eine Prüfsumme einschließt.
6. Verfahren, nach einem der vorherigen Ansprüche 1 oder 3, **gekennzeichnet dadurch**, daß die gebildete Information eine Versionsnummer und eine verschlüsselte Prüfsumme einschließt.
7. Verfahren, nach einem der vorherigen Ansprüche 1 bis 6, **gekennzeichnet dadurch**, daß die Dienstdaten Portotariftabellendaten einschließen und daß der Verarbeitungsmodul ein Portorechner ist.
8. Verfahren, nach Anspruch 7, **gekennzeichnet dadurch**, daß die Prüfsumme vom Portorechner zur Frankiermaschine übermittelt und daß die verschlüsselte Prüfsumme mittels eines symmetrischen Verschlüsselungs-Algorithmusses von der Frankiermaschine gebildet wird, in welcher ein geheimer Schlüssel gespeichert ist, sowie daß zur Prüfung in der Datenzentrale der gleiche geheime Schlüssel verwendet wird.
9. Verfahren, nach Anspruch 7, **gekennzeichnet dadurch**, daß die Prüfsumme vom Portorechner gebildet wird daß die verschlüsselte Prüfsumme mittels eines unsymmetrischen Verschlüsselungs-Algorithmusses vom Portorechner gebildet wird in welchem ein öffentlicher Schlüssel gespeichert ist, sowie daß zur Prüfung in der Datenzentrale ein zugehöriger privater geheimer Schlüssel verwendet wird, welcher sicher gespeichert und vor einer

dritten Partei geheim gehalten wird.

10. Verfahren, nach Anspruch 1, **gekennzeichnet** dadurch, daß die Dienstdaten neue Portotariffabellendaten einschließen, die in der Datenzentrale für eine zukünftige Portoberechnung bereitgestellt werden (210), und daß das Senden einer OK-Meldung während der zweiten Kommunikation (230) der Datenzentrale mit dem Endgerät, welche ein Empfangen und Prüfen der Information in der Datenzentrale mittels einer aus den Portotariffabellendaten generierten Vergleichsinformation umfaßt, auch ein Senden einer Lade-Anweisung an das Endgerät ist, die neuen Portotariffabellendaten in einen nichtflüchtigen Speicher eines Portorechner zu laden. 5
11. Verfahren, nach Anspruch 10, **gekennzeichnet dadurch**, daß nach dem Senden der Lade-Anweisung in der Datenzentrale ein Registrieren (Schritt 240) des Ladens erfolgt und daß nach Empfangen der Ladeanweisung ein Laden (Schritt 140) der Portotariffabellendaten in einen nichtflüchtigen Speicher des Portorechners erfolgt. 10
12. Anordnung zur Durchführung des Verfahrens, nach Anspruch 1, mindestens mit Ein-Ausgabemitteln (1, 2, 3, 4, 21, 23), einem Programmspeicher (11), einem Mikroprozessor (6) und Speichern (5a 5b, 16) zur nichtflüchtigen Speicherung von Dienstdaten und einem flüchtigen Arbeitsspeicher (7) im Endgerät, **gekennzeichnet dadurch**, daß das Endgerät mit einem Portorechner verbunden ist und daß der Mikroprozessor das Endgerätes oder des Portorechners programmiert ist, 15
- eine Speicherung der neuen Portotariffabellendaten im Speicher des Endgerätes bzw. des Portorechners vorzunehmen und eine Prüfsumme über die gespeicherten neuen Portotariffabellendaten zu bilden und zur Datenzentrale zu übermitteln, sowie 20
 - eine empfangene OK-Meldung auszuführen und das Endgerät oder den Portorechner in einen Betriebsmodus umzuschalten. 25
13. Anordnung, nach Anspruch 12, **gekennzeichnet dadurch**, daß der Mikroprozessor das Endgerätes oder des Portorechners programmiert ist, 30
- eine Zwischenspeicherung der neuen Portotariffabellendaten im flüchtigen Arbeitsspeicher des Endgerätes bzw. des Portorechners vorzunehmen und eine Prüfsumme über die zwischengespeicherten neuen Portotariffabellendaten zu bilden und zur Datenzentrale zu übermitteln, sowie 35
 - sowie beim Empfangen einer OK-Meldung eine 40
- Lade-Anweisung der Datenzentrale an das Endgerät auszuführen, die neuen Portotariffabellendaten in einen nichtflüchtigen Speicher (5a, 5b, 16) eines Portorechners zu laden und dannach das Endgerät oder den Portorechner in einen Betriebsmodus umzuschalten. 45
14. Anordnung, nach einem der vorherigen Ansprüche 12 oder 13, **gekennzeichnet dadurch**, daß der Portorechner im Endgerät intergriert ist oder separat vom Endgerät angeordnet ist. 50
15. Anordnung, nach einem der vorherigen Ansprüche 12 oder 13, **gekennzeichnet dadurch**, daß der Portorechnerin eine Waage intergriert ist oder separat vom Endgerät angeordnet ist. 55
16. Anordnung, nach Anspruch 14, **gekennzeichnet dadurch**, daß das Endgerät eine Frankiermaschine ist und daß ein symmetrischer Verschlüsselungs-Algorithmus zur Bildung einer verschlüsselte Prüfsumme und ein geheimer Schlüssel in der Frankiermaschine sicher gespeichert vorliegt. 60
17. Anordnung, nach Anspruch 15, **gekennzeichnet dadurch**, daß ein unsymmetrischer Verschlüsselungs-Algorithmus zur Bildung einer verschlüsselte Prüfsumme und ein öffentlicher Schlüssel in der Waage gespeichert ist, wobei der öffentliche Schlüssel ungesichert gespeichert vorliegt. 65
18. Verfahren zur sicheren Übertragung von Dienstdaten an ein Endgerät, **gekennzeichnet durch** die Schritte: 70
- Übertragung von unverschlüsselten Dienstdaten an das Endgerät,
 - Erzeugen eines Codes basierend auf den übertragenen Dienstdaten,
 - Rückübertragung des Codes zur Datenzentrale und
 - Überprüfen des rückübertragenen Codes in der Datenzentrale und Übertragen einer Meldung an das Endgerät im Ergebnis der Überprüfung. 75
19. Verfahren, nach Anspruch 18, **gekennzeichnet durch** die Schritte: 80
- Übertragung von unverschlüsselten Tariffabellendaten an einen Portorechner,
 - Erzeugen einer Prüfsumme basierend auf den übertragenen Tariffabellendaten,
 - Rückübertragung der Prüfsumme zur Datenzentrale und
 - Überprüfen der rückübertragenen Prüfsumme in der Datenzentrale anhand einer gespeicherten Prüfsumme und Übertragen einer OK-Mel- 85

dung an das Endgerät im Ergebnis der Überprüfung bei Übereinstimmung der rückübertragenen mit der gespeicherten Prüfsumme.

5

20. Verfahren, nach Anspruch 18, **gekennzeichnet durch** die Schritte:

- Übertragung von unverschlüsselten Tariftabellendaten an einen Portorechner, 10
- Erzeugen eines verschlüsselten Codes basierend auf den übertragenen Tariftabellendaten,
- Rückübertragung des verschlüsselten Codes zur Datenzentrale und
- Überprüfen des rückübertragenen Codes in der Datenzentrale anhand eines gespeicherten verschlüsselten Codes und Übertragen einer OK-Meldung an das Endgerät im Ergebnis der Überprüfung bei Übereinstimmung des rückübertragenen Codes mit dem gespeicherten verschlüsselten Code. 20

21. Verfahren, nach Anspruch 18, **gekennzeichnet durch** die Schritte:

25

- Übertragung von unverschlüsselten Tariftabellendaten an einen Portorechner,
- Erzeugen einer Signatur basierend auf einer Information betreff der übertragenen Tariftabellendaten, wobei die Information mit einem öffentlichen Schreibe Schlüssel zur Signatur verschlüsselt wird, 30
- Rückübertragung der Signatur zur Datenzentrale und
- Überprüfen der Information aus der rückübertragenen Signatur in der Datenzentrale nach dem Entschlüsseln der Signatur mittels einem geheimen Leseschlüssel nach einem unsymmetrischen Algorithmus und nach Vergleich mit einer gespeicherten Information, Übertragen einer OK-Meldung an das Endgerät im Ergebnis der Überprüfung bei Übereinstimmung der aus der rückübertragenen Signatur entschlüsselten Information mit der gespeicherten Information. 40

45

22. Verfahren, nach Anspruch 21, **dadurch gekennzeichnet**, daß Information eine Prüfsumme einschließt

50

55

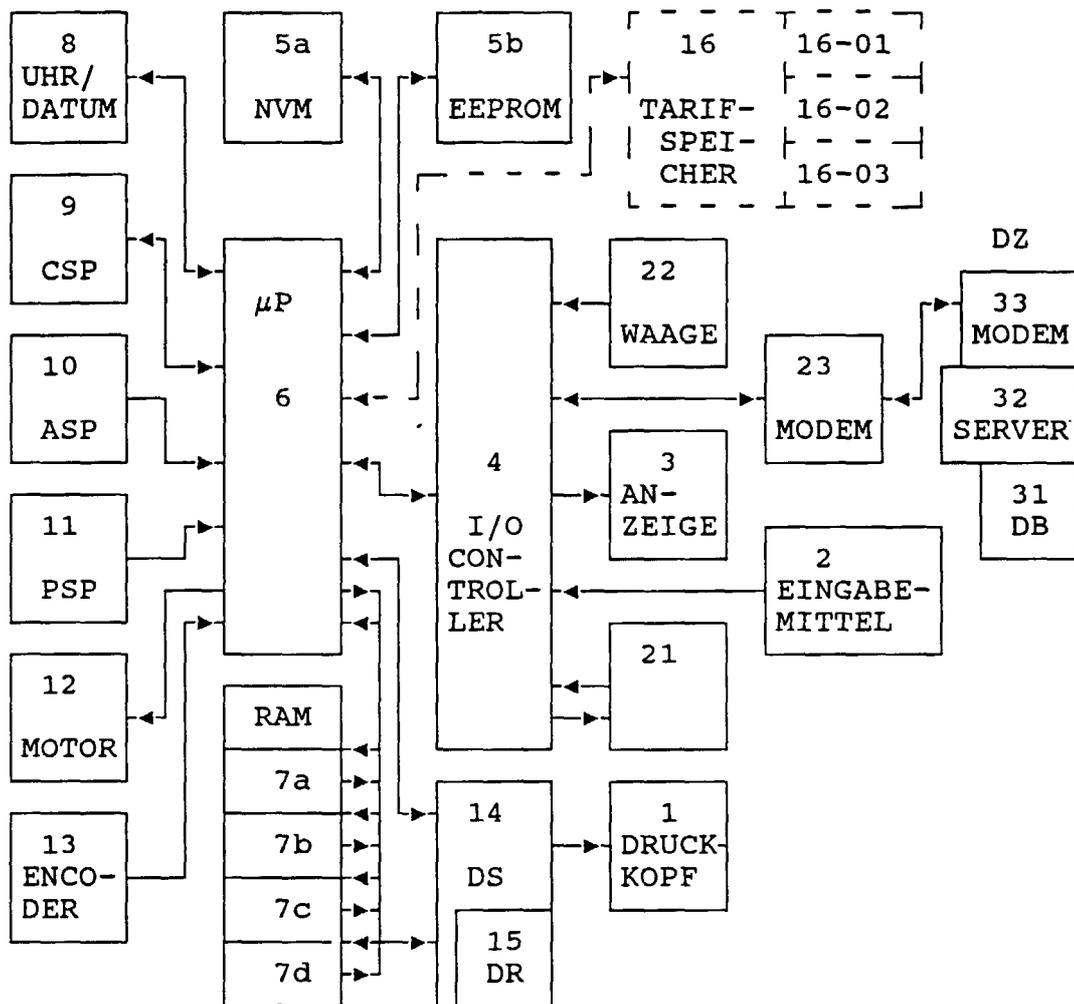


Fig. 1a

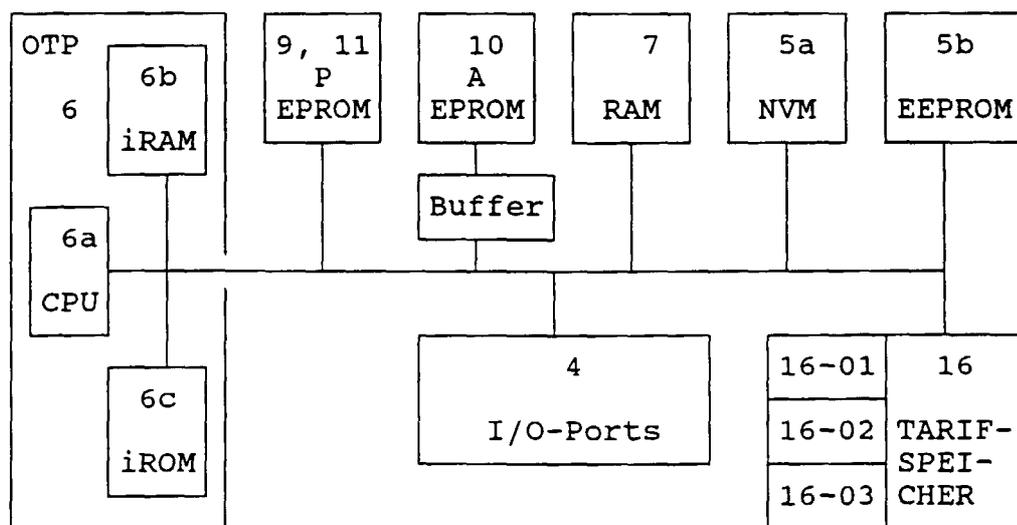


Fig. 1b

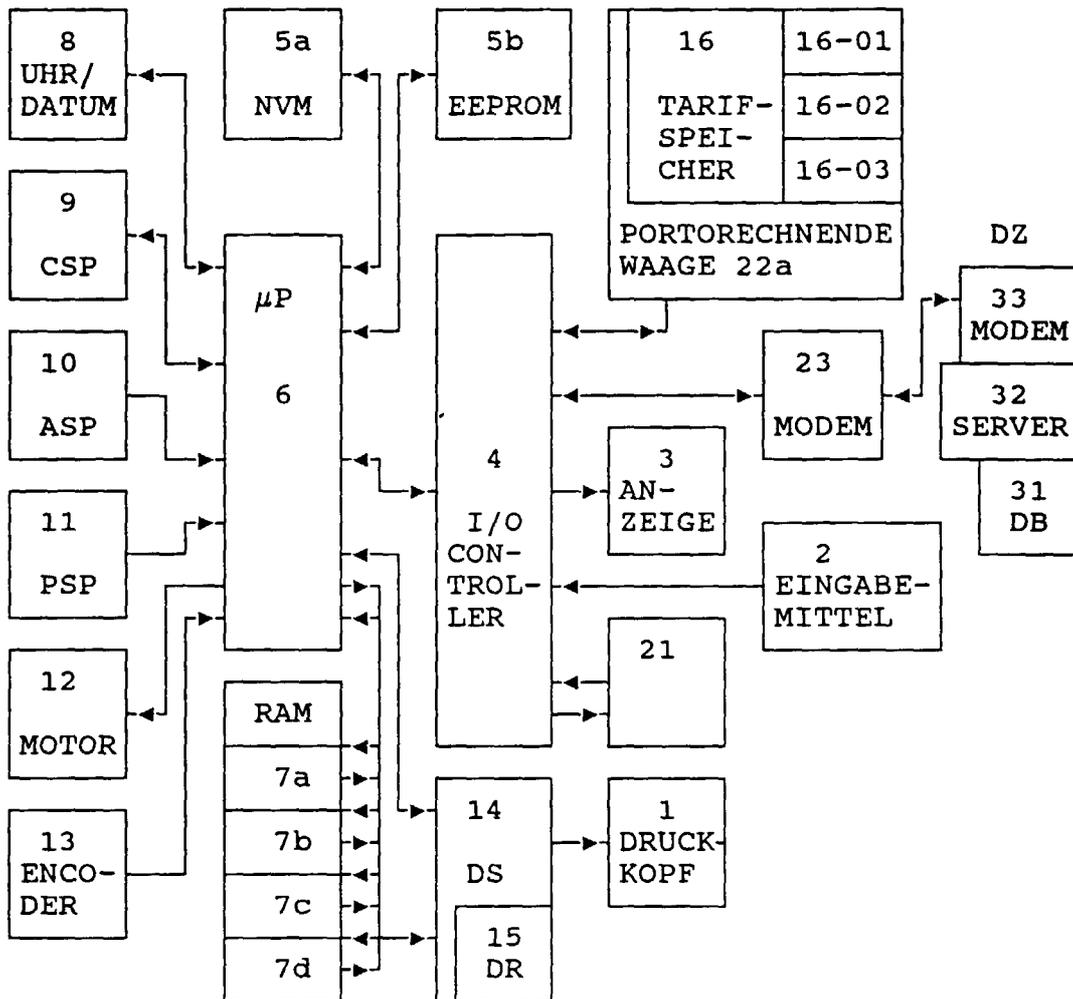


Fig. 1c

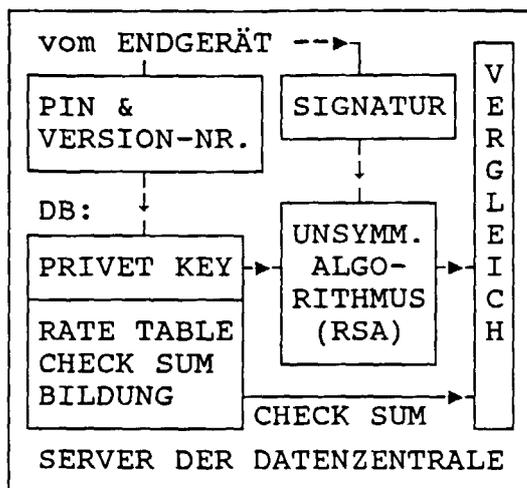


Fig. 3a

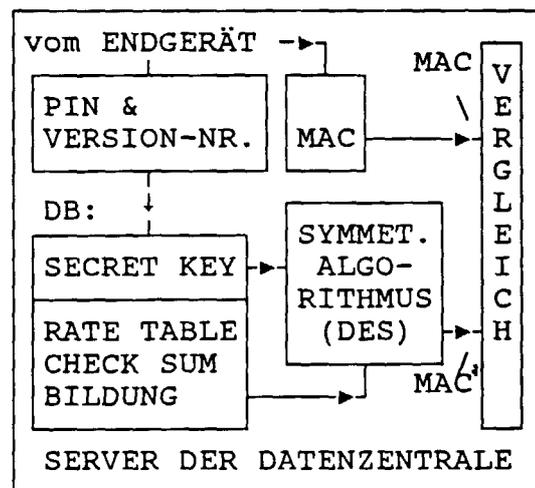


Fig. 3b

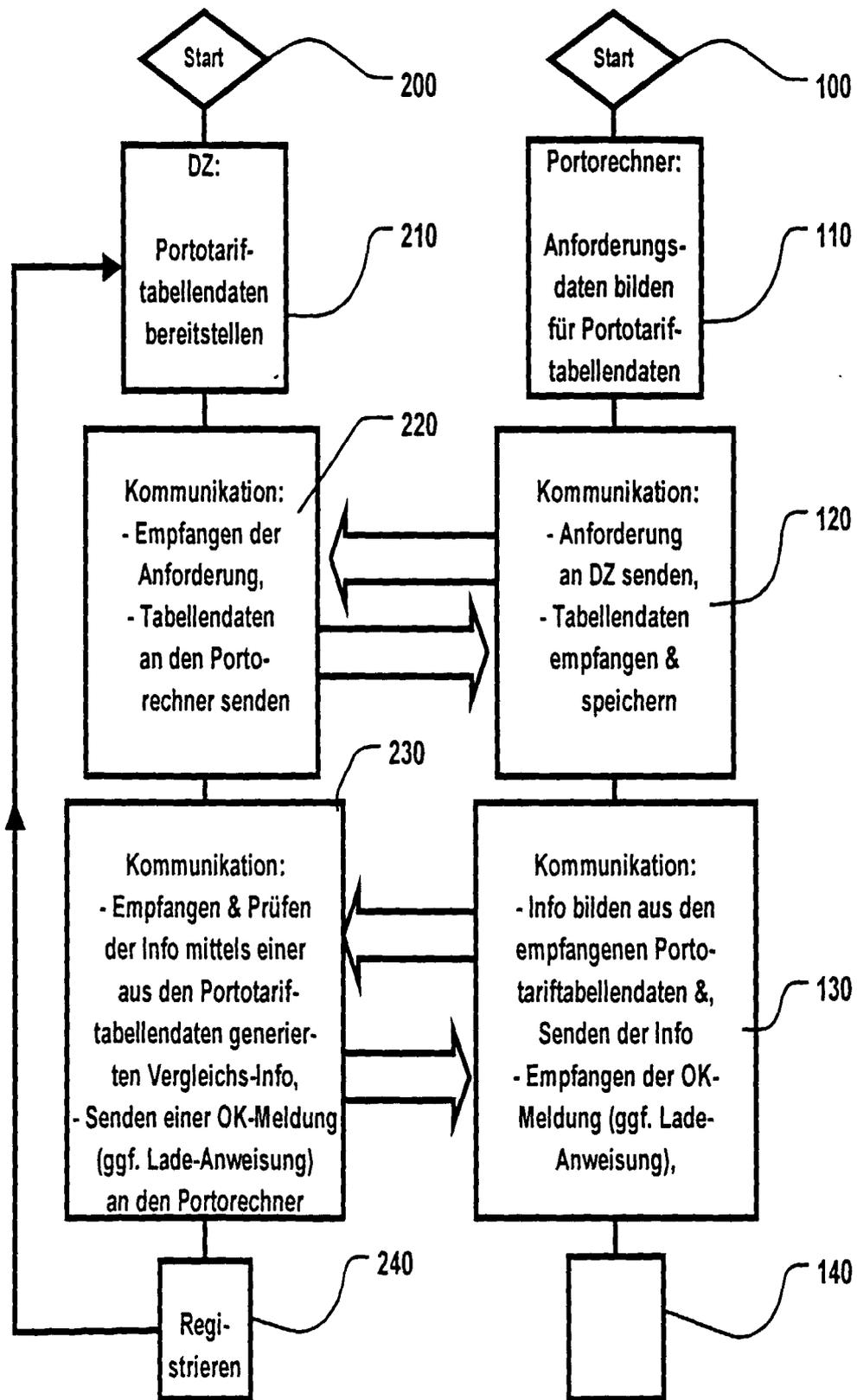


Fig. 2