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

(11) EP 1 577 840 A2

# (12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
**21.09.2005 Patentblatt 2005/38**

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

(21) Anmeldenummer: **05003805.8**

(22) Anmeldetag: **23.02.2005**

(84) Benannte Vertragsstaaten:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR**
Benannte Erstreckungsstaaten:
**AL BA HR LV MK YU**

(30) Priorität: **19.03.2004 DE 102004014427**

(71) Anmelder: **Francotyp-Postalia AG & Co. KG**
**16547 Birkenwerder (DE)**

(72) Erfinder:
- **Bleumer, Gerrit, Dr.**
  **16552 Schildow (DE)**
- **Heinrich, Clemens**
  **12161 Berlin (DE)**
- **Rosenau, Dirk**
  **13469 Berlin (DE)**

## (54) Verfahren für ein servergesteuertes Sicherheitsmanagement von erbringbaren Dienstleistungen und Anordnung zur Bereitstellung von Daten nach einem Sicherheitsmanagement für ein Frankiersystem

(57) Anordnung zur Bereitstellung von Daten entsprechend eines Sicherheitsmanagements für ein Frankiersystem (1) hat ein entferntes Datenzentrum (3), welches eine Liste von Datensätzen aufweist, die Sicherheitsinformationen sowie Informationen zur zugehörigen Sicherheitspolitik enthalten betreffend mindestens Sicherheitsmaßnahmen und den Ort der Speicherung im Frankiersystem. Das Verfahren für ein servergesteuertes Sicherheitsmanagement von erbringbaren Dienstleistungen umfaßt die Schritte: A) Empfangen der Anforderung einer gewünschten Dienstleistung, B) Ermitteln der zu wählenden Sicherheitsmerkmale und Generierung eines Datensatzes, C) Auswahl des logischen Kanals und Datensatzübermittlung, D) Feststellung des Dienstleistungsendes und E) Warten auf den Empfang einer weiteren Dienstleistungsanforderung oder auf die Beendigung der Kommunikationsverbindung.

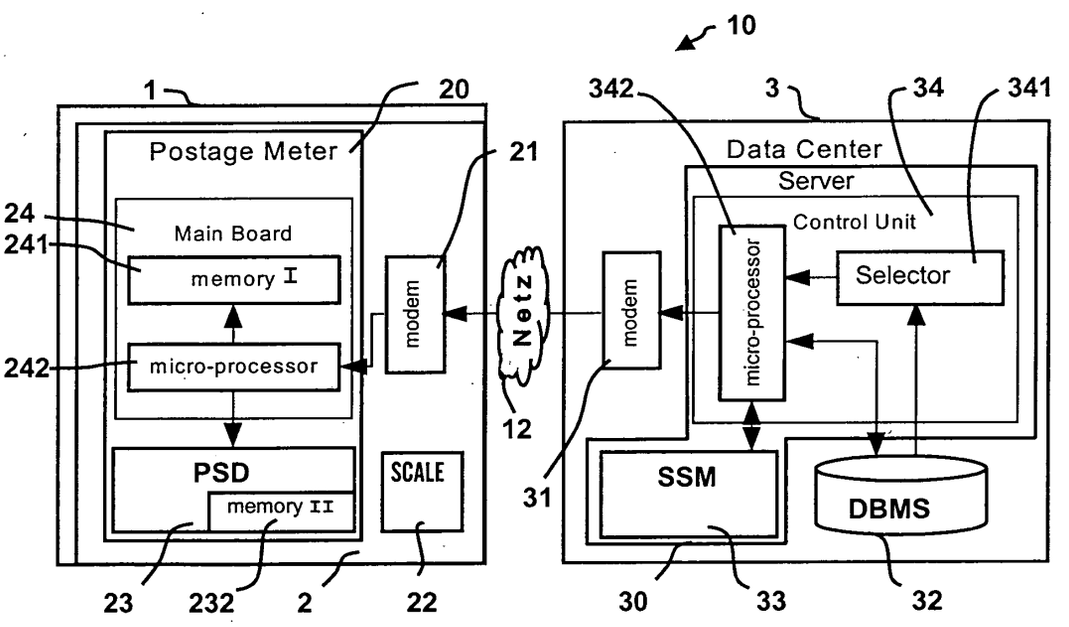


Fig. 2

EP 1 577 840 A2

## Beschreibung

**[0001]** Die Erfindung betrifft ein Verfahren für ein servergesteuertes Sicherheitsmanagement von erbringbaren Dienstleistungen gemäß des Oberbegriffs des Anspruchs 1 und eine Anordnung zur Bereitstellung von Daten nach einem Sicherheitsmanagement für ein Frankiersystem gemäß des Oberbegriffs des Anspruchs 5. Die Erfindung kommt für Frankiermaschinen und für andere Postverarbeitungsgeräte und deren Peripheriegeräte zum Einsatz, welche eine Dienstleistung eines entfernten Datenzentrums nutzen.

**[0002]** Die Frankiermaschine JetMail® der Anmelderin ist mit einer Base und mit einem abnehmbaren Meter ausgestattet. Letzterer ist mit einer im Base-Gehäuse integrierten statischen Waage betriebsmäßig verbunden und wird u.a. auch zur Portoberechnung eingesetzt. Im Zusammenhang mit einer Dienstleistung des Nachladens einer Portotariftabelle werden keine besonderen Sicherheitsmaßnahmen ergriffen, obwohl auf der vorgenannten Tabelle die Richtigkeit der Portoberechnung beruht und obwohl das Meter ein Sicherheitsmodul enthält, wobei der Sicherheitsmodul neben einer Abrecheneinheit auch mit einer kryptografischen Einheit ausgestattet ist. Letztere dient aber nur zum Absichern der zu druckenden Postgebührendaten. Das Meter enthält außerdem eine Steuerung zum Steuern des Druckens und zum Steuern von peripheren Komponenten der Frankiermaschine. Die Base enthält eine Postguttransportvorrichtung und eine Tintenstrahl-Druckvorrichtung zum Drucken des Postwertstempels auf das Postgut. Ein Auswechseln des Druckkopfes ist unnötig, da der Tintentank vom Druckkopf getrennt angeordnet ist und ausgewechselt werden kann. Auch müssen keine besonderen Sicherheitsmaßnahmen für den Druckkopf oder für einen Schutz der Ansteuer- und Datensignale getroffen werden, wenn mit einem speziellen Piezo-Tintenstrahl-Druckkopf ein Sicherheitsabdruck mit einer Markierung gedruckt wird, die eine Nachprüfung der Echtheit des Sicherheitsabdruckes (US 6,041,704) gestattet. Neben der Dienstleistung des Nachladens einer Portotariftabelle und einer bekannten Dienstleistung eines Teleportodatenzentrums, wie die des Nachladens (US 5699415 bzw. EP 689170 A2) eines Guthabens, von welchem jeweils vor dem Ausdrucken der frankierte Postwert abgebucht wird, kann eine weitere Dienstleistung im Basetracking bestehen. Zur Vorbeugung vor einer eventuellen Fälschung durch Manipulation mittels der Druckeinheit, d.h. insbesondere dann, wenn die Base mit der Druckeinheit vom Meter abtrennbar ist, ist die Postbehörde über eine Information über den Standort der Druckeinheit interessiert, wenn die Base mit einem Meter wieder betrieben wird. Beim Basetracking erfolgt eine Freigabe nur derjenigen Druckeinheit, welche durch einen Identifikationscode von der Datenzentrale identifiziert werden kann (EP 1154381 A1).

**[0003]** In Frankiermaschinen der Anmelderin - beispielsweise in der mymail® und ultimail® - werden auch Bubble-jet-Druckköpfe im Druckmodul eingesetzt. Der Tintentank und Bubble-jet-Druckkopf sind in einer auswechselbaren Tintenkartusche integriert, wie es beispielsweise von den ½ Zoll Tintenkartuschen der Firma Hewlet Packard (HP) vorbekannt ist. Die Kontaktierung der elektrischen Kontakte des Druckkopfes der auswechselbaren Tintenkartusche kann über einen Connector eines handelsüblichen Pen-Driver-Board's der Firma HP erfolgen. Sowohl die Postbehörde als auch der Kunde haben ein verstärktes Interesse an einer hohen Auswertesicherheit der auf das Poststück aufgedruckten Markierung. Eine weitere Dienstleistung der Datenzentrale kann deshalb im Piraterieschutz bestehen. Über den Connector können zusätzliche den Piraterieschutz ermöglichende Daten, beispielsweise ein Code des Druckkopfes abgefragt und via Modem zur Datenzentrale gesendet werden. Die Datenzentrale nimmt dann einen Codevergleich mit einem in einer Datenbank gespeicherten Referenzcode vor und übermittelt eine Nachricht an die Frankiermaschine über das Ergebnis der Überprüfung (EP 1103924 A2).

An solchen Dienstleistungen ist das Sicherheitsmodul in unterschiedlicher Weise beteiligt, mindestens jedoch dann, wenn bei der Kommunikation sicherheitsrelevante Daten über einen ungesicherten Datenübertragungsweg mit einer entfernten Datenzentrale ausgetauscht werden müssen. Einerseits bietet das Metergehäuse bzw. das Gehäuse einer Frankiermaschine einen ersten Schutz vor Manipulationen in Fälschungsabsicht. Eine Kapselung des Sicherheitsmoduls mittels eines speziellen Gehäuses bietet einen zusätzlichen mechanischen Schutz. Ein solcher gekapselter Sicherheitsmodul entspricht den aktuellen postalischen Anforderungen und wird nachfolgend auch als postisches Sicherheitsgerät (PSD) bezeichnet. Die Guthabennachladung erfordert in einigen Ländern Sicherheitsmaßnahmen, die nur ein PSD liefern kann. Die Frankiermaschinen der Anmelderin werden zur telefonischen Guthabennachladung in an sich bekannter Weise mit einem Teleportodatenzentrum verbunden und lassen sich mit weiteren Geräten zu einem Frankiersystem erweitern.

**[0004]** Neben der positiven Fernwertvorgabe bei der oben genannte Guthabennachladung ist auch eine negative Fernwertvorgabe bei der Rückzahlung des verbliebene Restguthabens des Kunden bekannt (EP 717379 B1 bzw. US 6587843 B1).

**[0005]** Aus der US 5,233,657 ist bereits außerdem ein Laden von nicht einer Guthabennachladung dienenden Daten vor einer Inbetriebnahme einer Frankiermaschine bekannt.

**[0006]** Aus EP 1037172 A2 ist die Bereitstellung und Übermittlung eines maschinen- und kundenspeziellen Datensatzes von einer Datenzentrale an eine Frankiereinrichtung bekannt. Der Datensatz umfaßt mindestens temporär und lokal am Frankierort gültige Daten, die in der Datenzentrale zugeordnet zu einem Nummerncode in einer Datenbank abrufbar gespeichert sind. Der Kunde der eine vorinitialisierte Frankiereinrichtung über einen Händlervertrieb erstan-

den hat, soll damit in die Lage versetzt werden, die Frankiereinrichtung vollständig in Betrieb zu nehmen, ohne daß ein Kundendienst oder Servicetechniker gerufen werden muß und ohne einen Besuch des Postamtes. Die in der Datenzentrale gespeicherten Daten unterliegen alle der gleichen Sicherheitmaßnahme. Unabhängig davon werden in der Frankiermaschine die Graphikdaten ohne weitere Sicherheitmaßnahmen in einem Speicher des Mainboard's der Frankiermaschine gespeichert. Die Graphikdaten können ein Stempelbild, beispielsweise den Städtestempel betreffen.

**[0007]** Für das Wechseln von Werbeklischees wird bereits in der US 4,831,554 eine telefonische Kommunikation vorgeschlagen.

**[0008]** Im US 4,933,849 wird bereits ein datumsabhängiges Wechseln von Stempelbildern (mit Städtestempel und mit Wertstempel) mitgeteilt, welche zu einem früheren Zeitpunkt per Modem geladen wurden.

**[0009]** Gemäß der EP 780 803 A2 wird nach einer Initialisierung die Möglichkeit bereitgestellt, daß von einer Datenzentrale Neuigkeiten bzw. carrierspezifische Werbung bereitgestellt werden, wenn dazu ein Auftrag in der Datenzentrale vorliegt. Der Kunde muß dazu zuvor einen Vertrag mit dem Dienstleister bzw. Betreiber der Datenzentrale abgeschlossen haben.

**[0010]** Aus dem EP 1067482 ist es bereits bekannt, unterschiedliche Sicherheitsstufen den Elementen eines zu druckenden Druckbildes zuzuordnen. Diese unterschiedliche Sicherheitsstufen entsprechen der unterschiedlich vergebbaren Berechtigung, um einzelne der Elemente zu ändern. Zur Authorisierung und Nachladung der Elemente zur Änderung des Druckbildes werden Chipkarten eingesetzt, die die Elemente nach einer speziellen Hierarchie gültig machen.

**[0011]** Eine andere Dienstleistung eines Postbeförderers steht in Verbindung mit einer statistischen Erfassung der frankierten Post nach Statistikklassen (EP 892368 A2). Zur Speicherung von Daten über einen Benutzung eines Endgerätes sind auch aus EP 992947 A2 und EP 101383 A2 bereits Lösungen bekannt, nach welchen die Einträge nach Statistikklassen (Class of Mail) gespeichert werden, bis die entfernte Datenzentrale darauf zugreift, um das Benutzerprofil abzufragen bzw. zu ermitteln.

**[0012]** Es ist weiterhin bekannt, dass ein entferntes Datenzentrum via Modem Sicherheitsdaten mit einem Frankiersystem austauschen kann, das ein postisches Sicherheitsgerät (PSD) enthält. Solche Frankiersysteme der Anmelderin, sind beispielsweise unter den Marken-Namen jetmail® und ultimail® bekannt.

**[0013]** Der Erfindung liegt die Aufgabe zugrunde, eine Anordnung und ein Verfahren zu entwickeln, welches es gewährleistet, dass sowohl das Frankiersystem als auch das postalische Sicherheitsgerät Sicherheitsdaten speichern und weiterverarbeiten können.

**[0014]** Die Aufgabe wird mit den Merkmalen des Verfahrens nach Anspruch 1 und den Merkmalen der Anordnung nach Anspruch 5 gelöst.

**[0015]** Die Erfindung geht davon aus, dass eine vom Hersteller authorisiert betriebene Datenzentrale am sichersten gegenüber Manipulationen ist und somit auch eine Sicherheit für Ferndienstleistungen gegeben ist, welche ein Frankiersystem nutzen kann. Für die Zukunft ist nicht auszuschließen, dass neben einer Frankiermaschine auch weitere bzw. andere Geräte eines Frankiersystems ebenfalls Dienstleistungen einer entfernten Datenzentrale nutzen werden. Wenn nun nachfolgend von Sicherheitsinformationen gesprochen wird, die in Form von Datensätzen zu speichern und weiterzuverarbeiten sind, soll mit umfasst und berücksichtigt werden, dass die Sicherheitsanforderungen für die einzelnen Ferndienstleistungen in den Ländern sehr unterschiedlich sind oder zum Teil sogar fehlen.

**[0016]** Es wird vorgeschlagen, dass ein entferntes Datenzentrum eine Liste von Datensätzen aufweist, die Sicherheitsinformationen und eine zugeordnete Sicherheitskategorie enthalten. Letztere betrifft Informationen, die vom Sicherheitsmanagementsystem des Datenzentrum gemäß einer hinterlegten Sicherheitspolitik erfasst, verarbeitet, übertragen und bereitgestellt werden, mindestens zu Sicherheitsmaßnahmen und/oder zum Ort der Speicherung im Frankiersystem. Beide Informationen sind typischerweise in einer Datenbank eines Datenbankmanagementsystems (DBMS) abgelegt. Die Sicherheitspolitik definiert für jede Sicherheitskategorie:

a) daß ein Speicherort für einen gewünschten Datensatz innerhalb oder außerhalb des PSD's des Frankiersystems verwendet wird,
b) auf welche Weise die übertragenen Daten beim Datenaustausch gesichert werden, und/oder
c) welche Elemente des Frankiersystems durch die übertragenen Daten beeinflusst werden.

**[0017]** Der Datensatz kann im Ergebnis der Anforderung einer Dienstleistung vom entfernten Datenzentrum zum Frankiersystem übermittelt werden und enthält in seinem Kopfteil (header) die Informationen zur zugehörigen Sicherheitspolitik. Ein gewünschter mit einem zur jeweiligen Sicherheitskategorie zugehörigen Kopfteil ausgestatteter Datensatz kann mittels Übertragungsmittel, beispielsweise drahtlos oder via Modem, vom Datenzentrum vom Frankiersystem übermittelt und dort im PSD intern oder extern vom PSD gespeichert werden.

**[0018]** Ein Verfahren für ein servergesteuertes Sicherheitsmanagement von erbringbaren Dienstleistungen ist durch folgende Schritte gekennzeichnet:

A) Rufannahme bei Kommunikationsverbindung zwischen Frankiermaschine bzw. -system und Datenzentrum mit automatischer Einwahl durch die Frankiermaschine bzw. -system in das Datenzentrum und Empfangen der Anforderung einer gewünschten Dienstleistung mittels eines Servers des Datenzentrums,
B) Ermitteln der dieser Dienstleistung zugeordneten Sicherheitsdaten und Sicherheitskategorie im Datenbankmanagementsystem des Datenzentrums, Steuerung eines Selectors des Servers entsprechend der jeweiligen Sicherheitskategorie und Generierung eines Datensatzes mit Dienstleistungsdaten und Sicherheitsdaten durch den Server,
C) Auswahl des betreffenden logischen Kanals gesteuert durch den Selector des Servers des Datenzentrums und Übermitteln des Datensatzes entsprechend der gewünschten Dienstleistung über die bereits aufgebaute Kommunikationsverbindung zwischen Frankiermaschine bzw. -system und Datenzentrum,
D) Abbau der logischen Verbindung zur Frankiermaschine durch den Server des Datenzentrums, sobald die Dienstleistung beendet ist und Empfang einer entsprechenden von der Frankiermaschine bzw. - system ausgegebenen Bestätigung und
E) Warten auf den Empfang einer weiteren Dienstleistungsan-forderung mittels des Servers oder auf die Beendigung der Kommunikationsverbindung, wobei die Beendigung durch die Frankiermaschine bzw. -system erfolgt.

**[0019]** Als logischen Kanal wird entweder ein ungesicherter Kanal oder ein gesicherter Kanal automatisch gebildet, um einen ausgewählten Datensatz an die Frankiermaschine bzw. -system zu übermitteln.

**[0020]** Der betreffende Datensatz kann beim Betrieb des Frankiersystems auch wieder aufgerufen bzw. ausgelesen werden. Durch Angabe einer Sicherheitskategorie kann dabei adressiert werden, ob der gewünschte Datensatz aus dem Frankiersystem von innerhalb oder außerhalb des PSD's gelesen wird.

**[0021]** Die Anordnung zur Bereitstellung von Daten nach einem Sicherheitsmanagement für ein Frankiersystem geht davon aus, dass ein entferntes Datenzentrum die vom Frankiersystem angeforderten Datensätze bereitstellt, welche Anwendungsdaten und Daten zu Sicherheitsinformationen enthalten. Erfindungsgemäß ist vorgesehen, dass das Datenzentrum einen Server umfaßt, der mindestens mit einem Server-Kommunikationsmittel und mit einem Datenbankmanagementsystem in betriebsmäßiger Verbindung steht, dass die angeforderten Datensätze Daten für eine Sicherheitskategorie enthalten, wobei letztere mindestens Informationen zur Sicherheitsmaßnahme für einen Datenaustausch zwischen dem Frankiersystem und Datenzentrum und/oder zum Ort der Speicherung im Frankiersystem umfaßt, die vom Datenbankmanagementsystem des Datenzentrums gemäß einer hinterlegten Sicherheitspolitik erfasst, verarbeitet, übertragen und bereitgestellt werden, dass das Frankiersystem einen Mikroprozessor aufweist, der mindestens mit einem postalischen Sicherheitsgerät, mit einem ersten nichtflüchtigen Speicher und mit einem Kommunikationsmittel zum Empfang der angeforderten Datensätze verbunden ist, wobei der Mikroprozessor programmiert ist, die Daten für eine Sicherheitskategorie auszuwerten, um einen entsprechenden logischen Kanal zu bilden und den Ort der Speicherung der Anwendungsdaten im Frankiersystem festzustellen.

**[0022]** Es ist weiterhin vorgesehen, dass der der Mikroprozessor zur Speicherung der Anwendungsdaten programmiert ist und der erste nichtflüchtige Speicher oder ein zweiter nichtflüchtiger Speicher zur Speicherung der Anwendungsdaten ausgebildet ist, wobei nur der zweite nichtflüchtige Speicher Bestandteil des postalischen Sicherheitsgeräts (PSD) ist.
Außerdem kann ein dritter nichtflüchtiger Speicher extern der Frankiermaschine in einem anderen mit der Frankiermaschine verbundenen Postgerät angeordnet sein, der zur Speicherung der Anwendungsdaten ausgebildet ist.

**[0023]** Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1, Blockbild mit Baugruppen eines bekannten Frankiersystems,

Figur 2, Blockschaltbild für eine Anordnung zur Bereitstellung von Daten nach einem Sicherheitsmanagement für ein Frankiersystem,

Figur 3, Frankierabdruck nach DPAG-Anforderungen,

Figur 4, Flußplan für ein servergesteuertes Sicherheitsmanagement,

Figur 5, Detail des Blockschaltbildes der Steuereinheit des Servers.

**[0024]** Die Figur 1 zeigt ein Blockbild mit Baugruppen eines bekannten Frankiersystems 1, bestehend aus einer Frankiermaschine 2, an welche poststromabwärts eine Ablagebox 4 und poststromaufwärts eine automatische Zuführstation 7 angeschlossen ist. Bei dem Frankiersystem vom Typ Jetmail® wird ein Stapel 6 an auf der Kante ste-

henden Poststücken der zugeführt. Der Ablagebox 4 ist ein Stapel 5 an liegenden Poststücken entnehmbar. An eine erste und zweite Schnittstelle der Frankiermaschine 2 sind über Kabel 71 und 91 die automatische Zuführstation 7 und ein Personalcomputer 9 elektrisch angeschlossen. Die Frankiermaschine 2 ist mit einem entfernten Teleportodatenzentrum 8 zwecks Guthabennachladung und mit einem entfernten Servicecenter 11 kommunikativ verbindbar. Die Frankiermaschine 2 weist eine interne statische Waage 22 auf und ist mit Mitteln zur Portogebührenberechnung ausgestattet. Von dem entfernten Servicecenter 11 kann eine aktuelle Portogebührentabelle zur Frankiermaschine 2 bzw. zum Frankiersystem 1 übermittelt werden. Das Frankiersystem kann optional eine - nicht gezeigte - dynamische Waage aufweisen, welche zwischen der automatischen Zuführstation 7 und der Frankiermaschine 2 anordenbar ist.

Ein weiteres bekanntes Frankiersystems der Anmelderin vom Typ ultimail® entspricht prinzipiell ebenfalls dem in der Figur 1 gezeigten Blockbild mit dem Unterschied, dass der Stapel 6 an liegenden Poststücken der automatische Zuführstation 7 zugeführt wird und keine dynamische Waage nachrüstbar ist.

**[0025]** Während nach der bekannten Lösung (Figur 1) die angewählte Datenzentrale nur eine Dienstleistung bzw. nur eine minimale Anzahl an Dienstleistung ohne Sicherheitsmerkmal erbringen kann, sind mit einer erfindungsgemäßen Datenzentrale eine Anzahl an Dienstleistung mit Sicherheitsmerkmal lieferbar. Ein weiterer Vorteil ist die Vermeidung von mehreren Anrufen bei unterschiedlichen Datenzentralen mit unterschiedlichen Telefonnummern.

**[0026]** Die Figur 2 zeigt ein Blockschaltbild für eine Anordnung zur Bereitstellung von Daten entsprechend eines Sicherheitsmanagements für ein Frankiersystem. Neben den Baugruppen einer entfernten Datenzentrale 3 sind die Baugruppen eines Frankiersystems 1 dargestellt, das mindestens eine Frankiermaschine 2 und gegebenfalls eine statische Waage 22 aufweist. Auch sind ggf. weitere - nicht gezeigte - Postverarbeitungsstationen anschließbar, für die ebenfalls Dienstleistungen über die Frankiermaschine 2 bereitstellbar sind. Die statische Waage 22 ist vorzugsweise ein optionaler Bestandteil der Frankiermaschine 2. Die Frankiermaschine 2 umfaßt ein postalisches Meter 20, welches mindestens ein Kommunikationsmittel 21, ein Mainboard 24 und ein postalisches Sicherheitsgerät (PSD) 23 aufweist. Das Mainboard 24 ist mit einem ersten nichtflüchtigen Speicher 241 und mit einem Mikroprozessor 242 ausgestattet, der mit dem PSD 23, dem Speicher 241 und dem Kommunikationsmittel 21 in betriebsmäßiger Verbindung steht. Das Kommunikationsmittel 21 ist beispielsweise ein Modem, welches über ein Telefonnetz 12 mit einem Modem 31 des Datenzentrums 3 kommu-nikationsmäßig verbindbar ist. Damit sollen jedoch andere Kommunika-tionsmittel, wie beispielsweise drahtlose Sender-/Empfängergeräte, Mobilfunkgeräte, Bluetooth-, WAN-, LAN- u.a. Kommunikationsgeräte sowie andere Netze, wie Internet, Ethernet u.a. nicht ausgeschlossen werden. Vielmehr kommen eine Vielzahl an Kommunikationsmitteln und Netzen zur Datenübertragung in Betracht. Das PSD 23 ist - in nicht gezeigter Weise - über eine Schnittstelle am Mainboard 24 angeschlossen und enthält u.a. einen zweiten nichtflüchtigen Speicher 232 für Buchungsdaten und sicherheitsrelevante Daten für eine sichere Kommunikation mit der entfernten Datenzentrale. Weitere Einzelheiten zum PSD sind den Druckschriften EP 789333 B1, EP 1035513 A1, EP 1035516 A1, EP 1035517 A1, EP 1035518 A1, EP 1063619 A1, EP 1069492 A1 und EP 1278164 A1 entnehmbar.

Das Datenzentrum 3 umfaßt einen Server 30, der mit mindestens dem einen Server-Kommunikationsmittel 31 und mit einem Datenbankmanagementsystem (DBMS) 32 in betriebsmäßiger Verbindung steht. Das Server-Kommunikationsmittel 31 ist in einer - nicht gezeigten - Variante Bestandteil eines Kommunikations-Servers, der eine Vielzahl an separaten Anschlüssen an das Netz 12 ermöglicht. Auch das Datenbankmanagementsystem 32 kann in einem separaten Server oder innerhalb des bestehenden Servers 30 realisiert sein. Eine Steuereinheit 34 des Servers 30 ist mit einem Selector 341 und mit einem Mikroprozessor 342 ausgestattet, der mit dem Serversicherheitsmodul (SSM) 33, dem Selector 341 und dem mindestens einen Server-Kommunikationsmittel 31 in betriebsmäßiger Verbindung steht. Der Selector 341 ist hardware- und/oder softwaremäßig realisiert.

Die Vielzahl an separaten Anschlüssen des Kommunikations-Servers an das Netz 12 ermöglicht die Verbindung mehrerer Frankiermaschinen 2 bzw. Frankiersystemen 1 mit dem Datenzentrum 3 zu einem Sicherheitsmanagementsystem 10.

**[0027]** Das Datenzentrum 3 hat eine Liste von Datensätzen, die Sicherheitsinformationen und Informationen zur zugehörigen Sicherheitspolitik enthalten. Beide Informationen sind typischerweise in einer Datenbank eines Datenbankmanagementsystems (DBMS) 32 gespeichert. Jedem Datensatz mit den die Sicherheitsinformationen ist eine Sicherheitskategorie zugeordnet, beispielsweise eine Zahl auf der Skala 1 bis 10.

Durch Angabe der Sicherheitskategorie kann wahlweise adressiert werden, ob der gewünschte Datensatz mit dem Frankiersystem 1 von innerhalb oder außerhalb des PSD 23 ausgetauscht wird, auf welche Weise die übertragenen Daten beim Datenaustausch gesichert werden, oder welche Elemente des Frankiersystems die übertragenen Daten beeinflussen. Die Sicherheitspolitik definiert beispielsweise, welche Elemente des Frankierabdruckes durch die übertragenen Daten beeinflußt werden.

**[0028]** Es ist vorgesehen, dass der gewünschte Datensatz in einem innerhalb oder außerhalb des PSD's angeordneten nichtflüchtigen Speicher einer Frankiermaschine des Frankiersystems gespeichert wird. In Verbindung mit einer Ferndienstleistung kann es erforderlich sein, dass Daten aus dem Frankiersystem 1 ausgelesen und zum Datenzentrum 3 fernübertragen werden. Liest also das Datenzentrum 3 die Sicherheitsdaten aus dem Frankiersystem 1, so kann ebenfalls durch Angabe einer Sicherheitskategorie adressiert werden, ob der gewünschte Datensatz aus dem

Frankiersystem 1 von innerhalb oder außerhalb des PSD 23 gelesen wird. Die Steuereinheit 34 des Datenzentrums 3 sorgt dafür, dass Datensätze gemäss ihrer Sicherheitskategorie kommuniziert, gespeichert und verarbeitet werden. Dafür benutzt die Steuereinheit den Selector 341. Letzterer bietet die Möglichkeit, einen von zwei logischen Kommunikationskanälen zu wählen, um einen Speicher des Frankiersystems innerhalb oder außerhalb des PSD's zu adressieren. Jeder logische Kommunikationskanal wird durch individuelle Sicherheitsmechanismen und -parameter geschützt, die von einer Komponente der Steuereinheit 34 angewendet werden. Diese Komponente der Steuereinheit 34 wird auch als Serversicherheitsmodul (SSM) 33 bezeichnet. Für dessen Steuerung wird ebenfalls die Sicherheitskategorie eines Datensatzes berücksichtigt. Der Datensatz enthält in seinem Kopfteil (header) mindestens die Informationen zur zugehörigen Sicherheitspolitik.

Außer der Adressierung im Frankiersystem kann die Steuereinheit diese Informationen zur zugehörigen Sicherheitspolitik auch dafür verwenden, einen geeigneten Sicherheitsmechanismus zum Schutz während der Kommunikation und/oder während der anschliessenden Speicherung auszuwählen. Dies wird unten anhand einiger Beispiele gezeigt.

**[0029]** Die Figur 3 zeigt einen Frankierabdruck nach den Frankit-Anforderungen der Deutschen Post AG. Der Frankierabdruck weist links einen eindimensionalen Balkencode (1 D-Barcode) 15 für einen identcode auf, welcher weiter unten noch erläutert wird. Außerdem weist der Frankierabdruck im Wertabdruck einen zwei-dimensionalen Balkencode (2D-Barcode) 17 für die Verifizierung der ordnungsgemäßen Bezahlung der Poststückes-Beförderungsgebühr auf.

**[0030]** Die Figur 4 zeigt einen Flußplan für ein servergesteuertes Sicherheitsmanagement. Das Datenzentrum 3 wartet im Schritt A auf den Empfang einer Dienstleistungsanforderung. Für die Bearbeitung eines Ferndienstes (Remote Service) wählt sich die Frankiermaschine in Datenzentrum ein und fordert den gewünschten Ferndienst an. Nach dem Empfang der Dienstleistungsanforderung ermittelt das Datenzentrum im Schritt B in der Sicherheitspolitik dieses Ferndienstes die zu wählenden Sicherheitsmerkmale. Im Schritt C erfolgt eine Auswahl des logischen Kanals und eine Datensatzübermittlung vom Datenzentrum 3 zur Frankiermaschine 2 bzw. zum Frankiersystem 1. Dabei wird der logischen Kanal zum Speicher I des Mainbords oder zum Speicher II des PSD's ausgewählt. Die Datensatzübermittlung erfolgt über die bereits aufgebaute Modemverbindung vom Datenzentrum 3 zur Frankiermaschine 2 bzw. zum Frankiersystem 1. Im Schritt D erfolgt die Feststellung des Endes der angeforderten Dienstleistung. Sobald der Ferndienst beendet ist, baut der Server die logische Verbindung zur Frankiermaschine wieder ab und gibt der Frankiermaschine eine entsprechende Bestätigung. Im Schritt E wird festgestellt, ob die Kommmunikationsverbindung von der Frankiermaschine beendet worden ist. Ist das der Fall, dann wird der Punkt e erreicht. Anderenfalls wird auf einen Anfangspunkt a vor dem ersten Schritt A zurückverzweigt, zum Empfangen einer weiteren Dienstleistungsanforderung.

**[0031]** Beispiele für Sicherheitskategorien sind in der folgenden Tabelle aufgezeigt:

| Sicherheitskategorie | Schutzziel | Logischer Kanal | Speicher Ort | Komponenten des Frankiersystems | Ort im Abdruck |
|---|---|---|---|---|---|
| IdentCodes | Einmaligkeit/Eindeutigkeit | Plain Session | Mainboard NVM | Druckeransteuerung | 1D-Barcode ausserhalb Wertabdruck |
| Preis/Produkt Tabelle (PPT) | Datenintegrität/ ursprungsauthentikation/ Timeliness | Plain Session | Mainboard NVM | Preisberechnungsmodul | --- |
| Benutzerprofil Ursprungsauthentikation | Datenintegrität/ | Plain Session | Mainboard NVM | Aufzeichnung im NVM | --- |
| PVD | Schutz des Entgelts/ Datenintegrität/ Ursprungsauthentikation/ Empfängerdatenschutz | Secure Session | PSD NVM | Druckeransteuerung | 2D-Barcode im Wertabdruck |
| Withdraw | Schutz des Restguthabens | Secure Session | PSD NVM | Postalische Register, | --- |
| MAC Key | Verschluesselung | Secure Session | PSD NVM | Schlüsselspeicher, und Klicheé-Prüfung und Generierung | --- |

**[0032]** Die Tabellenspalten Schutzziel und logischer Kanal beschreiben für jede der in der ersten Spalte genannten Sicherheitskategorien, auf welche Weise die übertragenen Daten beim Datenaustausch gesichert werden. Die übrigen Tabellenspalten kennzeichnen der Speicherort, die beeinflußten Komponenten des Frankiersystems und wo im Abdruck der Einfluß sichtbar wird.

IdentCodes

**[0033]** IdentCodes sind Referenznummern, die Poststücke eindeutig bezeichnen, solange sie nicht erfolgreich zugestellt worden sind. Anhand seines IdentCodes kann ein Poststück in einem Briefverteilzentrum oder bei der Zustellung eindeutig wiedererkannt werden. Der IdentCode kann genutzt werden, um Tracking-Information über Poststücke bereitzustellen und für den Absender abfragbar zu machen. Jeder IdentCode darf während seiner Gültigkeitsdauer nur höchstens einmal (Einmaligkeit) für höchstens ein Poststück (Eindeutigkeit) vergeben werden. Als Speicherort wird der nichtflüchtige Speicher auf dem Mainboard der Frankiermaschine benutzt.

Preis-Produkt-Tabelle

**[0034]** Durch die übertragenen Daten werden ein Preisberechnungsmodul und der Abdruck beeinflußt. Eine Preis-Produkt-Tabelle (bzw. Portotariftabelle) hat ein Gültigkeitsdatum, ab dem sie gültig ist. Die Einträge einer Preis-Produkt-Tabelle sollten gegen Manipulation geschützt sein (Datenintegrität). Die Quelle einer Preis-Produkt-Tabelle sollte authorisiert sein (Ursprungsauthentifikation), und eine Preis-Produkt-Tabelle sollte spätestens an ihrem Gültigkeitstag bereitgestellt sein (Timeliness). Als Speicherort wird der nichtflüchtige Speicher auf dem Mainboard der Frankiermaschine benutzt.

Benutzerprofil

**[0035]** Die Benutzerprofile werden in der Maschine passiv aufgezeichnet und an das Datenzentrum übertragen. Die Einträge eines Benutzerprofils sollten gegen Manipulation geschützt sein (Datenintegrität). Alternativ genügt auch ein Integritätsschutz des Gesamtvolumens eines Benutzerprofils. Ausserdem sollte der Ursprung authentisiert sein (Ursprungsauthentikation). Dabei handelt es sich um einen speziellen Buchungswert, der im Rahmen einer speziellen Dienstleistung (Class of Mail) zur Datenzentrale übermittelt werden kann. Dieser spezielle Buchungswert ist einen gewöhnlich nicht ausdruckbarer MAC-gesicherter Summenwert aller summierten Postwerte, welche während einer Abrechnungsperiode frankiert wurden. Wird der vorgenannte Wert auf eine Postkarte ausgedruckt, dann spricht man auch von einer Abrechnungsfrankierung. Der vorgenannte MAC (Message Authorization Code) wird vorzugsweise in Form eines CryptoTags realisiert. Als Speicherort wird der nichtflüchtige Speicher auf dem Mainboard der Frankiermaschine benutzt. Nach dem Übertragen der CoM-Daten an das Datenzentrum wird der nichtflüchtige Speicher gelöscht, um Speicherplatz für neu aufgezeichnete Daten zu schaffen.

PVD

**[0036]** Die Daten, die während einer Guthabennachladung (Postage Value Download) übertragen werden, sind teilweise entgeltrelevant. Das heisst, wenn zum Beispiel ein Betrag von 50€ angefordert und im Datenzentrum verbucht und bestaetigt wird, so dürfen anschliessend im Sicherheitsmodul auch nur 50 € mehr Guthaben stehen. Würden dort 100 € zusätzlich ankommen, so wäre der Zusteller (also z.B. eine Postbehörde) um den Differenzbetrag von 50 € betrogen. Daher müssen die Nachrichten, die bei einem postage value download übertragen werden, gegen Manipulation geschützt sein und ihr jeweiliger Datenursprung muss authentisiert sein.
Zusätzlich kann hier auch der Datenschutz des Empfängers ein Schutzziel sein. Es soll für Aussenstehende z.B. nicht zu erkennen sein, welchen Betrag ein Kunde gerade vom Datenzentrum lädt. Um dieses Schutzziel zu erreichen, werden bestimmte Nachrichten zwischen Datenzentrum und Sicherheitsmodul verschlüsselt. Als Speicherort dient der nichtflüchtige Speicher des PSD's. Die beeinflussten Komponenten des Frankiersystems sind das PSD und dessen postalische Register.

Withdraw

**[0037]** Die Rückzahlung (Withdraw) des verbliebene Restguthabens des Kunden ist ein wesentliches Schutzziel beim Zurückgeben einer Maschine. Als Speicherort dient der nichtflüchtige Speicher des PSD's. Die beeinflussten Komponenten des Frankiersystems sind das PSD und dessen postalische Register.

MACKey

**[0038]** Wesentliches Schutzziel bei der Übertragung des MACKeys ist es, den Schlüssel gegenüber Aussenstehenden (einschliesslich dem Benutzer der Frankiermaschine) geheimzuhalten. Daher wird dieser Schlüssel vor der Übertragung verschlüsselt und erst im Sicherheitsmodul wieder entschlüsselt. Als Speicherort dient der nichtflüchtige Speicher des PSD's. Durch die übertragenen Daten werden Komponenten des Frankiersystems, wie PSD, Schlüsselspeicher, Cliché-Prüfung und -generierung in der Frankiermaschine beeinflusst.

**[0039]** Als logischer Kanal wird beispielhaft nur eine Klartextsitzung (plain session) von einer Sicherheitstextsitzung (secure session) unterschieden. Vereinfacht ist eine Klartextsitzung eine zuverlässige Datenverbindung über eine Telefonnetz, bei der die Daten ohne kryptographische Absicherung übertragen werden. Wenn nötig können fehlerkorrigierende Codes eingesetzt werden, um die Zuverlässigkeit der Übertragungsstrecke zu verbessern. Wegen der allgemeinen Bekanntheit erübrigt sich ein näheres Eingehen auf die Ausprägung eines Klartextkanals ein.

Eine Sicherheitstextsitzung ist eine zuverlässige Datenverbindung über ein Telefonnetz, bei der die Daten kryptographisch abgesichert übertragen werden. Wenn nötig, können auch hier fehlerkorrigierende Codes eingesetzt werden, um die Zuverlässigkeit der Übertragungsstrecke zu verbessern.

Der Selector steuert die Auswahl des Kanals (gesichert / ungesichert) zum Beispiel anhand einer Entscheidungsmatrix, die die entsprechende Behandlungsweise zum Beispiel für den angeforderten Dienst oder eine zur Übertragung anstehende Nachrichtenkennung vorhält. Die Entscheidungsmatrix kann zum Beispiel in Form einer oder mehrerer Datenbanktabellen ausgeprägt sein, so dass Änderungen der Kanalzuordnung im Betrieb des Servers dynamisch vorgenommen werden können.

**[0040]** Die Figur 5 zeigt ein Detail des Blockschaltbildes der Steuereinheit 34 des Servers. Der Selector 341 ist zum Beispiel eine Hardware- und/oder Software-Komponente, die dazu vorgesehen ist, einen Datensatz D1 ... Dn bis Dx aus einem Speicher 321 des Datenbankmanagementsystems 32 zu entnehmen und wenigstens teilweise solange zwischenzuspeichern, bis die Verarbeitung des Datensatzes durch den betriebsmäßig mit dem Selector 341 verbundenen Mikroprozessor 342 beendet ist. Der Datensatz D1 ... Dn bis Dx umfaßt mindestens erste Daten, d.h. einen adressierbaren Datenteil der zugeordnete Anwendungsdaten kennzeichnet und /oder umfaßt Anwendungsdaten AD direkt. Der Datensatz umfaßt weiterhin zugeordnete Sicherheitsdaten SD sowie eine Zuordnungsvorschrift, die auf weitere Schritte, Datentabellen bzw. auf eine Entscheidungsmatrix verweist, was den Mikroprozesser in die Lage versetzt, im Ergebnis einen ausgewählten logischen Kanal zu erzeugen. Diese Zuordnungsvorschrift wird auch als Sicherheitskategorie SC einer Sicherheitspolitik bezeichnet. Der Mikroprozesser 342 greift dazu auf ein in einem Programmspeicher 343 gespeichertes Programm zu und arbeitet das Programm und die gewünschten Protokolle ab. Die ersten Daten sind Anwendungsdaten AD des adressierten Datensatzes D1 und werden über einen Bus zum Mikroprozesser 342 oder beim kleinsten Level der Sicherheitskategorien direkt zur Ein/Ausgabe-Einheit 344 übermittelt. An letztere kann beispielsweise ein Modem angeschlossen sein. Bei einem höheren Level der Sicherheitskategorien, wenn der Selector weitere Sicherheitsdaten SD und Daten der Sicherheitskategorie SC zwischenspeichert, die eine vorbestimmte Sicherheitspolitik kennzeichnen, wird ein Interrupt I oder ein Steuersignal für den Mikroprozesser 342 erzeugt, der anhand der vom Selector dem Mikroprozesser übergebenen zweiten Daten CD die Art der weiteren Datenverarbeitung feststellt. Die zum Mikroprozesser 342 übermittelten ersten Daten können weiterbehandelt und dabei zum Beispiel verschlüsselt werden, d.h. entsprechend derjenigen Art weiterbehandelt werden, welche die übergebenen zweiten (Steuer)Daten CD mitteilt. Der in der Figur 5 gezeigte Datensatz D1 enthält Daten AD, SD und SC, wobei deren Reihenfolge anders realisiert werden kann, als gezeichnet wurde. Vorzugsweise enthält ein Datensatz Dn in seinem Kopfteil (header) mindestens die Sicherheitskategorie SC, d.h. Informationen zur zugehörigen Sicherheitspolitik. Der Selector ist vom Mikroprozessor zum Beispiel über einen Adressenbus ADD-BUS 345 adressierbar und die vom Selector übergebenen zweiten (Steuer)Daten CD können somit wiederholt vom Mikroprozessor abgefragt werden. Neben den angeforderten ersten Daten können vom Mikroprozessor auch die Daten zur Sicherheitskategorie SC via Ein/Ausgabe-Einheit 344 ausgegeben werden, um den Ort der Speicherung im Frankiersystem 1 zu kennzeichnen. Mit den Darlegungen zur Figur 5 soll nur eine Ausführungsvariante erläutert jedoch nicht ausgeschlossen werden, dass die Steuereinheit 34 des Servers teilweise auf andere Weise realisiert wird. Alternativ kann der Selector 341 als Bestandteil des Mikroprozessors 342 hardware- und/oder softwaremäßig ausgeführt werden.

**[0041]** Der Selector steuert den logischen Kanal durch die Verwendung von kryptographischen Verfahren auf Nachrichten oder Teilnachrichten (oder deren Auslassung); d.h. zu den Verfahren des technischen Transports der Information zum Beispiel durch eine Übertragung per Modem oder via einem anderen geeigneten Server-Kommunikationsmittel 31, werden mathematische Verfahren der Kryptographie angewandt.

Ein andere Möglichkeit besteht darin, die Zuordnung des Kanals fest zur Entwicklungszeit an die Dienste oder Datenfelder zu koppeln, d.h. fest zu kodieren, welcher Kanal zu verwenden ist. In diesem Fall ist der Selector eine logische Komponente des Ablaufprogramms im Server.

**[0042]** Im Allgemeinen werden sichere Kanäle gekennzeichnet durch Autentisierung von Nachrichten oder Teilnachrichten mittels Message Authentication Codes (MAC), die eine typischerweise verschlüsselte (kryptographische) Prüf-

summe enthalten. Verfahren wie zum Beispiel HMAC-SHA1 leisten dies. Weiterhin können Nachrichten oder Teilnachrichten mit Hilfe von Chiffrierverfahren (3DES, AES) verschlüssselt werden. Das verwendete Schlüsselmaterial für die Authentisierung und Verschlüsselung wird statisch gewählt und zum Beispiel während der Produktion dem Dienstgerät eingeprägt oder auf Basis eines Schlüsselaustauschverfahrens für jede Sitzung neu erzeugt.

**[0043]** Die Identität der beiden Kommunikationspartner kann z.B. durch digitale Signaturen sicher bestimmt werden, die im Sinne einer gemeinsamen Public Key Hierarchie miteinander verknüpft sind. Beide Entitäten sind in diesem Falle mit einer eigenen Schlüsselidentität ausgestattet.

**[0044]** Die kryptographischen Merkmale eines sicheren Kanals werden detalliert zum Beispiel in der nicht vorveröffentlichten Deutschen Patentanmeldung 10 2004 032 057.8 unter dem Titel: Verfahren und Anordnung zum Generieren eines geheimen Sitzungsschlüssels, insbesondere anhand der Figuren 3 und 4, beschrieben.

**[0045]** Die im Rahmen einer Ferndienstleistung von dem Datenzentrum gelieferten Sicherheitsinformationen können sowohl von der Frankiermaschine als auch von anderen Geräten eines Frankiersystems genutzt werden.

**[0046]** Unter einem Frankiersystem kann auch ein sogenannter PC-Frankierer verstanden werden, welcher mindestens aus einem Personalcomputer mit PSD und einem handelsüblichen Bürodrucker besteht.

**[0047]** In einer anderen - in der Figur 2 nicht gezeigten - Variante wird das Datenbankmanagementsystem (DBMS) 32 innerhalb des Servers 30 realisiert. Außerdem ist vorgesehen, dass der Selector 341 als Bestandteil des Mikroprozessors 342 hardware- und/oder softwaremäßig ausgeführt ist.

**[0048]** Die Erfindung ist nicht auf die vorliegende Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die - vom gleichen Grundgedanken der Erfindung ausgehend - von den anliegenden Ansprüchen umfaßt werden.

## Patentansprüche

1. Verfahren für ein servergesteuertes Sicherheitsmanagement von erbringbaren Dienstleistungen, **gekennzeichnet durch** die Schritte:

   A) Rufannahme bei Kommunikationsverbindung zwischen Frankiermaschine (2) bzw. -system (1) und Datenzentrum (3) mit automatischer Einwahl **durch** die Frankiermaschine (2) bzw. -system (1) in das Datenzentrum (3) und Empfangen der Anforderung einer gewünschten Dienstleistung Dienstleistung mittels eines Servers (30) des Datenzentrums (3),
   B) Ermitteln der dieser Dienstleistung zugeordneten Sicherheitsdaten und Sicherheitskategorie im Datenbankmanagementsystem (32) des Datenzentrums (3), Steuerung eines Selectors (341) des Servers (30) entsprechend der jeweiligen Sicherheitskategorie und Generierung eines Datensatzes mit Dienstleistungsdaten und Sicherheitsdaten **durch** den Server (30),
   C) Auswahl des betreffenden logischen Kanals gesteuert **durch** den Selector (341) des Servers (30) des Datenzentrums und Übermitteln des Datensatzes entsprechend der gewünschten Dienstleistung über die bereits aufgebaute Kommunikationsverbindung zwischen Frankiermaschine (2) bzw. -system (1) und Datenzentrum (3),
   D) Abbau der logischen Verbindung zur Frankiermaschine **durch** einen Server (30) des Datenzentrums (3), sobald die Dienstleistung beendet ist und Empfang einer entsprechenden von der Frankiermaschine (2) bzw. -system (1) ausgegebenen Bestätigung und
   E) Warten auf den Empfang einer weiteren Dienstleistungsanforderung mittels des Servers (30) oder auf die Beendigung der Kommunikationsverbindung, wobei die Beendigung **durch** die Frankiermaschine (2) bzw. -system (1) erfolgt.

2. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet, dass** in Verbindung mit einer Ferndienstleistung für ein Frankiersystem (1) Daten ausgetauscht und vom oder zum Datenzentrum (3) fernübertragen werden, wobei durch Angabe einer Sicherheitskategorie wahlweise adressiert werden kann, welcher Speicherort für einen gewünschten Datensatz innerhalb oder außerhalb des PSD's (23) des Frankiersystems (1) verwendet werden soll.

3. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet, dass** in Verbindung mit einer Ferndienstleistung für ein Frankiersystem (1) Daten ausgetauscht und vom oder zum Datenzentrum (3) fernübertragen werden, wobei durch Angabe einer Sicherheitskategorie wahlweise adressiert werden kann, auf welche Weise die übertragenen Daten beim Datenaustausch gesichert werden.

4. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet, dass** in Verbindung mit einer Ferndienstleistung für ein Frankiersystem (1) Daten ausgetauscht und vom oder zum Datenzentrum (3) fernübertragen werden, wobei durch

Angabe einer Sicherheitskategorie wahlweise adressiert werden kann, welche Elemente des Frankiersystems durch die übertragenen Daten beeinflusst werden.

**5.** Anordnung zur Bereitstellung von Daten nach einem Sicherheitsmanagement für ein Frankiersystem (1), wobei ein entferntes Datenzentrum (3) die vom Frankiersystem (1) angeforderten Datensätze bereitstellt, welche Anwendungsdaten (AD) und Daten (SD) zu Sicherheitsinformationen enthalten, **dadurch gekennzeichnet, dass** das Datenzentrum (3) einen Server (30) umfaßt, der mindestens mit einem Server-Kommunikationsmittel (31) und mit einem Datenbankmanagementsystem (32) in betriebsmäßiger Verbindung steht, dass die angeforderten Datensätze Daten (SC) für eine Sicherheitskategorie enthalten, wobei letztere mindestens Informationen zur Sicherheitsmaßnahme für einen Datenaustausch zwischen dem Frankiersystem und Datenzentrum (3) und/oder zum Ort der Speicherung im Frankiersystem (1) umfaßt, die vom Datenbankmanagementsystem (32) des Datenzentrums (3) gemäß einer hinterlegten Sicherheitspolitik erfasst, verarbeitet, übertragen und bereitgestellt werden, dass das Frankiersystem (1) einen Mikroprozessor (242) aufweist, der mindestens mit einem postalischen Sicherheitsgerät (23) einem ersten nichtflüchtigen Speicher (241) und einem Kommunikationsmittel (21) zum Empfang der angeforderten Datensätze verbunden ist, wobei der Mikroprozessor programmiert ist, die Daten (SC) für eine Sicherheitskategorie auszuwerten, um einen entsprechenden logischen Kanal zu bilden und den Ort der Speicherung der Anwendungsdaten (AD) im Frankiersystem (1) festzustellen.

**6.** Anordnung, nach Anspruch 5, **dadurch gekennzeichnet, dass** der der Mikroprozessor zur Speicherung der Anwendungsdaten (AD) programmiert ist und der erste nichtflüchtige Speicher (241) oder ein zweiter nichtflüchtiger Speicher (232) zur Speicherung der Anwendungsdaten (AD) ausgebildet ist, wobei nur der zweite nichtflüchtige Speicher (232) Bestandteil des postalischen Sicherheitsgeräts (23) ist.

**7.** Anordnung, nach den Ansprüchen 5 bis 7, **dadurch gekennzeichnet, dass** ein dritter nichtflüchtiger Speicher extern der Frankiermaschine in einem anderen mit der Frankiermaschine verbundenen Postgerät angeordnet und zur Speicherung der Anwendungsdaten (AD) ausgebildet ist.

**8.** Anordnung, nach Anspruch 5, **dadurch gekennzeichnet, dass** eine Steuereinheit (34) des Servers (30) mit einem Selector (341) und mit einem Mikroprozessor (342) ausgestattet ist, der mit einem Serversicherheitsmodul (33), dem Selector (341) und dem Server-Kommunikationsmittel (31) in betriebsmäßiger Verbindung steht, wobei die Liste in einer Datenbank des Datenbankmanagementsystems (32) gespeichert in der Form vorliegt, dass jedem Datensatz eine Sicherheitskategorie zugeordnet ist, wobei die Sicherheitspolitik für jede Sicherheitskategorie definiert, ob der betreffende Datensatz zum Frankiersystems (1) übertragen und im postalischen Sicherheitsgerät (23) des Frankiersystems (1) gespeichert wird oder zum Frankiersystem (1) übertragen und dort aber außerhalb des postalischen Sicherheitsgeräts (23) gespeichert wird.

**9.** Anordnung, nach Anspruch 8, **dadurch gekennzeichnet, dass** das Server-Kommunikationsmittel (31) Bestandteil eines Kommunikations-Servers ist, der eine Vielzahl an separaten Anschlüssen an ein Netz (12) ermöglicht und dass zwischen dem Datenzentrum (3) und dem Frankiersystem (1) das Server-Kommunikationsmittel (31) und ein weiteres Übertragungsmittel (21) angeordnet sind, über welche ein mit betreffender Sicherheitskategorie ausgestatteter Datensatz bei Bedarf übermittelbar ist.

**10.** Anordnung, nach Anspruch 9, **dadurch gekennzeichnet, dass** das Server-Kommunikationsmittel (31) und das Übertragungsmittel (21) des Frankiersystems (1) ein drahtlos arbeitendes Übertragungsmittel ist.

**11.** Anordnung, nach Anspruch 9, **dadurch gekennzeichnet, dass** das Server-Kommunikationsmittel (31) und das Übertragungsmittel (21) des Frankiersystems (1) ein Modem ist.

**12.** Anordnung, nach Anspruch 8, **dadurch gekennzeichnet, dass** das Datenbankmanagementsystem (32) in einem separaten Server realisiert ist.

**13.** Anordnung, nach Anspruch 8, **dadurch gekennzeichnet, dass** das Datenbankmanagementsystem (32) innerhalb des bestehenden Servers (30) realisiert ist.

**14.** Anordnung, nach Anspruch 8, **dadurch gekennzeichnet, dass** der Selector (341) hardware- und/oder softwaremäßig realisiert ist.

**15.** Anordnung, nach Anspruch 14, **dadurch gekennzeichnet, dass** der Selector (341) als Bestandteil des Mikropro-

zessors (342) ausgeführt ist.

**Prior Art**

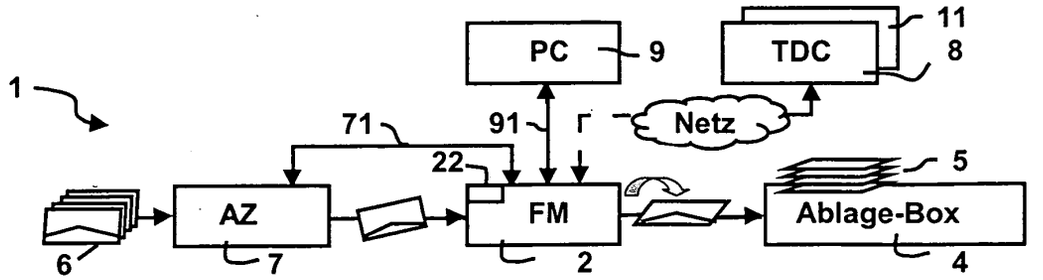


Fig. 1

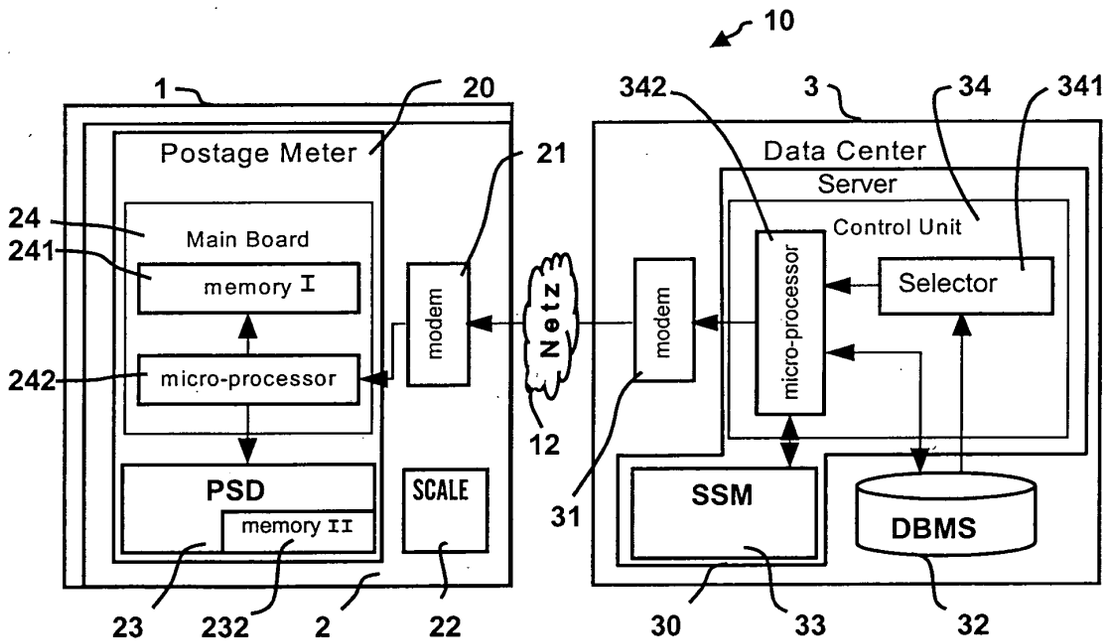


Fig. 2

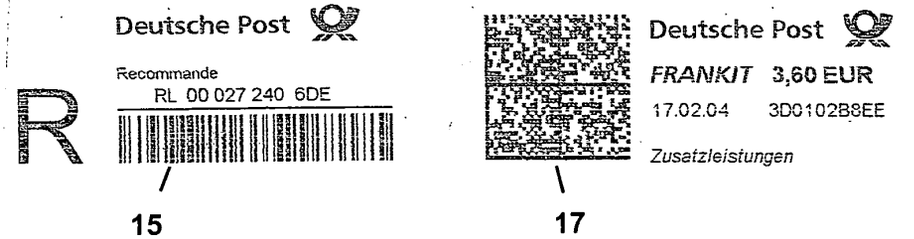


Fig. 3

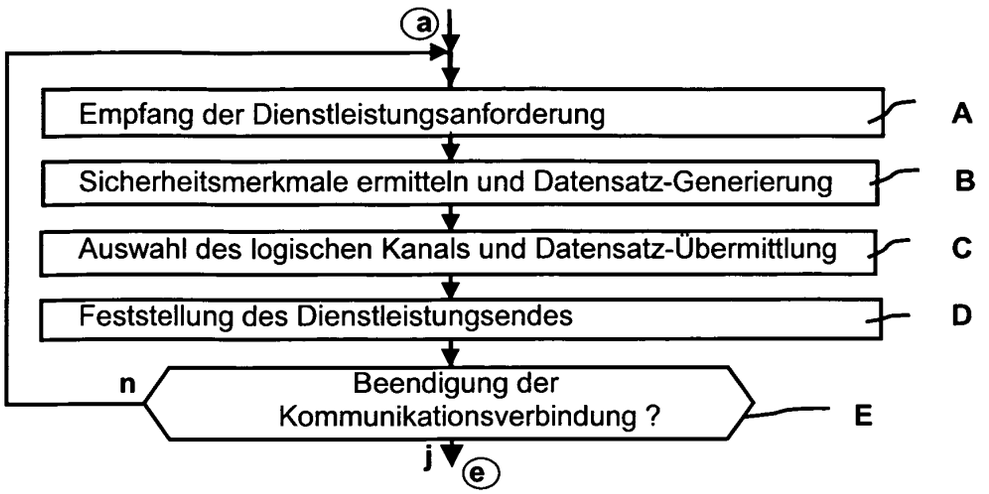
a
Empfang der Dienstleistungsanforderung
A
Sicherheitsmerkmale ermitteln und Datensatz-Generierung
B
Auswahl des logischen Kanals und Datensatz-Übermittlung
C
Feststellung des Dienstleistungsendes
D
n
Beendigung der Kommunikationsverbindung ?
E
j
e

Fig. 4

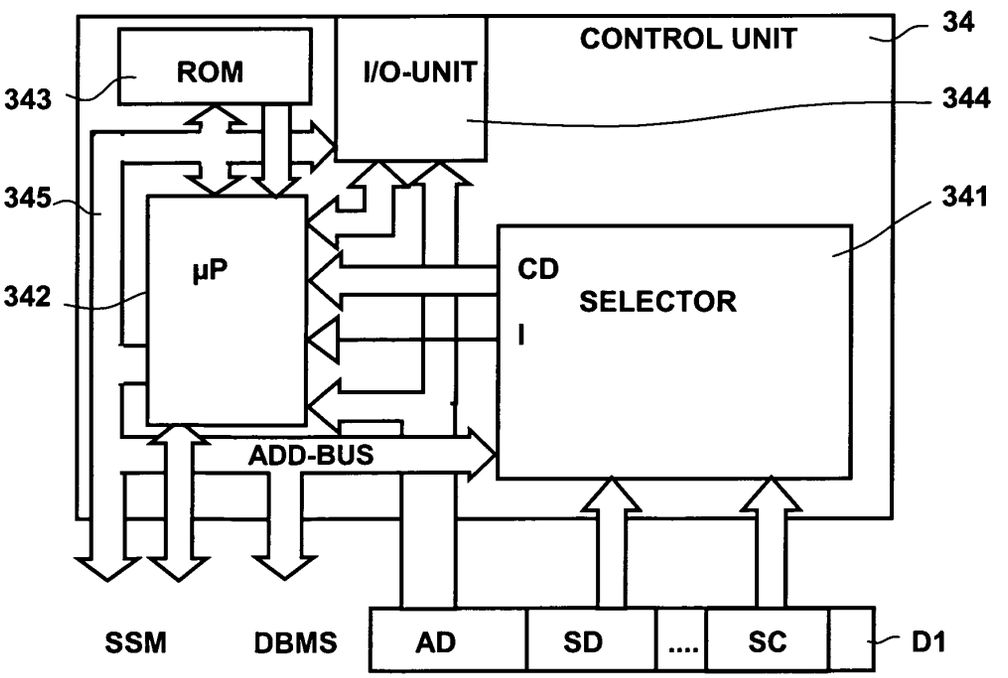
CONTROL UNIT
34
ROM
I/O-UNIT
343
344
345
341
µP
342
CD
SELECTOR
I
ADD-BUS
SSM
DBMS
AD
SD
....
SC
D1

Fig. 5