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

(11) **EP 2 058 769 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
13.05.2009 Patentblatt 2009/20

(51) Int Cl.:
G07B 17/00 *(2006.01)*

(21) Anmeldenummer: **08017285.1**

(22) Anmeldetag: **01.10.2008**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA MK RS

(30) Priorität: **02.11.2007 DE 102007052458**

(71) Anmelder: **Francotyp-Postalia GmbH**
16547 Birkenwerder (DE)

(72) Erfinder: **Bleumer, Gerrit, Dr.**
16552 Schildow (DE)

(54) Frankierverfahren und Postversandsystem mit zentraler Portoerhebung

(57) Ein Postversandsystem mit zentraler Portoerhebung gestattet eine Verlagerung des Nachweises der Abrechnung der Postbeförderdienstleistung vom Kunden auf den Postbeförderer und basiert auf einer Gerätekennung, welche eine Unterscheidung der Frankiergeräte voneinander und eine korrekte Zuordnung der Abrechnung der verbrauchten Portoge-bühren zum Kunden erlaubt. Das Frankierverfahren umfasst die Schritte: Erzeugen einer Frankierung (1), Befördern und Einliefern (2) von Poststücken in ein Briefzentrum des Postbeförderers nach dem Frankieren, Abtastung (3) des Frankierbilds im Briefzentrum des Postbeförderers und Weiterverarbeitung von abgetasteten Daten in einer Routine (300) beim Postbeförderer, wobei eine Dekodierung (301) der abgetasteten Daten, eine Ermittlung des jeweiligen Absenders (302), eine Ermittlung (303) der jeweiligen Portogebühr, eine Sicherheitsüberprüfung (304) jedes Frankier-bildes und eine zentrale Buchung (306) der Portogebühr auf ein Konto des Absenders erfolgt sowie Transport (4) und Auslieferung (5) von Poststücken an die Empfänger oder Aussonderung von Poststücken im Briefzentrum, wenn die Weiterverarbeitung der abgetasteten Daten in der Routine (300) nicht möglich ist. Beim Erzeugen einer Frankierung (1) wird für jedes Frankierbild ein neuer Frankierbildschlüssel aus einem Vorgänger des Frankierbildschlüssels nach einem ersten Krypto-Algorithmus abgeleitet und ein Integritäts-Checkcode M basierend auf dem neuen Frankierbildschlüssel, einer Schlüsselgenerationsnummer i, einer Gerätekennung g des Frankiergeräts und basierend auf einem zweiten Krypto-Algorithmus erzeugt. Bei der Sicherheitsüberprüfung (304) wird ein Vergleichs-Integritäts-Checkcode zum Vergleich mit dem aufgedruckten Integritäts-Checkcode gebildet. Die Gebühren werden zur zentralen Buchung erfasst und zeitlich entkoppelt von deren Buchung dem Absender der Poststücke in Rechnung gestellt. Beim Prüfen der Frankierbilder erfolgt eine Fehlerbehandlung.

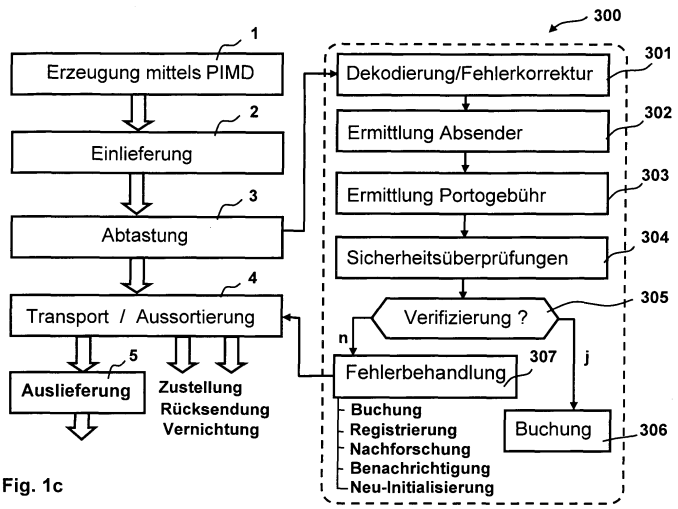

Fig. 1c

EP 2 058 769 A1

Beschreibung

[0001] Die Erfindung betrifft ein Frankierverfahren und Postversandsystem mit zentraler Portoerhebung. Das Postversandsystem umfasst ein Datenzentrum eines Postbeförderers, ein Datenzentrum eines Betreibers und mindestens ein Frankiergerät. Der Postbeförderer trans-portiert die vom Frankiergerät frankierten Poststücke zum Briefzentrum. Zweck der Erfindung ist es, mit einfach aufgebauten Frankiergeräten ein sicheres Postversandsystem zu schaffen.
Bisher fehlte eine einfache Lösung, die beim Absender entweder einen Personalcomputer (PC) mit Drucker oder ein spezielles sehr einfach zu bedienendes Frankiergerät voraussetzt, dabei aber weder eine Online-Verbindung für jede Frankierung noch ein Sicherheitsmodul erfordert. Eine solche Offline Lösung ohne Sicherheitsmodul wird möglich, wenn die Postbeförderer die Portoermittlung und -abrechnung im Rahmen ihrer Diensterbringung vornehmen. Das heißt, während die Postsendungen im Briefzentrum des Postbeförderers gelesen werden und die Zieladresse ermittelt wird, erhebt eine geeignete Software das erforderliche Porto für die Postsendung. Sie übermittelt einen Datensatz aus Absender und Portobetrag an die Kundenkontenverwaltung des Postbeförderers, die ihn auf ein Kundenkonto des Absenders bucht. Die Abrechnung mit dem Kunden (Absender) kann zeitlich entkoppelt von der Buchung erfolgen.

[0002] Wir nennen dies Verfahren "zentrale Portoerhebung", weil die erforderlichen Portowerte zentral in den Briefzentren des Postbeförderers erhoben werden, und nicht, wie bei der herkömmlichen "dezentralen Portoerhebung", von den Absendern vor Einlieferung in Postämtern oder Briefkästen.

[0003] Es wurde aus der DE 38 40 041 A1 eine Anordnung zum Frankieren von Postgut, mit einer Frankiereinrichtung bekannt, deren Wertdruck durch einen Rechner einer zentralen Verrechnungsstelle abgebucht wird, mit einem Speicher, dessen Inhalt bei jedem Frankiervorgang erhöht wird und dessen Inhalt durch den Benutzer der Frankiereinrichtung ablesbar ist. Der Rechner wird nach Deckungsprüfung zur Abrechnung des Wertdrucks mit einem Giro-Rechner der Postbehörde verbunden, welcher ein Postgirokonto des Eigentümers der Frankiereinrichtung führt. Der Giro-Rechner gibt jeden einzelnen Wertdruck nach Deckungsprüfung und Abbuchung frei.
Das heißt, bevor die Postsendungen zum Briefzentrum des Briefbeförderers befördert und dort gelesen werden sowie die Zieladresse ermittelt wird, wird das erforderliche Porto für die Postsendung bestimmt und bezahlt. Bei diesem Postversandsystem mit zentraler Portoerhebung ist keine nachträgliche Bezahlung der Dienstleistung vorgesehen.
Um sowohl für den Postbeförderer als auch für den Benutzer eine größtmögliche Sicherheit hinsichtlich der Portoerhebung zu erzielen, ist der Inhalt des als Stückzahl und Summenspeicher ausgebildeten Speichers durch den Benutzer und durch den Rechner der Verrechnungsstelle lediglich lesbar und ist die Verbindung des Rechners der Verrechnungsstelle mit der Frankiereinrichtung als ständig in Betrieb befindliche Standleitung (TEMEX) ausgebildet.

[0004] Für kleine SOHOs (Small Office Home Office) sind am Markt noch immer keine wirklich angemessenen elektronischen Frankierlösungen erhältlich.
Es gibt online Lösungen, die beim Absender einen PC mit Drucker voraussetzen und bei jeder Frankierung eine Datenverbindung zum Postage Provider aufbauen.

[0005] Weiterhin gibt es offline Lösungen, die spezielle Frankiergeräte mit Sicherheitsmodul voraussetzen, in denen vorausbezahlte Portowerte manipulationssicher verwaltet werden (Gerrit Bleumer: Electronic Postage Systems; Springer-Verlag, New York, 2007, Kapitel 4.1 Basic Cryptographic Mechanisms, Seite 91).

[0006] In den Postmärkten weltweit ist es bis heute weit verbreitet, die Portogebühren dezentral am Eingang des postalischen Transportkanals zu erheben, zum Beispiel durch Briefmarkenverkauf oder Annahme von DV-freigemachten Sendungen in Postämtern und Postagenturen, durch Frankiermaschinen oder Frankierservicestationen. Für den Absender werden Portogebühren fällig, wenn die entsprechenden Postwertzeichen zum Beispiel in Form von Briefmarken, DV-Aufdrucken und Einlieferungslisten, Frankierabdrucken bei Frankiermaschinen und PC-Frankierlösungen und Frankierservice, usw. bestellt oder geliefert werden.
In dem Maße, wie Postbeförderer dazu übergehen, die bearbeitete Post zwecks Adresserkennung und Zusatzdienstleistungen wie Sendungsverfolgung automatisiert vollständig zu erfassen, ergibt sich die Möglichkeit, auch die fälligen Portogebühren erst bei der Bearbeitung im Briefzentrum zu erheben. Bei diesem Abrechnungsmodell müssen Kunden keine Portogebühren im Voraus entrichten, sondern erhalten z.B. am Monatsende eine Rechnung über ihre transportierten Sendungen. Bei Bedarf können Einzeltransportnachweise bestellt werden, ähnlich wie dies heute für Telekommunikationsrechnungen üblich ist.
Im Fall von Frankiermaschinen bedeutet dieses Abrechnungsmodell, dass keine Guthabennachladungen mehr nötig sind, sondern dass die Frankiermaschine nur dazu dient, das gewünschte postalische Produkt zu erfassen und einen entsprechenden Frankierabdruck zu berechnen und aufzubringen.
Wir nennen dieses Abrechnungsmodell "Zentrale Portoerhebung" im Gegensatz zur bisher üblichen "Dezentralen Portoerhebung". Zentrale Portoerhebung führt zu einer verzögerten Zahlungsforderung an den Absender. Dennoch wäre die Bezeichnung "postpay" oder "pay later" nicht charakteristisch, denn auch bei herkömmlicher dezentraler Portoerhebung kann zum Beispiel durch Lastschriftverfahren oder Kreditkartenzahlung die effektive Belastung des Kundenkontos de facto später erfolgen, als die postalische Dienstleistung erbracht wird.

[0007] Aus dem US 7,110,576 B2 sind ein System und ein Verfahren zur Authentifikation eines Postabsenders bekannt,

der eine Postsendung unterschreibt. Eine handgeschriebene Unterschrift stellt eine biometrische Identität des Absenders dar, welche der Absender auf eine Postsendung aufbringt, indem er eine handschriftliche Unterschrift mithilfe eines Digitalisierstift leistet. Ein Postbeförderer scannt anschließend die Unterschrift und lässt von einem zentralen Ferndienst überprüfen, ob die gelesene Unterschrift gültig ist. Bei dem Ferndienst ist auch der Digitalisierstift ursprünglich mittels Unterschriftenprobe registriert worden. In einer speziellen Ausprägung schreibt der Digitalisierstift eine Information in ein Radio Freqency Identity Device (RFID), wobei das RFID-Schildchen auf der Postsen-dung angebracht ist. Im Ergebnis der Überprüfung des biometrischen Merkmals auf hinreichende Ähnlichkeit eines vom behaupteten Absender geleisteten biometrischen Referenzmerkmals erhält der Postbeförderer eine Antwort und bringt das Ergebnis auf der Postsendung auf, sofern es positiv ist. In nachteiliger Weise erlaubt eine biometrische Absenderkennung keine eindeutige Geräte-kennung. Es ist keinerlei Integritäts-Checksumme über die Absenderkennung vorgesehen. Außerdem wäre es aufwändig sicherzustellen, dass in der Postsendung besondere technische Merkmale wie z.B. ein RFID-Tag vorhanden sind.

[0008] Aus der US 6,801,833 B2 ist ein System zur Identifikation von Postsendungen mittels RFID bekannt. Die Postsendungen werden in Stapeln gebündelt, die wiederum in Containern zusammengefasst werden, die selbst in Lieferwagen transportiert werden. Jeder Behälter ist mit einem eigenen RFID-Tag ausgerüstet, der alle enthaltenen Behälter bzw. Postsendungen auflistet, so dass an definierten Punkten des Posttransportweges jeder Behälter und jedes Poststück automatisch erfasst und durch einen Zentralcomputer verfolgt werden kann. Das RFID-Tag kann folgende Informationsmerkmale tragen: Adressat, Absender, Sendungs-ID, Integritätschecksumme einer Sendungs-ID, Sendungswert oder verschlüsselter Sendungswert. Dadurch ergibt sich, dass Postsendungen mit eindeutigen Absenderkennungen markiert werden, jedoch in anderer Form und zusammen mit anderen Merkmalen als denen der vorliegenden Erfindung. Der Absender kann eine größere Menge Postsendungen einliefern, indem er gleichzeitig eine Einlieferungsliste (mailing manifest) bereitstellt. Bei manifest mailing Systemen ermittelt nicht der Absender, sondern das Einlieferungspostamt den erforderlichen Portobetrag aufgrund der Einlieferungsliste. Auf den einzelnen Postsendungen muss daher nur ein Merkmal angebracht sein, das einen Bezug zur zugehörigen Einlieferungsliste herstellt (permit imprint). In unüblicher Weise ist dazu ein RFID-Tag vorgesehen. Eine Absender-ID ist nur in der Form als RFID-Informationsmerkmal vorgesehen. Eine mailing-ID identifiziert das Poststück einzigartig, wobei die mailing-ID aus folgenden Teilen bestehen kann: Absenderkontonummer, Datum, tray-ID, piece-ID in mailtray, e-mail Adresse des Absenders, Sendungswert, Sendungskategorie und Postbeförderer. Für die Kennungen der Postsendungen und aller Behälter kann ein fehlerkorrigierender Code (CRC) oder eine digitale Signatur oder ein Message Authentication Code (MAC) erwendet werden. Die Integritätschecks sollen verhindern, dass aufgrund von technischen Fehlern (fehlerkorrigierender Code) oder betrügerischer Manipulation (digitale Signatur oder Message Authentication Code) Postsendungen einer falschen Postablage (mail tray) zugeschlagen oder eine falsche Postablage einer falschen Palette, usw. zugeordnet werden. Auf den einzelnen Postsendungen muss daher ein RFID-Tag angebracht sein, jedoch ist es bei der Vielzahl von Absendern schwierig zu sichern, dass für alle die gleichen Bedingenden herrschen. Das ist kaum möglich, wenn der Absender den RFID-Tag am Poststück anbringt. Ein falscher Klebstoff kann dazu führen, dass sich ein RFID-Tag ablöst. Für den Absender ist es nicht ohne weiteres möglich, Informationen aus dem RFID-Tag auszulesen. Um diese Informationen im RFID-Tag zu speichern, wären beim Absender ein Einsatz von speziellen Geräten erforderlich.

[0009] Aus dem US 5,612,889 A ist ein Postverarbeitungssystem mit eindeutiger Poststückautorisierung bekannt, die vor dem Eintritt eines Poststücks in den Bearbeitungsstrom eines Posttransportdienstes zugeordnet wird. Auf Postsendungen wird eine eineindeutige Sendungs-ID aufgeprägt, die als Index in eine Einlieferungsliste dient, die die Zustelladressen aller eingelieferten Postsendungen enthält. Dadurch wird eine Adresskorrektur auf Basis der Einlieferungslisten ermöglicht. Eine Einlieferung von Postsendungen wird vorab elektronisch beim Postbeförderer angemeldet. Dafür erstellt der Absender eine elektronische Einlieferungsliste, die er kryptographisch gesichert an den Postbeförderer überträgt. Der Briefbeförderer wertet die Informationen über die erwarteten Postsendungen und ihre Zustelladressen aus, korrigiert ggfs. Adressen und ermittelt die erforderlichen Portogebühren, und stellt sie dem Absender anschließend in Rechnung. Der Postbeförderer schickt dem Absender eine Liste von Sendungs-IDs zurück, die dieser auf seine Postsendungen aufdruckt. Anschließend liefert der Absender seine Postsendungen beim Briefbeförderer ein. Die Einlieferungsliste liegt dem Postbeförderer zu diesem Zeitpunkt bereits vor. Die SendungsID bezeichnet für sich allein keinen Absender, sondern sie ist lediglich ein Index in einer Einlieferungsliste. Eine Bedeutung erhält diese SendungsID erst in Verbindung mit der Einlieferungsliste. Die SendungsID ist jedoch keine eindeutige Kennung, die auf all den Postsendungen eines Frankiergeräts verwendet werden und den Absender identifizieren kann.

[0010] Aus dem EP 710 930 B1 ist bekannt, dass den Postsendungen eine eineindeutige SendungsID aufgeprägt wird, die als Index in eine Einlieferungsliste dient, die die Zustelladressen bzw. destination ZIP-Codes aller eingelieferten Postsendungen enthält. Ziel ist es hier, die Adresslesung und -erkennung im Briefzentrum durch einen vorgeschalteten elektronischen Prozess zu ersetzen. Dabei wird dasselbe Basissystem beschrieben, wie im vorherigen US 5,612,889 A. Somit trifft hier derselbe Nachteil zu.

[0011] Aus dem EP 1 058 212 A1 ist ein Verfahren zur Postgutverarbeitung und Postgutverarbeitungssystem bekannt, mit gestaffelter Postgutverarbeitung. Private Postbeförderer (Carrier), die regional aufgestellt sind, leiten Postsendungen zu deren Verteilung außerhalb ihrer Geschäftsregion an einen überregionalen Postbeförderer weiter. Eine Identifikation

des Absenders erfolgt mittels Chipkarte, die der Kunde des privaten Postbeförderers bei sich trägt und in einen Kartenleser der Postaufgabestation (Briefkasten) einsteckt, wenn der Kunde die Post aufgibt. Es ist vorgesehen, dass der Kunde einen Beleg über die in einen Briefkasten eingelegte und zunächst an einen ersten Carrier/Ort zuliefernde Post erhält. Die Chipkarte dient als Kundenkarte, die bereits eine Identifikationsnummer aufweist. Jedes Postgut wird mit einer maschinenlesbaren Markierung versehen, die aus einer für jedes Postgut spezifischen Nummer und weiteren Versanddaten besteht. Der erste Carrier transportiert die Post von der Postaufgabestation (Briefkasten) zum ersten Ort und frankiert dort den Brief mit einem Frankierstempel und nimmt eine Abbuchung vom Kundenkonto bei einer Kundenbank vor sowie liefert den frankierten Brief bei einer Postverteilzentrale eines zweiten Carriers ein, welcher die Post weiterbefördert. Nach der Markierung des Postguts wird also eine herkömmliche Frankierung durchgeführt und eine herkömmliche Einlieferungsliste erzeugt. Der fällige Portobetrag wird ermittelt und erhoben während die Postgüter eingeliefert werden. Im selben Prozess werden die entsprechenden Markierungen auf die Postgüter aufgebracht. Die Markierung kann Datum und Uhrzeit der Einlieferung und außerdem eine Identifizierung des Kunden enthalten, die zuvor von dessen Kundenkarte in die Aufgabestation eingelesen worden ist. Dieses Verfahren kann als "semi-zentrale Portoerhebung" bezeichnet werden. Sicherheitsprüfungen zusätzlich zur Sendungskennung und Absenderkennung wurden jedoch nicht offenbart.

[0012] Bei dezentraler Portoerhebung wird vorausbezahltes elektronisches Geld bzw. Guthaben in das Frankiergerät geladen. Gelingt es, diese Geldmenge zu manipulieren, so kann in der Folge unbezahlte postalische Dienstleistung in Anspruch genommen werden. Dies ist vom geschädigten Postbeförderer schwer erkennbar und noch schwerer zum individuellen Betrüger rückverfolgbar. Nachteilig ist der erforderliche Aufwand durch Hardware-Sicherheitsmodul oder eine online Datenverbindung zum Frankieren, welche die betrügerischen Manipulationen verhindern sollen.

[0013] Der Erfindung liegt die Aufgabe zugrunde, die Nachteile zu vermeiden und ein Frankierverfahren und Postversandsystem mit zentraler Portoerhebung zu schaffen und aufzubauen, wobei mithilfe von einfacher aufgebauten und bedienungsfreundlichen Frankiergeräten dennoch die Sicherheit des Systems garantiert wird. Das Frankiergerät soll eine manipulationssichere Gerätekennung auf dem Postgut aufbringen.

[0014] Erfindungsgemäß wird diese Aufgabe durch ein Verfahren mit den Merkmalen nach Anspruch 1 und ein Postversandsystem mit den Merkmalen nach Anspruch 17 gelöst.

[0015] Ausgehend von der Überlegung, dass ein anderes Vertrauensmodell als bei dezentraler Portoerhebung erforderlich ist, wurde die Sicherheit der Buchungen für Frankiergeräte trotz deren vereinfachten Bauweise erhöht. Zentral gespeicherte Daten können besser vor Fälschung geschützt werden. Bei zentraler Portoerhebung benutzt jedes Frankiergerät eine individuelle Gerätekennung, die auf all seinen Frankierabdrücken eingeprägt ist. Bei der Registrierung jedes Frankiergeräts assoziiert der Postbeförderer dessen Gerätekennung mit einem elektronischen Gerätekonto, dem er später alle Portogebühren für Postsendungen zuordnet, die die entsprechende Gerätekennung tragen. Die Abrechnung mit dem Kunden kann von der Buchung zeitlich entkoppelt durchgeführt werden. Das Bankkonto des Absenders wird mit den aufgelaufenen Kosten eines elektronischen Gerätekontos vorzugsweise am Ende jeder Abrechnungsperiode entsprechend belastet.

[0016] Die zentrale Portoerhebung ermöglicht Frankierlösungen beim Absender, die offline und ohne Sicherheitsmodul sicher funktionieren können. Die Postsendungen müssen jedoch eine fälschungssichere Kennung des Absenders bzw. seines Frankiergeräts tragen, damit die Portokosten den verursachenden Absendern korrekt zugeordnet werden können. Das wird mittels einer symmetrischen Verschlüsselung von Parametern und mit einem Schlüssel erreicht, der sich mit jedem Frankierabdruck ändert und welcher im Beförderer-Datenzentrum synchon gehalten werden kann, ohne dass bei jeder Frankierung eine Kommunikation zwischen dem Frankiergerät und dem Beförderer-Datenzentrum nötig ist. Vielmehr genügt eine anfängliche Initialisierung des Frankiergeräts.

[0017] Dabei wird vom Frankiergerät über das Betreiber-Datenzentrum zum Postbeförderer-Datenzentrum ein geheimer erster Frankierbildschlüssel verschlüsselt übermittelt. Letzterer kann im Frankiergerät mittels eines privaten Kommunikationsschlüssels verschlüsselt und im Betreiber-Datenzentrum mittels eines öffentlichen Kommunikationsschlüssels entschlüsselt werden. Auf prinzipiell dieselbe Weise kann der geheime erste Frankierbildschlüssel weiter zum Postbeförderer-Datenzentrum verschlüsselt übermittelt werden. Letzteres verfügt damit über einen aktuell gültigen ersten Frankierbildprüfschlüssel, welcher dem Absender bzw. seiner Gerätekennung zugeordnet gespeichert wird. Eine Markierung auf einem Poststück bzw. ein Frankierbild weist mindestens eine Gerätekennung des Frankiergeräts, eine Schlüsselgenerationsnummer und einen Integritäts-Checkcode auf. Letzterer erlaubt eine Überprüfung der Integrität von solchen Parametern, wie Gerätekennung und Schlüsselgenerationsnummer, weil letztere mittels des aktuell gültigen ersten Frankierbildschlüssels zum Integritäts-Checkcode verschlüsselt werden. Während der Initialisierung des Frankiergeräts werden die Gerätekennung des Frankiergeräts, die Schlüsselgenerationsnummer und der erste Frankierbildschlüssel an das Datenzentrum des Postbeförderers übermittelt.

[0018] Nach einem Frankieren wird im Frankiergerät aus dem ersten bzw. vorher gültigen Frankierbildschlüssel ein aktuell gültiger zweiter Frankierbildschlüssel erzeugt, welchem ein aktuell gültiger zweiter Frankierbildprüfschlüssel entspricht, der aber auf der Postbefördererseite erzeugt wird. Die lokale Schlüsselgenerationsnummer in einem Frankiergerät und deren lokale Kopie auf Seite des Postbeförderers werden synchron gehalten, um dort aus einem vorher

gültigen Frankierbildprüfschlüssel den aktuell gültigen Frankierbildprüfschlüssel ableiten zu können.

[0019] Jede Gerätekennung ist eindeutig einem Kundenkonto zugeordnet, dem die verbrauchten Portogebühren am Ende jeder Abrechnungsperiode in Rechnung gestellt werden. Nach jeder Frankierung wird die Schlüsselgenerationsnummer im Frankiergerät geändert, wobei ein schrittweises Verändern der Schlüsselgenerationsnummer um einen festgelegten Zahlenwert erfolgt. Zum Beispiel wird die Schlüsselgenerationsnummer um eins erhöht. Dann wird ein nächstgültger kryptographischer Schlüssel aus dem aktuell gültigen kryptographischer Schlüssel nach einem ersten Algorithmus abgeleitet.

Das Frankiergerät ist mit einer Elektronik zum sicheren Verwalten einer postalischen Identität ausgestattet und wird zum besseren Unterscheiden von den gewöhnlichen Frankiermaschinen nachfolgend Postal Identity Management Device (PIMD) genannt.

Vorteilhaft muss nunmehr kein vorausbezahltes elektronisches Geld oder elektronisches Guthaben in die Frankiergeräte geladen werden. Es gibt daher keine Möglichkeit, vorausbezahlte elektronische Geldmengen zu manipulieren. Es gibt auch keine Möglichkeit, den Postbeförderer durch Kopieren von Abdrucken zu betrügen. Es gibt überhaupt keinen Anreiz für einen Absender, sein eigenes Frankiergerät zu manipulieren. Daher gibt es aus Sicht des Postbeförderers auch keinen Bedarf, Frankiergeräte gegen Eingriffe ihrer Benutzer zu schützen, womit auch kein Bedarf nach einem Hardware-Sicherheitsmodul in Frankiergeräten besteht. Ebensowenig muss eine Online-Verbindung vor oder während des Frankierens hergestellt werden, außer bei einer Initialisierung des PIMD.

Es gibt allerdings grundsätzlich die Möglichkeit für jeden Absender, eine ungültige oder falsche Gerätekennung (Geräte-ID) zu verwenden. Wenn es einem Absender gelingt, eine fremde Gerätekennung zu kapern, so könnte er seine Post auf Kosten des gekaperten Geräts verschicken.

[0020] Ungültige Geräte-Identitäten sind jedoch von den Briefzentren grundsätzlich erkennbar, wenn sie online, d.h. bei der Briefsortierung, ausgewertet werden. Nur falsche Gerätekennungen sind von den Briefzentren grundsätzlich nicht erkennbar, da die wahre Identität des Absenders nicht bekannt ist. Dies könnte zwar durch eine biometrische Erkennung des Einlieferers am Briefkasten, etc. erfasst werden, das Frankiergerät wäre dann aber nicht einfacher aufgebaut. Die Verwendung falscher Gerätekennungen ist daher ohne zusätzlich Maßnahmen im Einlieferungsprozess nicht erkennbar, und demzufolge ist das Betrugspotenzial hierfür relativ groß. Eine betrügerische Manipulation der Gerätekennung kann jedoch durch eine Kombination von folgenden Maßnahmen wesentlich erschwert werden:

a) Schutz vor Missbrauch der Identifikation des Absender-Frankiergeräts mittels Passwort-Eingabe via Tastatur oder alternativ mittels RFID-Ausweis, Magnetkarte, Chipkarte, mobiles Gerät (Handy, Organizer) verbunden über persönliches Netzwerk (Bluetooth, USB, etc.) auf der Frankiergeräteseite.

b) Authentikation der Gerätekennung in jedem Frankierabdruck auf der Postbefördererseite, um die Verwendung falscher Gerätekennungen auszuschließen.

c) Einmal-Authentikation der Gerätekennung in jedem Frankierabdruck auf der Postbefördererseite, um die Wiederverwendung kopierter Authentikationen falscher Gerätekennungen auszuschließen. Es ist vorgesehen, dass jeder kryptographische Frankierbildschlüssel für höchstens ein Frankierbild verwendet wird, welches abtastbare Informationen, wie die Gerätekennung des Frankiergeräts, die Schlüsselgenerationsnummer und den Integritäts-Checkcode enthält.

d) Sicherung der Kommunikations-Verbindung mindestens zum Betreiber-Datenzentrum durch Verschlüsselung.

e) Bei Multi-User-Frankiergeräten, zum Beispiel PC-Frankierer, müssen die verschiedenen Benutzer eines Frankiergeräts gegeneinander geschützt werden. Das kann beim Einsatz eines PC's mithilfe bekannter Betriebssysteme gelöst werden, die separate Benutzerkonten verwalten können.

[0021] Da die erste Schlüsselgenerationsnummer zusammen mit dem ersten Frankierbildschlüssel und der Gerätekennung an ein Datenzentrum des Postbeförderes weiter übermittelt wird, kann dort eine entfernte Abtastung und Auswertung von zu überprüfenden Frankierbildern erfolgen, die vom Frankiergerät auf den Poststücken aufgebracht worden sind.

Ein Integritäts-Checkcode wird nach einem zweiten Krypto-Algorithmus mittels des geheimen kryptographischen Frankierbildschlüssels des Frankiergeräts des Absenders, der Gerätekennung des Frankiergeräts und der aktuellen Schlüsselgenerationsnummer erzeugt, wobei das Frankierbild, mindestens die Gerätekennung des Frankiergeräts, die aktuelle Schlüsselgenerationsnummer und den Integritäts-Checkcode abtastbar enthält.

Im Datenzentrum kann ein Ableiten eines Frankierbildprüfschlüssels, der dem nächsten geheimen Frankierbildschlüssel entspricht, aus dem ersten Frankierbildschlüssel und aus der im Frankierbild abtastbaren von jedem weiteren Poststück übermittelten aktuellen Schlüsselgenerationsnummer nach einem ersten Krypto-Algorithmus erfolgen, wenn für jedes

Frankierbild ein neuer Frankierbildschlüssel aus einem Vorgänger des Frankierbildschlüssels nach demselben ersten Krypto-Algorithmus abgeleitet wurde.

Es ist vorgesehen, dass ein Auswerten der gescannten Daten mittels eines Prüfablaufs im Datenzentrum des Postbeförderers, eine Ermittlung der mathematischen Beziehung der abgetasteten Schlüsselgenerationsnummer zu der Kopie der zuletzt verwendeten Schlüsselgenerationsnummer umfasst. Der Wert der Veränderung gegenüber der Kopie der zuletzt verwendeten Schlüsselgenerationsnummer ergibt sich aus dem Produkt jedes einzelnen Schrittwertes mit der Anzahl an Veränderungen. Bei einem schrittweisen Verändern der Schlüsselgenerationsnummer um einen festgelegten Zahlenwert in Vorbereitung eines nachfolgenden Frankierbildschlüssels ergibt sich die vorgenannte mathematische Beziehung aus der Anzahl der Veränderungen. Ein Frankierbildprüfschlüssel wird nach dem ersten Krypto-Algorithmus berechnet, wobei der erste Krypto-Algorithmus so oft angewendet wird, wie durch die mathematische Beziehung vorgegeben wird. Das Poststück wird einer Aussortierung und die abgetasteten Daten einer Fehlerbehandlung unterworfen, wenn ein schrittweises Verändern der Schlüsselgenerationsnummer um einen festgelegten Zahlenwert nicht zum erwarteten Ergebnis führt, d.h. wenn die mathematische Beziehung der vorgegebenen mathematischen Beziehung nicht entspricht. Das ist zum Beispiel der Fall, wenn sich die festgestellte mathematische Beziehung nicht aus der Anzahl der Veränderungen ergibt. Wenn auf die vorgenannte Weise eine Synchronität zwischen Frankiergerät und Datenzentrum, d.h. sowohl zwischen der abgetasteten Schlüsselgenerationsnummer und ihrer berechneten Kopie als auch zwischen dem geheimen kryptographischen Frankierbildschlüssel und dem berechneten Frankierbildprüfschlüssel hergestellt wird, kann ein Vergleichs-Integritäts-Checkcode im Datenzentrum berechnet werden, um den abgetasteten Integritäts-Checkcode kryptographisch zu verifizieren. Eine zentrale Portoerhebung wird im Datenzentrum des Postbeförderers durchgeführt, wenn die Echtheit des Integritäts-Checkcodes nachweislich vorliegt.

Ein Postversandsystem mit zentraler Portoerhebung umfasst ein Briefzentrum und Datenzentrum eines Postbeförderers, ein Datenzentrum eines Betreibers und eine Vielzahl von Frankiergeräten. Der Postbeförderer transportiert die vom Frankiergerät frankierten Poststücke in üblicher Weise zum Briefzentrum. Jedes Frankiergerät steht über eine Kommunikationsverbindung via Netz und über eine Kommunikationsverbindung bedarfweise in Kontakt mit dem Betreiber-Datenzentrum, das die Gerätekennung seiner Benutzer registriert und zusätzliche Dienste anbietet. Jedes Frankiergerät kann Frankierabdrucke auf Briefe und/oder Etiketten für Poststücke drucken, die anschließend zur weiteren Postbeförderung in das Briefzentrum eingeliefert werden, welches mit dem Datenzentrum des Postbeförderers kommunikativ verbunden ist. Das Datenzentrum des Briefzentrums ist via eine Kommunikationsverbindung mit dem Netz verbunden und kann ebenso mit dem Betreiber-Datenzentrum kommunizieren, wie umgekehrt das Betreiber-Datenzentrum mit dem Briefzentrum-Datenzentrum. Somit kann im Ergebnis einer Initialisierung eines Frankiergerätes eine Information vom Frankiergerät via dem Betreiber-Datenzentrum zum Datenzentrum des Postbeförderers gelangen, obwohl das Frankiergerät in keine direkte Kommunikation mit dem Datenzentrum des Postbeförderers eintritt. Durch die vorgenannte Information ist das Datenzentrum des Postbeförderers zur Auswertung von Informationen des Frankierbildes in der Lage, insbesondere zum Lesen und Zuordnen der Gerätekennung zu einem Absender und zur Buchung der Portogebühren für Poststücke desselben Absenders auf ein separates Konto oder zur Fehlerbehandlung.

Es ist vorgesehen, dass das Frankiergerät ein Schlüsselgenerierungsmittel enthält, das für jedes nächste Frankierbild einen neuen Frankierbildschlüssel generiert.

Weiter sind Kommunikationsmittel vorgesehen, um über die Kommunikationsverbindung eine Synchronität zwischen Frankiergerät und Datenzentrum bedarfsweise herzustellen.

Es sind Abtastmittel im Briefzentrum und erste Auswertemittel im Datenzentrum eines Postbeförderers vorgesehen, die kommunikativ miteinander verbunden sind, wobei durch die ersten Auswertemittel der Absender des Poststückes über eine in einer Datenbank gespeicherte Zuordnung der Gerätekennung zu einem Absender bestimmt und durch Portzoberechnungsmittel die Portogebühr ermittelt wird.

Die Auswertemittel im Datenzentrum schließen zweite Mittel zur Sicherheitsüberprüfung jedes abgetasteten Frankierbildes ein, welche dann, wenn sich zwischen der abgetasteten Schlüsselgenerationsnummer und ihrer berechneten Kopie und zwischen dem geheimen kryptographischen Frankierbildschlüssel und dem berechneten Frankier-bildprüfschlüssel Synchronität herstellen lässt, einen Vergleichs-Integritäts-Checkcode im Datenzentrum berechnet, um den abgetasteten Integritäts-Checkcode kryptographisch zu verifizieren.

Ein Mittel zur Buchung der Portogebühren für Poststücke desselben Absenders auf ein separates Konto und ein Mittel zur Fehlerbehandlung ist im Datenzentrum des Postbeförderers vorgesehen, wobei die zentrale Portoerhebung dann durchgeführt wird, wenn die Echtheit des Integritäts-Checkcodes nachweislich vorliegt.

[0022] Die zweiten Mittel zur Sicherheitsüberprüfung sind programmiert, so dass eine Ermittlung der mathematischen Beziehung der abgetasteten Schlüsselgenerationsnummer zu der Kopie der zuletzt verwendeten Schlüsselgenerationsnummer erfolgt, wobei ein Frankierbildprüfschlüssel, der dem aktuellen nachfolgenden Frankierbildschlüssel des Frankiergeräts entspricht, nach dem ersten Krypto-Algorithmus erzeugt, wobei letzterer entsprechend der ermittelten mathematischen Beziehung z-Mal angewendet wird sowie wobei der Frankierbildprüfschlüssel zusammen mit der Kopie der aktuell verwendeten Schlüsselgenerationsnummer und mit der Gerätekennung zur Bildung eines Vergleichs-Integritäts-Checkcodes nach dem zweiten Krypto-Algorithmus verwendet wird.

[0023] Die Erfindung besitzt folgende Vorteile gegenüber Stand der Technik:

- Die beschriebenen Frankiergeräte eines Systems mit zentraler Portoerhebung brauchen nicht mit einer speziellen Sicherheits-Hardware ausgestattet zu werden. Da das Betrugsrisiko für Postbeförderer verschwindend gering wäre, können die Zulassungsanforderungen gegenüber Frankiersystemen mit dezentraler Portoerhebung deutlich reduziert werden. Die beschriebe-nen Frankiergeräte können deutlich preiswerter hergestellt und in Verkehr gebracht werden, als Frankiermaschinen mit dezentraler Portoerhebung.
- Frankierabdrucke für zentrale Portoerhebung können sehr einfach gestaltet werden. Notwendig ist nur die einmal authentisierte Gerätekennung. Weitere Informationen herkömmlicher Frankierabdrucke wie z.B. Datum, Portowert, Postproduktcode, brauchen nicht im Frankierabdruck enthalten zu sein, weil sie alle im Wege der zentralen Portoerhebung bestimmt werden können.
- Eine Kommunikation über ein Kommunikationsnetz ist innerhalb des Postversandsystems bei Bedarf möglich und muss nicht für jedes Poststück erfolgen.

[0024] Weitere vorteilhafte Merkmale der Erfindung sind den Unteransprüchen zu entnehmen. Die Erfindung wird nachstehend am Ausführungsbeispiel näher erläutert. Es zeigen:

Fig. 1a, Frankiersystem mit unterschiedlichen Varianten an Kommunikationsverbindungen,

Fig. 1 b, Prinzipdarstellung einer bedruckten Briefoberseite,

Fig. 1 c, schematische Darstellung der Abläufe beim Postbeförderer,

Fig. 2, Blockschaltbild eines Frankiergrätes (PIMD's),

Fig. 3, Darstellung der Ebenen des Speicherschutzes eines PIMD's,

Fig. 4, Flussplan bei der Initialisierung eines PIMD's,

Fig. 5, Flussplan beim Wechseln eines Passworts,

Fig. 6, Flussplan beim Berechnen eines Frankierabdrucks,

Fig. 7, Flussplan zur Echtheitsüberprüfung einer Geräte-ID,

Fig. 8, Flussplan beim Senden eines Frankierbildschlüssels des PIMD's an dasPostbeförderer-Datenzentrum.

[0025] Anhand der Fig. 1a wird ein Frankiersystem mit unterschiedlichen Varianten an Kommunikationsverbindungen zwischen einem Betreiber-Datenzentrum und Frankiergeräten dargestellt. Kleine mobile Frankiergeräte 10, 10', 10", 10* können mit ihrem Druckermodul Frankierabdrucke erzeugen, in welche eine Gerätekennung fälschungssicher eingeprägt ist. Solche Frankiergeräte werden nachfolgend auch als Postal Identity Management Device (PIMD) bezeichnet. Jedes PIMD steht über eine Kommunikationsverbindung 11, 11', 11", 11* via Netz 18 und eine Kommunikationsverbindung 19 in Kontakt mit dem Betreiber-Datenzentrum 14. Dort registriert es die Gerätekennung für seine Benutzer und erhält zusätzliche Dienste angeboten. Jedes PIMD kann Frankierabdrucke 9.3 auf Briefe 9 und/oder Etiketten für Poststücke drucken, die anschließend zur weiteren Postbeförderung in ein Briefzentrum- Datenzentrum 7 eingeliefert werden. Das Briefzentrum 7 ist via eine Kommunikationsverbindung 8 mit dem Netz 18 verbunden und kann ebenso mit dem Betreiber-Datenzentrum 14 kommunizieren, wie umgekehrt das Betreiber-Datenzentrum 14 mit dem Briefzentrum-Datenzentrum 7. Die Kommunikationsverbindungen 8 und 19 ermöglichen beispielsweise eine Kommunikation via Internet- oder Telefon-Netz.

[0026] Jedes PIMD steht über das Netz 18 mit dem Betreiber-Datenzentrum 14 in Verbindung. Zur Sicherung der Kommunikationsverbindung kann eine symmetrische oder asymmetrische Verschlüsselung verwendet werden. Beispielsweise wird vom Frankiergerät über das Betreiber-Datenzentrum 14 zumPostbeförderer-Datenzentrum 7 ein geheimer erster Schlüssel verschlüsselt übermittelt. Letzterer kann im Frankiergerät mittels eines privaten Schlüssels verschlüsselt und im Betreiber-Datenzentrum mittels eines öffentlichen Schlüssels entschlüsselt werden. Das Betreiber-Datenzentrum 14 kann beispielsweise ebenso über eine durch Verschlüsselung gesicherte Verbindung via Netz 18 oder über eine - nicht gezeigte - Standleitung mit demPostbeförderer-Datenzentrum 7 kommunizieren. Dabei ist eine mehr oder weniger unterschiedliche Technik einsetzbar. Einige Verbindungs-Varianten sind in Fig. 1a dargestellt:

A) Ein PIMD 10' verbindet sich über ein Funk-WAN 13' (beispielsweise GSM, UMTS Modem) mit eine Funk-Station 6', welche via der Kommunikationsverbindung 11', Netz 18 und der Kommunikationsverbindung 19 mit dem Betreiber-Datenzentrum 14 verbindbar ist.

B) Ein PIMD 10 ist über ein leitungsgestütztes Telefonnetz 11, 18, 19 direkt mit dem Betreiber-Datenzentrum 14 verbindbar.

C) Ein PIMD 10" ist über ein Funk-LAN (WiFi) oder Funk Personal Network (Bluetooth) 13" mit einer Funkstation 6" eines PC 12" verbunden, der sich via Kommunikationsverbindung 11" (zum Beispiel Internet), Netz 18 und Kommunikationsverbindung 19 mit dem Betreiber-Datenzentrum 14 verbinden läßt.

D) Ein PIMD 10* ist über eine Punkt-zu-Punkt Verbindung (USB) 15* mit einem PC 12* verbunden, der sich via Kommunikationsverbindung 11* (zum Beispiel Internet), Netz 18 und Kommunikationsverbindung 19 mit dem Betreiber-Datenzentrum 14 verbinden läßt.

E) Die Funktion eines PIMD's ist in den PC 12* integriert. Das kann durch eine entsprechende Software und/oder Hardware (Einschub nicht dargestellt) geschehen. Der PC 12* steht einerseits via einer Punkt-zu-Punkt Verbindung (USB) 16* mit einem handelsüblichen Drucker 17* und andererseits via Kommunikationsverbindung 11* (zum Beispiel Internet), Netz 18 und Kommunikationsverbindung 19 mit dem Betreiber-Datenzentrum 14 in Kommunikationsverbindung.

[0027] Die grundlegende Arbeitsweise des Systems gliedert sich in die Verfahrensschritte:

- Übermitteln des ersten Frankierbildschlüssels $IDAKey_1$ zur entfernten Auswertung von zu überprüfenden Frankierbildern auf Poststücken,
- Berechnung eines Frankierbilds vor der Erzeugung einer Frankierung, wobei für jedes Frankierbild ein neuer Frankierbildschlüssel aus einem Vorgänger des Frankierbildschlüssels nach einem ersten Krypto-Algorithmus abgeleitet und wobei ein Integritäts-Checkcode M basierend auf dem neuen Frankierbildschlüssel, einer Schlüsselgenerationsnummer i, einer Gerätekennung *g* des Frankiergeräts und basierend auf einem zweiten Krypto-Algorithmus erzeugt wird, wobei das Frankierbild, mindestens die Gerätekennung *g* des Frankiergeräts, die Schlüsselgenerationsnummer i und dem Integritäts-Checkcode M aufweist,
- Befördern und Einliefern von Poststücken in ein Briefzentrum des Postbeförderers nach dem Frankieren, Abtasten und Prüfung von Frankierbildern beim Postbeförderer, wobei der Integritäts-Checkcode M kryptographisch verifiziert wird, indem ein Vergleichs-Integritäts-Checkcode zum Vergleich mit dem aufgedruckten Integritäts-Checkcode gebildet wird und wobei Gebühren zur zentralen Buchung erfaßt werden, welche dem Absender der Poststücke zeitlich entkoppelt von der Buchung am Ende der Abrechnungsperiode in Rechnung gestellt werden sowie
- Fehlerbehandlung beim Prüfen.

Berechnung von Frankierabdrucken

[0028] Um eine Frankierung vorzunehmen, bestimmt der Absender in bekannter Weise das erforderliche Porto und startet die Frankierung mit seinem PIMD. Das PIMD kann eine integrierte Waage und/oder einen Portorechner enthalten. Das PIMD druckt optionale Klartextinformationen wie den erforderlichen Portowert, das aktuelle Datum und ggfs. Angaben zur Postsendung (Produktbezeichnung, etc.)
Das PIMD druckt außerdem eine Markierung, beispielsweise einen maschinenlesbaren Barcode, der folgende Informationen enthält:

g Eine Geräte-ID (deviceID) ist die Kennung des Frankiergeräts, die zu dessen Identifikation herangezogen werden kann.
Benutzt ein Kunde mehrere verschiedene Frankiergeräte, so verwendet er verschiedene eindeutige Gerätekennungen für jedes Frankiergerät. Jede Gerätekennung ist eindeutig einem Kundenkonto zugeordnet, dem am Ende jeder Abrechnungsperiode (z.B. am Monatsende) die Umsätze aller zugeordneten Frankiergeräte belastet werden.

i Eine Schlüsselgenerationsnummer.
Ein schrittweises Verändern der Schlüsselgenerationsnummer *i* kann um irgendeinen festgelegten Zahlenwert ***h*** erfolgen. Die Schlüsselgenerationsnummer i wird mit jeder Frankierung um vorzugsweise den Wert ***h*** = 1 erhöht oder verringert. Jeder Schlüsselgenerationsnummer ist eineindeutig ein kryptographischer Schlüssel *IDAKeyi* zugeordnet, der zur Berechnung von Integritäts-Checkcodes von Frankierabdrucken (Indicia) verwendet wird.

M Ein Integritäts-Checkcode.

[0029] Dieser Code *M* wird mithilfe eines Algorithmus für einen Message Authentication Code (MAC) über die oben bezeichneten Daten berechnet (Henk C. A. van Tilborg: Encyclopedia of Cryptography and Security; Springer-Verlag New York, 2005, Seiten 361-367). Vorzugsweise wird ein hash based message authentication code (HMAC) verwendet (ebenda Seiten 14 und 267). Zur HMAC-Bildung wird ein geheimer kryptographischer Schlüssel des Absenders nach folgender Formel (1) verwendet:

$$M \leftarrow HMAC(IDAKey_i, f(g, i, IDAKey_i)). \quad (1)$$

[0030] Hierbei ist f eine Funktion mit den Parametern *g*, i und *IDAKeyi*. Vorzugsweise liefert die Funktion f als Ergebnis den String *g* || *i* bestehend aus der bitweisen Hintereinanderschreibung der Parameter *g* und *i:*

$$M \leftarrow HMAC(IDAKey_i, g \,||\, i). \quad (2)$$

[0031] Bei der Initialisierung eines Frankiergeräts, wird dessen Schlüsselgenerationsnummer auf Eins gesetzt und ein initialer kryptographischer (erster) Schlüssel $IDAKey_1$ generiert. Während der anschließenden Registrierung des Frankiergeräts wird die Frankiergerätekennung *g*, die erste Schlüsselgenerationsnummer *i* = 1 sowie der zugehörige erste kryptographische Schlüssel $IDAKey_1$ an den Postbeförderer übermittelt. Auf diese Weise erhält der Postbeförderer denselben geheimen kryptographischen Schlüssel, den das Frankiergerät verwendet.

[0032] Die vom Postbeförderer erhaltenen und in der Folge verwalteten Schlüsselgenerationsnummern und kryptographischen Schlüssel seien im folgenden mit *j* bzw. $IDAKey_j$ bezeichnet. Ziel ist es, die lokale Generationsnummer *i* in einem Frankiergerät und seine lokale Kopie *j* auf der Seite des Postbeförderers synchron zu halten. Wie dieses Ziel erreicht wird, wird anhand der nachfolgend behandelten Verfahrensschritte Prüfung von Frankierabdrucken und Fehlerbehebung genauer erklärt.

[0033] Nach jeder Frankierung wird die Schlüsselgenerationsnummer i im PIMD um eins erhöht und ein neuer kryptographischer Schlüssel $IDAKey_{i+1}$ aus dem aktuellen Schlüssel $IDAKey_i$ nach Formel (3) abgeleitet:

$$IDAKey_{i+1} \leftarrow hash(i, IDAKey_i) \quad (3)$$

[0034] Die Bildung eines Hash-Wertes nach einer Hash-Funktion geht u.a. auch aus Henk C. A. van Tilborg: Encyclopedia of Cryptography and Security; Springer-Verlag New York, 2005, Seiten 256-264 hervor.

[0035] Für die *i*-te Frankierung nach Initialisierung des Frankiergeräts wird die Schlüsselgenerationsnummer *i* und der kryptographische Schlüssel $IDAKey_i$ verwendet. Auf diese Weise ist sichergestellt, dass jeder kryptographische Schlüssel für höchstens eine Frankierung verwendet wird.

Prüfen von Frankierungen

[0036] Die frankierten Sendungen werden wie bekannt beim gewünschten Briefbeförderer eingeliefert. Der Postbeförderer sortiert die Postsendungen, liest automatisch die Frankierabdrucke einschließlich der enthaltenen Barcodes ein, transportiert anschließend die Postsendungen zur Zieladresse und liefert sie dort aus. Die vorliegende Erfindung geht davon aus, dass vor der Sortierung alle Postsendungen gelesen und ihre Barcodes zu annähernd 100 % erkannt und korrekt dekodiert werden können.

[0037] Bei der Lesung der Postsendungen werden die Klartextinformationen ausgewertet und für die Ermittlung des Portowerts verwendet. In einer Ausführung kann der Portowert einfach abgelesen werden. In einer zweiten Ausführung kann der aufgedruckte Portowert stichprobenhaft überprüft werden. In einer dritten Ausführung wird der Portowert gar nicht gedruckt und gelesen, sondern direkt aus den physischen Parametern (Länge, Breite, Dicke, Gewicht, Zusatzdienste) der Postsendung im Briefzentrum ermittelt.

[0038] Weiterhin wird bei der Lesung der Inhalt des Barcodes ermittelt, ausgewertet und wie folgt geprüft:

(I) Zuerst wird mittels eines ersten Prüfschrittes geprüft, ob die Frankiergerätekennung *g* in der Datenbank des Datenzentrums bekannt ist. Ist die Prüfung erfolgreich, so ermittelt der Postbeförderer aus seiner Datenbank die lokale Kopie *j* auf der Seite des Postbeförderers der zuletzt gelesenen Schlüsselgenerationsnummer i und den zugehörigen Frankierbildprüfschlüssel $IDAKey_j$.

(II) Anschließend wird mittels eines zweiten Prüfschrittes geprüft, ob die lokale Kopie *J* der aktuell gelesenen Schlüsselgenerationsnummer i + *x* größer bzw. ob i - *x* kleiner ist, als die letzte von diesem Frankiergerät mit derselben Gerätekennung *g* gespeicherte lokale Kopie *j* der Schlüsselgenerationsnummer i. Ist diese Prüfung erfolgreich, so wird der aktuelle Frankierbildschlüssel $IDAKey_J$ berechnet. Im allgemeinen Fall gilt $J = j + x$ für aufsteigende oder $J = j - x$ fallende Schlüsselgenerationsnummern. Aufgrund eines konstanten Schrittwertes *h* und der Anzahl z der Schritte ergibt sich der Wert x der Veränderung der Schlüsselgenerationsnummer insgesamt nach der Formel (4) zu:

$$x = h \cdot z \qquad (4)$$

Bei einem Schrittwert $h = 1$ und der Anzahl $z = 1$ der Schritte, d.h. im bevorzugten Normalfall $J = j + 1$ berechnet man den aktuellen Schlüssel nach folgender Formel (4):

$$IDAKey_J \leftarrow hash\,(j, IDAKey_j). \qquad (5)$$

Anderenfalls, muss die Prüfung zum Beispiel bei einem Vorkommen von Abtast- oder Lesefehlern nicht immer erfolgreich sein. Das betreffende Poststück wird ausgesondert. Das nächstfolgende Poststück desselben Absenders weist in der aktuell gelesenen Schlüsselgenerationsnummer eine größere Änderung auf, weil die Anzahl z der Schritte mit dem Schrittwert $h = 1$ erhöht ist. Folglich wird die obige Rechenvorschrift umgestellt und im Datenzentrum $(J - j) \cdot 1/h = z$ Mal rekursiv angewendet. Das vorgenannte nächstfolgende Poststück desselben Absenders hat im bevorzugten Normalfall (h = 1) ein Frankierbild mit einer aktuell gelesenen Schlüsselgenerationsnummer $i + 2$ und einen aktuellen Frankierbildschlüssel $IDAKey_{i+2}$. Der Wert der lokalen Kopie *j* muss folglich entsprechend dem Wert x der Veränderung, d.h um x = 2 geändert und die Formel (5) noch einmal zusammen mit dem zuletzt berechneten Frankierbildprüfschlüssel für das ausgesonderte Poststück angewendet werden, um einen aktuellen Frankierbildschlüssel ableiten zu können.

(III) Danach wird im dritten Prüfschritt der gelesene Integritäts-Checkcode *M* kryptographisch verifiziert, indem die folgende Gleichung (6) geprüft wird:

$$M = HMAC\,(IDAKey_J,\ f(g, J,\ IDAKey_J)). \qquad (6)$$

Hierbei ist, *f* eine Funktion mit den Parametern *g*, *J* und $IDAKey_J$.
Es wird die Funktion ,*f*, die vorzugsweise eine Zusammenstellung der Parameter *g*, *J* zu einer (alphanumerischen) Zahl umfasst, mit dem geheimen Frankierbildschlüssel $IDAKey_J$ verschlüsselt, um einen Zahlenwert als Basis der HMAC-Bildung zu erzeugen. Wenn also vorzugsweise nach der Formel (2) gearbeitet wird, dann ist auch vereinfachend für die Sicherheitsüberprüfung vorgesehen, dass nach der Gleichung (7) geprüft wird, um den Integritäts-Checkcode *M* kryptographisch zu verifizieren:

$$M = HMAC\,(IDAKey_J,\ (g \,||\, J)). \qquad (7)$$

Ist auch diese Prüfung erfolgreich, so wird der ermittelte Portobetrag dem elektronischen Gerätekonto zugeschlagen, das der Postbeförderer für dieses Gerät im Datenzentrum des Briefzentrums führt. Am Ende der Abrechnungsperiode

werden alle auf diesem Gerätekonto aufgelaufenen Gebühren dem betreffenden Kundenkonto belastet.

Fehlerbehandlung mit Fehlerbehebung

[0039] Scheitert die Prüfung mittels des ersten Prüfschrittes (I) so wurde offenbar eine ungültige Absenderkennung verwendet. Übertragungsfehler wären bereits durch die Fehlerkorrektur des verwendeten Barcodes kompensiert worden. Es liegt beim jeweiligen Postbeförderer, für diesen Fall eine Fehlerbehandlung zu definieren. Mögliche Behandlungen sind:

a) Der Brief wird an den Absender zurückgeschickt.

b) Die Postbeförderung kann beendet, und der Brief vernichtet werden.

c) Der Adressat kann informiert und gefragt werden, ob er den Brief auf eigene Rechnung zugestellt bekommen möchte. Falls das nicht der Wunsch des Adressaten ist, kann wie unter a) beschrieben verfahren werden.

[0040] Scheitert Prüfung mittels des zweiten Prüfschrittes (II), so liegt entweder ein Replay Angriff vor, oder die Steuerung des PIMD arbeitet fehlerhaft. In jedem Fall druckt der Postbeförderer auf der Postsendung die letzte gespeicherte Schlüsselgenerationsnummer des betreffenden Frankiergeräts auf und schickt diese an den Betreiber des erkannten Frankiergeräts zurück. Zusätzlich sollte dieser auch auf elektronischem Wege über die Retour und die aktuelle am Datenzentrum bekannte Schlüsselgenerationsnummer benachrichtigt werden (e-mail, SMS), damit er in der Zwischenzeit nicht weitere Postsendungen mit falschen Schlüsselgenerationsnummern frankiert.

[0041] Scheitert die Prüfung mittels des dritten Prüfschrittes (III), so liegt ein fataler Fehler vor, denn da die Schlüsselgenerationsnummer i des erzeugenden PIMD und deren Kopie *j* im prüfenden Briefzentrum übereinstimmen, d.h. Prüfung (II) war erfolgreich, müssten die kryptographischen Schlüssel ebenfalls übereinstimmen. In diesem Fehlerfall ist eine erneute Initialisierung und Registrierung des PIMD zu veranlassen.

[0042] Bevorzugt kann eine neue Initialisierung dadurch geschehen, dass das Datenzentrum 7 des Postbeförderers einen neuen Frankierbildschlüssel $IDAKey^*_j$ erzeugt und einen Differenzwert Δ nach folgender Formel (8) ermittelt:

$$\Delta \leftarrow IDAKey_1 \text{ XOR } IDAKey^*_j \qquad (8)$$

[0043] (XOR bezeichnet die BOOL'sche Operation des bitweisen Exklusiv-ODER). Der Differenzwert Δ wird anschließend auf die Retoursendung aufdruckt, die an den Absender des Poststückes zurückgeschickt wird. Der Differenzwert Δ wird zusätzlich auf elektronischem Wege an das Datenzentrum 14 des Betreibers des erkannten Frankiergeräts übermittelt. Da der erste Frankierbildschlüssel dem Betreiberdatenzentrum bekannt ist und über Exklusiv-Oder-Funktion mit dem neuen Frankierbildschlüssel logisch verknüpft ist, kann der neue Frankierbildschlüssel $IDAKey^*_j$ ermittelt werden. Der neue Frankierbildschlüssel kann nun auf dem Wege einer gesicherten Kommunkiation dem betreffenden PIMD zugeschickt bzw. übermittelt werden. Die bei der PIMD-Initialisierung erforderlichen Schritte können dementsprechend modifiziert zur Anwen-dung kommen, dass das PIMD den neuen Frankierbildschlüssel übernimmt.

[0044] Die Fig. 1b zeigt eine Prinzipdarstellung einer bedruckten Briefoberseite mit einem ersten Feld für die Absenderadresse oder Werbung, mit einem zweiten Feld 9.2 für eine Markierung im Empfängeradressenfeld und mit einem dritten Feld 9.3 für die Frankierung. Die vorgenannte Markierung und/oder die Frankierung enthält eine manipulationssichere Gerätekennung. Selbstverständlich sind die Gerätekennung/Frankierabdrucke in 2D-Barcodes kodiert ausdruckbar. Die Gerätekennung kann augrund der kleinen Datenmenge auch als 1D-Barcode aufgedruckt werden. Hier eignen sich zum Beispiel GS1-128 (UCC/EAN-128), oder USPS OneCode. Diese Barcodes sind bei hoher Geschwindigkeit zuverlässig lesbar und erlauben dem Lesegerät gleichzeitig, eine gewisse Fehlerrate automatisch zu korrigieren. Sie werden bereits in vielen Postbriefzentren gelesen und erfordern in diesen keine weiteren Investitionen in Scannertechnologie.

[0045] Alternativ könnten auch OCR-Fonts verwendet werden, um die Gerätekennungen zu drucken und zu lesen. Wieviel Information für eine authentisierte Gerätekennung benötigt wird, hängt im Wesentlichen von der Anzahl der möglichen Absender ab. Bei 4 Byte, die für eine Checksum benötigt werden und einer Anzahl von x Millionen möglichen Absendern werden mindestens eine Anzahl von $\#I = \log_{256}(x \cdot 10^6)+4 = \log_{256}(x)+6 \cdot \log_{256}(10)+4 = \log_{256}(x)+6{,}5$ Bytes für die Kodierung einer Gerätekennung benötigt. Ein postalischer Markt von bis zu 17 Millionen Absendern erfordert daher 7 Byte, ein Markt bis zu 4 Milliarden Absendern 8 Byte und ein Markt bis zu 1,09 Billionen Absendern 9 Byte lange Gerätekennungen. Insgesamt ca. 1,6 Millionen Frankiermaschinen sind zur Zeit auf dem US-amerikanischen Markt im

Bestand. Eine 7 Byte-Gerätekennung erscheint hier ausreichend zu sein. Wenn die frankierten Poststücke die entsprechenden Sortieranlagen der postalischen Briefzentren durchlaufen, werden die Abdrucke gelesen, das aufgedruckte Porto, die Gerätekennung und weitere Informationen erfasst, überprüft und in einem Datenzentrum des Post Briefzentrums ausgewertet. Jedem Absender wird anhand dieser Auswertung die für ihn erbrachte postalische Leistung in Rechnung gestellt.

[0046] Die Fig. 1c zeigt eine schematische Darstellung der Abläufe beim Briefbeförderer. Nach einer Erzeugung einer Markierung und/oder Frankierung in einem ersten Schritt 1, welche ein Erzeugen einer manipulationssicheren Gerätekennung umfasst, erfolgt ein Transport des Poststückes. Ein weisser Pfeil gibt die Transportrichtung an.

[0047] Die grundlegende Arbeitsweise im Briefzentrum des Postbeförderers geht von einer Einlieferung des Poststücks im Briefzentrum in einem zweiten Schritt 2, einer Abtastung und Auswertung einer Markierung und/oder Frankierbildes in einem dritten Schritt 3, den weiteren Transport des Poststücks im vierten Schritt 4 und dessen Auslieferung im fünften Schritt 5 oder dessen Aussortierung im vierten Schritt 4 aus. Die Informationen aus der abgetasteten Markierung und/oder des Frankierbildes werden im Datenzentrum des Briefzentrums in einer Auswertungs-Routine 300 zu deren Auswertung weiter verarbeitet. Die Auswertung in der Routine 300 umfasst mindestens die folgenden Schritte:

301 Dekodierung und Fehlerkorrektur der Information nach dem Abtasten,
302 Ermittlung des Absenders,
303 Ermittlung der Portogebühr,
304 Sicherheitsüberprüfungen,
305 Abfrage nach Verifizierung und
306 Buchung oder
307 Fehlerbehandlung.

[0048] Im Briefzentrum ist ein Abtastmittel und im Datenzentrum eines Postbeförderers ist ein erstes Auswertemittel vorgesehen, die kommunikativ miteinander verbunden sind, um im Schritt 301 eine Dekodierung und Fehlerkorrektur der Information nach dem Abtasten, im Schritt 302 eine Ermittlung des jeweiligen Absenders und im Schritt 303 eine Ermittlung der Portogebühr durchzuführen. Das erste Auswertemittel umfasst eine Datenbank, die mit einem Server gekoppelt ist.

[0049] Alternativ kann die Reihenfolge der Schritte 302 und 303 vertauscht oder die beiden Schritte können nebenläufig ausgeführt werden.

[0050] Dabei ist vorgesehen, dass

- die Ermittlung (302) des jeweiligen Absenders eine Suche nach der Gerätekennung $_g$ des Frankiergeräts in einer Datenbank des Briefzentrums oder Datenzentrums und nach der zugehörig gespeicherten Kopie *j* der zuletzt verwendeten Schlüsselgenerationsnummer umfasst, zu der ein zugehörig gespeicherter Frankierbildschlüssel existiert,

- die Sicherheitsüberprüfung (304) jedes Frankierbildes, eine Ermittlung der mathematischen Beziehung der abgetasteten Schlüsselgenerationsnummer $i \mp x$ zu der Kopie *j* der zuletzt verwendeten Schlüsselgenerationsnummer sowie eine kryptographische Verifizierung des Integritäts-Checkcodes M umfasst, wobei ein Frankierbildprüfschlüssel $IDAKey_J$, welcher dem aktuellen nachfolgenden Frankierbildschlüssel $IDAKey_{i \mp x}$ des Frankiergeräts entspricht, nach dem ersten Krypto-Algorithmus erzeugt, wobei letzterer entsprechend der Ermittlung der mathematischen Beziehung *z*-Mal angewendet wird sowie wobei der Frankierbildprüfschlüssel $IDAKey_J$ zusammen mit der Kopie *J* der aktuell verwendeten Schlüsselgenerationsnummer $i \mp x$ und mit der Gerätekennung *g* zur Bildung eines Vergleichs-Integritäts-Checkcodes *Mref* nach dem zweiten Krypto-Algorithmus verwendet wird.

[0051] Im Datenzentrum sind zweite Mittel zur Sicherheitsüberprüfung jedes abgetasteten Frankierbildes vorgesehen, vorzugsweise ein Server, der gegen Missbrauch gesichert ist.
Nach nach einem Durchlaufen der Schritte 301 bis 304 erfolgt eine Abfrage nach einer Verifizierung der Frankiergerätekennung *g*. Wenn nach einem Durchlaufen der Schritte 301 bis 304 eine Verifizierung möglich ist, dann erfolgt im Schritt 306 eine Buchung der Portogebühr im Rahmen der zentralen Portoerhebung auf das Konto des im Schritt 302 ermittelten Absenders. Wenn nach einem Durchlaufen der Schritte 301 bis 304 aber keine Verifizierung möglich ist, dann wird das im Abfrage-Schritt 305 festgestellt und auf einen Schritt 307 zur Fehlerbehandlung verzweigt. Das Prüfen von Frankierungen und die drei Prüfschritte wurden oben bereits erläutert. Im Rahmen der Fehlerbehandlung wird ein Weichensignal erzeugt, um den weiteren Transport des Poststücks im vierten Schritt 4 zu unterbinden und um statt dessen eine Aussortierung des Poststücks zu veranlassen. Das Poststück wird zum Empfänger transportiert, wenn der Adressat (Empfänger) des Poststücks benachrichtigt worden ist und einer Zustellung zugestimmt hat. Das Poststück kann zum Absender zurücktransportiert werden, wenn der Absender des Poststücks benachrichtigt worden ist und einer Rücksendung zugestimmt hat. Andernfalls wird ein nicht zustellbares Poststück vernichtet. Im Rahmen der Zustellung

an den Adressat (Empfänger) des Poststücks erfolgt ebenfaslls eine Buchung, jedoch auf den Empfängernamen.
Im Rahmen der Fehlerbehandlung können weitere Nachforschungen und auch eine Registrierung nicht zustellbarer Poststücke erfolgen.

[0052] Ein Blockschaltbild 100 eines Frankiergrätes (PIMD's) ist in der Figur 2 gezeigt. Das Frankiergerät hat eine Tastatur 112 (keyboard), eine Anzeigeeinheit 114 (LCD) und ein Druckermodul 116 (printer), die mit einer jeweils zugehörigen Ansteuerelektronik (keyboard controller 111, display controller 113, printer driver 115) vebunden sind. Es hat weiterhin einen Prozessor 104 (CPU), eine Speichermanagementeinheit 117 (MMU), sowie flüchtige und nicht-flüchtigen Speicher (volatile memory 102, 107 und nonvolatile memory 101, 103) und ein Kommunikations-Interface 109 mit seriellen Ein-/Ausgang zum Datenaustausch mit einem Betreiber-Datenzentrum. Das Kommunikations-Interface kann leitungsgebunden (z.B. USB, LAN, etc.) oder drahtlos (z.B. WLAN, GSM, Bluetooth) ausgelegt sein. Zusätzlich gibt es einen zeitgesteuerten Treiber 108 (Time threshold), der auf einen flüchtigen Speicher 102 zugreift und einen kryptographisch verschlüsselnden Treiber 106, der auf einen nicht-flüchtigen Speicher 103 zugreift. Der zeitgesteuerte Treiber 108 (Time threshold) schreibt in den flüchtigen Speicher 102 (RAM, SD-RAM) Daten, und löscht diese Daten sobald für eine im Betriebsprogamm eingestellte Zeit lang (time-out) nicht mehr auf diese Daten zugegriffen wurde. Das Löschen geschieht durch automatisches Überschreiben der Daten mit vom Treiber zufällig generierten Bytes. Wird anschließend versucht, die Daten auszulesen, gibt der Treiber nur die zuvor zufällig eingestellten Daten aus.

[0053] Der kryptographisch verschlüsselnde Treiber 106 schreibt Daten in verschlüsselter Form in den nicht-flüchtigen Speicher 103 (z.B. Flash), wofür er einen fest einprogrammierten Schlüssel einer symmetrischen Blockchiffre verwendet. Sollen diese Daten anschließend wieder ausgelesen werden, so entschlüsselt der Treiber die Daten zuerst mit demselben fest einprogrammierten Schlüssel.

[0054] Der Programmcode zur Steuerung des Frankiergeräts steht vorzugsweise im Programmspeicher 105 (NV-Memory), zum Beispiel in einem Flash-Speicher, kann aber alternativ auch in einem EPROM Baustein stehen. Letztere Variante ist preiswert, aber nicht so flexibel, weil ein Austausch des Betriebsprogramms einen Wechsel des EPROM Bausteins erfordert. Die Kommunikation innerhalb des Frankiergeräts läuft über einen internen Bus 110 und wird gesteuert durch die Speichermanagementeinheit 117 (MMU) beim Speichern von Daten. Der flüchtige Speicher (volatile memory) 107 ist als Arbeitsspeicher vorgesehen.

[0055] Das Kommunikations-Interface 109 kann über ein - mit gezeigtes - internes oder externes Modem zum Datenaustausch mit einem Betreiber-Datenzentrum verbunden sein oder mit einem anderen geeigneten Kommunikationsgerät. Die Kommunikationsverbindungen, das Kommunikationsnetz und die Kommunikationsgeräte an den Enden der Kommunikationsverbindungen bilden in bekannter Weise die Kommunikationsmittel.
Die vorgenannten Mittel 103 bis 107 bilden ein Schlüsselgenerierungsmittel, das durch Berechnen für jedes nächste Frankierbild einen neuen Frankierbildschlüssel generiert. Dabei wird vom unmittelbar vorhergehenden Frankierbildschlüssel ausgegangen. Letzterer und ein Kommunikationsschlüssel sind beide im nichtflüchtigen Speicher 103 gespeichert. Die Berechnung wird unter Verwendung eines ersten und zweiten Krypto-Algorithmus vor dem Frankieren durchgeführt, wobei für ein erstes Frankierbild ein erster Integritäts-Checkcode basierend auf dem zweiten Krypto-Algorithmus erzeugt wird, wobei für jedes nachfolgende Frankierbild ein nachfolgender Frankierbildschlüssel aus einem Vorgänger des Frankier-bildschlüssels nach dem ersten Krypto-Algorithmus abgeleitet und ein Integritäts-Checkcode erzeugt wird, basierend auf dem nachfolgenden Frankierbildschlüssel, einer Schlüsselgenerationsnummer, einer Gerätekennung des Frankiergeräts und basierend auf dem zweiten Krypto-Algorithmus.

[0056] Ein PIMD 10 kann mit seinem Betreiber-Datenzentrum 14 gesichert kommunizieren, wofür üblicherweise ein in beide Richtungen authentisiertes und optional verschlüsseltes Kommunikationsprotokoll verwendet wird. Übliche Verfahren basieren auf einem Protokoll für key agreement (Henk C. A. van Tilborg: Encyclopedia of Cryptography and Security; Springer-Verlag New York, 2005, Seite 325) oder key establishment.

[0057] In der Fig. 3 wird eine Darstellung der Ebenen des Speicherschutzes gezeigt. Nach Eingabe 200 einer Gerätekennung *g* (device-ID) und des aktuellen Passwortes, wird eine erste Routine 201 zum Verarbeiten der Daten durchlaufen, um ein Passwort durch ein Zufalls und Datenmix (salt & hash) zu bilden und in einer Datei im nichtflüchtigen Speicher 101 softwaregeschützt intern zu speichern. Die erste Routine 201 führt somit zu einer Passwortspeicherung auf einer unteren Ebene des Speicherschutzes. Nach der ersten Routine 201 folgt eine zweite Routine 202 zum Ableiten eines interen Verschlüsselungsschlüssels *IMDKey* und zu dessen zeitgesteuerten Speicherung in einer *IMDKey*-Datei im flüchtigen Speicher 102. Die zweite Routine 202 führt somit zu einer flüchtigen Speicherung auf einer mittleren Ebene des Speicherschutzes.
Nach der zweiten Routine 202 folgt eine dritte Routine 203 zum Verschlüsseln von Schlüsseln *COMKey* und *IDAKey* mittels des interen Verschlüsselungsschlüssels *IMDKey* und eine verschlüsselte interne flüchtige Speicherung von Daten im flüchtigen Speicher 103, wobei die Daten die verschlüsselten Schlüssel enthalten. Die dritte Routine 203 führt somit zu einer flüchtigen Speicherung auf einer oberen Ebene des Speicherschutzes.
Das PIMD verwendet vorzugsweise zwei Schlüssel bzw. Schlüsselpaare zur Sicherung seiner Interaktionen mit Nachbar-Systemen. Für die elektronische Kommunikation mit dem Betreiberdatenzentrum wird ein Kommunikationsschlüssel *COMKey* verwendet. Dies kann ein symmetrischer Schlüssel sein. Alternativ kann ein asymmetrisches Schlüsselpaar

eingesetzt werden. Im Fall eines asymmetrischen Schlüsselpaars bezeichnen wir den privaten Kommunikationsschlüssel als *COMPrivKey* und den öffentlichen Kommunikationsschlüssel als *COMPubKey.*

Für die Frankierabdrucke, die von dem betreffenden Postbeförderer im Postbeförderdatenzentrum bei der Postbeförderung gelesen und ausgewertet werden, wird ein geheimer Frankierbildschlüssel *IDAKey* zur Bildung des Integritäts-Checkcode *M* verwendet, wobei letzterer beim Frankieren auf das Poststück aufgedruckt wird. Dies ist vorzugesweise ein symmetrischer Schlüssel.

Beide Schlüssel *COMKey* und *IDAKey* bzw. *COMPrivKey* und *IDAKey* sind in einem verschlüsselten internen Speicherbereich, beispielsweise im flüchtigen Speicher 103, des Postal Identity Management Device (PIMD) abgelegt und werden nur bei Bedarf entschlüsselt. Nach Gebrauch werden die Klartextkopien beider Schlüssel sofort gelöscht und die entsprechenden Speicherbereiche mit zufälligen Bitmustern überschrieben, so dass die Klarschlüssel nicht von Unbefugten ausgelesen werden können.

[0058] Für die Verschlüsselung des geheimen Kommunikationsschlüssels *COMKey* bzw. des privaten Kommunikationsschlüssels *COMPrivKey* und des geheimen Frankierbildschlüssels *IDAKey* wird ein interer Verschlüsselungsschlüssel *IMDKey* für eine symmetrische Blockchiffre, zum Beispiel Advanced Encryption Standard (AES), verwendet. Dieser interne Verschlüsselungsschlüssel *IMDKey* wird nicht permanent im Klartext abgespeichert, sondern wird jeweils bei Bedarf aus dem Passwort algorithmisch abgeleitet. Klartextkopien des internen Verschlüsselungsschlüssel *IMDKey* werden temporär im flüchtigen Speicher 102 gehalten (time controlled internal storage) und dort wieder gelöscht, sobald ihre Verweilzeit (time-out) abgelaufen ist, ohne dass sie verwendet wurden.

[0059] Für ein neues Passwort wird ein zufälliger Bitstring (salt) generiert (Henk C. A. van Tilborg: Encyclopedia of Cryptography and Security; Springer-Verlag New York, 2005, Seite 541). Der zufällige Bitstring wird an das vom Benutzer gewählte Passwort angehängt. Das Ergebnis wird durch eine Hashfunktion (ebenda, hash function, Seite 256-264) auf einen Hashwert (zum Beispiel SHA256) abgebildet und aus diesem wird der Frankierbildschlüssel *IDAKey* abgeleitet, indem der Hashwert entweder direkt verwendet oder einer Hashfunktion unterworfen wird. Das Paar aus Salt und Hashwert zu einem Passwort werden anschließend in der Passwort-Datei indiziert nach Passworten abgespeichert (soft protected internal memory). Um diesen Speicher gegen unbefugtes Auslesen zu schützen, werden Software-Verschleierungstechniken eingesetzt, die zum Beispiel einen Datensatz in mehreren Teilen ablegen, die im Speicher 101 an unterschiedlichen Adressen stehen.

[0060] Zu den Hauptprozessen des Betreibens eines PIMD gehören:

- eine Initialisierung (Fig.4) des PIMDs,
- ein Wechseln (Fig.5) eines bestehenden Passworts und
- eine Berechnung (Fig.6) des Frankierabdrucks.

[0061] Zu den Unterprozessen des Betreibens eines PIMD gehören:

- eine Geräte-ID Authentikation (Fig.7),
- ein Senden (Fig.8) von Frankierbildschlüsseln (IDAKey).

[0062] Die Fig. 4 zeigt als Routine 400 einen Flussplan zur Initialisierung eines PIMDs. Nach dem Start der PIMD Initialisierung im Schritt 401 und einer Eingabe der Geräte-ID und eines neuen Passworts in das PIMD im Schritt 402 erfolgt im Schritt 403 eine Abfrage nach neuen Passworten. Bei einer Passworteingabe über die Tastatur des Frankiergerätes sind beispielsweise die neuen Passworte diejenigen, die doppelt eingegeben wurden. Bei der erstmaligen Eingabe eines Passwortes via Tastatur muss folglich eine Doppeleingabe der Passworte erfolgen. Damit soll aber weder ein mehrmaliges Eingeben von gleichen Passworte ausgeschlossen werden, noch eine einmaliges Eingeben eines Passwortes, wobei das Frankiergerät auf eine andere Art und Weise erkennen kann, dass eine Routine 400 zur Initialisierung eines PIMDs ablaufen soll. Zum Beispiel erfolgt bei einer ersten Eingabe eine Eingabe der Art der Routine, die ablaufen soll und in einer zweiten Eingabe eine Passworteingabe, oder umgekehrt. Alternativ sind andere Varianten der Passworteingabe als per Hand möglich, vorausgesetzt das Frankiergerät besitzt eine entsprechend angepasste Schnittstelle. Beispielsweise kann die Passworteingabe via Chipkarte erfolgen, was voraussetzt dass das Frankiergerät eine Schreib/Leseeinheit für Chipkarten besitzt. Auch muss dann folglich keine Doppeleingabe der Passworte erfolgen, wenn auf eine andere Weise festgestellt werden kann, ob beabsichtigt ist, ein bisheriges durch ein neues aktuelles Passwort zu ersetzen.

Nachfolgend erfolgt im Schritt 404 ein Verarbeiten des Passworts durch einen ansich bekannten Prozess (salt & hash-Prozess), auf welchen oben bereits in Verbindung mit Fig.3 hingewiesen wurde. Im Schritt 405 erfolgt ein Einspeichern des neuen Passworts in einer Passwort-Schlüsseldatei im nicht-flüchtigen Speicher 101. Auf den Schritt 404 folgend wird im Schritt 406 ein neuer Verschlüsselungsschlüssel $IMDKey_k$ vom neuen Hash-Wert abgeleitet, der im Schritt 404 gebildet wurde. Nach dem Ableiten des neuen Verschlüsselungsschlüssels $IMDKey_k$ im Schritt 406 wird im Schritt 407 der neue Verschlüsselungsschlüssel $IMDKey_k$ zeitgesteuert intern im flüchtigen Speicher 102 gespeichert. Im auf den

Schritt 406 folgenden Schritt 408 kann nun ein Generieren eines neuen Kommunikationsschüssels *COMKey* und Frankierbildschlüssels $IDAKey_1$ erfolgen. Diese beiden Schlüssel werden im darauf folgenden Schritt 409 im Crypto-Treiber 106 zu Daten D_{k1} verschlüsselt, die anschließend im nach folgenden Schritt 410 intern flüchtig gespeichert werden. Der Frankierbildschlüssel $IDAKey_1$ ist ein erster Schlüssel, welcher zur Bildung eines Integritäts-Checkcode M verwendet wird. Der *COMKey* ist ein Kommunikationsschlüssel für die elektronische Kommunikation mit dem Betreiberdatenzentrum. Ein Verschlüsseln der beiden Schüssel *COMKey* und $IDAKey_1$ erfolgt im Schritt 409 durch Anwendung des neuen Verschlüsselungsschlüssels $IMDKey_k$ beim Verschlüsseln nach einem der bekannten Verschlüsselungsalgoritmen, beispielsweise nach dem Avanced Encryption Standard (AES)-Algorithmus nach Formel (9):

$$AES(IMDKey_k, (COMKey, IDA\ Key_1)) \rightarrow D_{k1} \qquad (9)$$

[0063] Nach der im Schritt 410 erfolgten internen Speicherung der Daten D_{k1} der verschlüsselten Schüssel *COMKey* und $IDAKey_1$ wird im nachfolgenden Schritt 411 der Unterprozess gemäß Fig. 8 durchgeführt und der erste Frankierbildschlüssel $IDAKey_1$ gesendet. Während der Initialisierung des Frankiergeräts werden außer dem ersten Frankierbildschlüssel $IDAKey_1$ auch die Gerätekennung *g* des Frankiergeräts und die Schlüsselgenerationsnummer *i* an das Datenzentrum des Postbeförderers übermittelt. Im anschließenden Schritt 412 ist die Initialisierung des PIMD vollständig.

[0064] Die Arbeitsweise der Initialisierung eines PIMDs gehört zu den Hauptprozessen und endet mit der Übermittlung des erzeugten ersten Frankierbildschlüssels $IDAKey_1$ an den Postbeförderer über ein gesichertes Kommunikationsprotokoll.

[0065] Der Postbeförderer registriert daraufhin das neue Frankiergerät mit dessen Gerätekennung *g,* seiner ersten Schlüsselgenerationsnummer *i* und dem zugehörigen Frankierbildschlüssel $IDAKey_i$, welche zur Bildung eines Integritäts-Checkcode M verwendet werden. Die erste Schlüsselgenerationsnummer *i* hat vorzugsweise den Wert 'Eins'.

[0066] Die Fig. 5 zeigt als Routine 500 einen Flussplan beim Wechseln eines Gerätepassworts. Die Routine 500 des PIMDs führt zur Änderung des Passworts, d.h. zur Aktualisierung des Passworts des PIMDs. Nach dem Start eines Wechselns des Passworts im ersten Schritt 501 und einer Eingabe der Geräte-ID und des vorherigen Passworts in das PIMD im zweiten Schritt 502 erfolgt im dritten Schritt 503 eine Echtheitsüberprüfung der Geräte-ID. Ist die Echtheitsüberprüfung der Geräte-ID fehlgeschlagen, dann wird auf einen vierten Schritt 504 verzweigt und die Routine 500 endet. Anderenfalls falls die Echtheitsüberprüfung der Geräte-ID erfolgreich war, dann wird zur Abfrage nach neuen Passworten auf einen sechsten Schritt 506 verzweigt. Nach einer Eingabe eines neuen Passworts im fünften Schritt 505, kann im sechsten Schritt 506 eine Abfrage nach dem neu eingegebenen Passwort erfolgen. Beispielsweise kann bei einer Handeingabe via Tastatur des Frankiergerätes im fünften Schritt 505 ein neues Passwort doppelt eingegeben werden und im sechsten Schritt 506 wird nach einer solchen doppelten Eingabe eines neuen Passworts gefragt. Alternativ kann nach anderen Kriterien festgestellt werden, ob die Eingabe eines neuen Passwortes beabsichtigt ist.

Der Benutzer kann also ein neues Passwort etablieren, indem er es zweimal identisch eingibt. Das Frankiergerät kann gegebenenfalls auf eine andere Art und Weise erkennen, dass eine Routine 500 zum Wechseln des Passworts ablaufen soll. Alternativ sind andere Varianten der Passworteingabe als per Hand möglich, was voraussetzt, dass das Frankiergerät eine entsprechend angepasste Schnittstelle besitzt. Mit der Passwort-Eingabe oder alternativ mittels RFID-Ausweis, Magnetkarte, Chipkarte, mobiles Gerät (Handy, Organizer), welche über persönliches Netzwerk (Bluetooth, USB, etc.) mit dem Frankiergerät kommunikativ verbunden werden können, wird ein Missbrauch der Gerätekennung *g* des Absender-Frankiergeräts erschwert.

Nachdem die Authentikation der Geräte-ID im dritten Schritt 503 und die Abfrage im sechsten Schritt 506 erfolgreich war, erfolgt eine Verarbeitung des neuen Passwortes nach dem sogenannten salt & hash-Prozess in einem siebenten Schritt 507 zu einem neuen Hash-Wert $Hash_{k+1}$. Der vorgenannte Prozess ist identisch mit der ersten Routine 201 zum Verarbeiten der Daten, die anhand der Darstellung in Fig.3 bereits erläutert wurde bzw. mit dem vierten Schritt 404 der Routine 400, welche gemäß der Fig.4 durchlaufen wird.

Nach dem salt & hash-Prozess im siebenten Schritt 507 wird das neue Passwort in einer Passwort- und Schlüsseldatei in einem achten Schritt 508 gespeichert und zum neunten Schritt 509 weitergesteuert, zur Entnahme von intern gespeicherten Daten D_k, wobei die Daten die verschlüsselten Schlüssel enthalten. Die verschlüsselte interne Speicherung der Schlüssel im flüchtigen Speicher 103 erfolgte in Form von Daten D_k bereits vor der Routine 500 im Schritt 410 (Fig.4) oder 203 (Fig 3). Die entnommenen Daten D_k werden mittels des aktiven internen Schlüssels $IMDKey_k$ zu den beiden in Klartext benötigten Schlüsseln entschlüsselt. Dabei handelt es sich um den geheimen Frankierbildschlüssel $IDAKey_k$ und den geheimen Kommunikationsschlüssel *COMKey* bzw. privaten Kommunikationsschlüssel *COMPubKey.* Auf den neunten Schritt 509 folgend erfolgt im zehnten Schritt 510 ein Ableiten eines neuen internen Verschlüsselungsschlüssels $IMDKey_{k+1}$ vom neuen Hash-Wert $Hash_{k+1}$, der im siebenten Schritt 507 ermittelt wurde. In einem dem zehnten Schritt 510 nachfolgenden elften Schritt 511 erfolgt ein Rückverschlüsseln der benötigten Schlüssel mittels des neuen *IMD-*

Key_{k+1}, wobei sich die benötigten Schlüssel aus der Entschlüsselung im neunten Schritt 509 ergeben. Die Rückverschlüsselung erfolgt wieder beispielsweise nach dem Advanced Encryption Standard (AES)-Algorithmus nach der Formel (10) zu den neuen verschlüsselten Daten D_{k+1}:

$$AES(\ IMDKey_{k+1},\ (COMKey_k,\ IDA\ Key_k\ ))\ \rightarrow\ D_{k+1} \qquad (10)$$

[0067] In einem dem elften Schritt 511 nachfolgenden zwölften Schritt 512 erfolgt dann wieder eine interne flüchtige Speicherung der neuen verschlüsselten Daten D_{k+1} im flüchtigen Speicher 103. Im Ergebnis des zehnten Schrittes 510 erfolgt außerdem in einem dreizehnten Schritt 513 eine zeitgesteuerte interne flüchtige Speicherung des neuen internen Verschlüsselungsschlüssels $IMDKey_{k+1}$ im flüchtigen Speicher 102. Das Wechseln des Passworts ist im vierzehnten Schritt 514 vollständig.

[0068] Die Fig. 6 zeigt als Routine 600 einen Flussplan zum Berechnen eines Frankierabdrucks. Die Routine 600 zum Berechnen eines Frankierabdrucks gehört zu den Hauptprozessen. Nach dem Start einer Bearbeitung der Daten eines Frankierabdrucks im ersten Schritt 601 erfolgt im zweiten Schritt 602 eine Abfrage, ob eine erneute Authentifizierung der Geräte-ID nötig sei, weil der Zeitablauf der Speicherung des IMDKeys erfolgt ist.

Ist das der Fall, dann kann - in nicht gezeigter Weise - eine Meldung zum Beispiel via Display erfolgen, welche den Benutzer des Frankiergerätes zu einer Eingabe der Geräte-ID und des Passwortes auffordert.

Anschließend erfolgt im dritten Schritt 603 eine Eingabe der Geräte-ID und des Passworts bevor im vierten Schritt 604 ein Unterprozess des Betreibens eines PIMD zwecks einer Authentifizierung der Geräte-ID abläuft. Ist eine Authentifizierung der Geräte-ID nicht möglich, dann wird ein Schritt 605 erreicht und eine Meldung zur Anzeige gebracht, dass die Authentifizierung fehlgeschlagen ist.

Anderenfalls, wenn die Abfrage im zweiten Schritt 602 ergibt, dass eine erneute Authentifizierung der Geräte-ID unnötig ist oder wenn die Authentifizierung der Geräte-ID im vierten Schritt 604 erfolgreich war, dann wird auf einen sechsten Schritt 606 verzweigt. Im sechsten Schritt 606 werden die im flüchtigen Speicher 103 verschlüsselt intern gespeicherten Daten D_i mittels des aktiven $IMDKey_i$ zu den Klartextschlüsseln entschlüsselt. Dabei handelt es sich um den geheimen Frankierbildschlüssel $IDAKey_i$ und den geheimen Kommunikationsschlüssel $COMKey_i$ bzw. privaten Kommunikationsschlüssel $COMPubKey_i$. Nun erfolgt ein Bilden eines Integritäts-Checkcodes M nach der vorgenannten Formel (1) oder (2).

Nach Eingabe von Frankierdaten und -bilddaten in einem siebenten Schritt 607 erfolgt in einem achten Schritt 608 eine Verarbeitung der Frankierdaten und -bilddaten zusammen mit dem Integritäts-Checkcode M, um im Ergebnis der Routine 600 einen einzigartigen Frankierabdruck zu erzeugen. Auf den achten Schritt 608 folgend, wird in einem neunten Schritt 609 die Schlüsselgenerationsnummer i für die auf die aktuelle Frankierung folgende nächste der Frankierung um den Wert Eins erhöht. Nach dem Inkrementieren im neunten Schritt 609 erfolgt im nachfolgenden zehnten Schritt 610 ein Ableiten eines nächsten Verschlüsselungsschlüssels $IMDKey_i$, ein Verschlüsseln der Schlüssel $IDAKey_i$ und $COMKey_i$ mittels des aktiven $IMDKey_i$ und eine verschlüsselte interne Speicherung der Schlüssel $IDAKey_i$ und $COMKey_i$. Im weiteren elften Schritt 611 erfolgt ein Überschreiben der Klarschlüssel und des Verschlüsselungsschlüssels in den flüchtigen Speichern 102 und 103. Mit einem zwölften Schritt 612 kann eine Meldung über die Integrität des Checkkodes ausgegeben werden. Mit dem dreizehnten Schritt 613 ist die Routine 600 zum Berechnen eines Frankierabdrucks vollständig.

[0069] Die Fig. 7 zeigt als erste Sub-Routine 700 einen Flussplan zur Echtheitsüberprüfung einer Geräte-ID. Die Sub-Routine 700 gehört zu den Unterprozessen des Betreibens eines PIMD, die in beiden Hauptprozessen nach Fig. 5 und 6 sowie im Unterprozess nach Fig. 8 benötigt wird. Die beim Durchlaufen der Sub-Routine veranlasste Arbeitsweise des PIMDs wird im ersten Schritt 701 gestartet und führt zur Geräte-ID-Authentikation. Nach dem Start erfolgt im zweiten Schritt 702 der ersten Sub-Routine 700 eine Eingabe der Geräte-ID und des Passworts, wobei dann, wenn die Eingabe im dritten Schritt 703 bestätigt wird, ein vierten Schritt 704 der ersten Sub-Routine 700 erreicht wird, um eine salt & hash-Verarbeitung des Passworts durchzuführen. Anschließend erfolgt im sechsten Schritt 706 eine Abfrage, ob ein aktueller Hash-Wert gleich einem Hash-Wert für die Geräte-ID ist. Dabei wird im siebenten Schritt 707 auf eine Hash-Datenbank mit einer Liste von Gerätepasswörtern und Benutzernamen zugegriffen, um den Hash-Wert für die Geräte-ID aufzufinden. Ergibt die Abfrage im sechsten Schritt 706 keine Gleichheit, dann wird auf einen fünften Schritt 705 verzweigt und eine Meldung ausgegeben, dass die Authentifizierung fehlgeschlagen sei.

Anderenfalls erfolgt eine Verzweigung auf einen achten Schritt 708 zum Ableiten eines Verschlüsselungsschlüssels vom aktuellen Hash-Wert. Der Verschlüsselungsschlüssel wird zeitgesteuert intern gespeichert, bis der Zeitablauf der Speicherung des *IMDKeys* eintritt (Schritt 709). Damit ist auch der zehnte Schritt 710 der ersten Sub-Routine 700 erreicht und die Authentikation ist vollständig.

[0070] Die Fig. 8 zeigt als zweite Sub-Routine 800 einen Flussplan beim Senden eines Frankierbildschlüssels des

PIMD's an das Datenzentrum des Postbeförderers. Das Senden von Frankierbildschlüsseln *IDAKey* gehört zu den Unterprozessen des Betreibens eines PIMD. Anhand der zweiten Sub-Routine 800 wird die Arbeitsweise der Übermittlung eines *IDAKey* eines PIMD näher dargestellt. Diese zweite Sub-Routine wird benötigt, wenn ein PIMD am Ende seiner Initialisierung seinen *IDAKey* an den Postbeförderer übermittelt. Der Unterprozess des Sendens des Schlüssels eines Frankierabdrucks wird im ersten Schritt 801 gestartet und erreicht einen zweiten Schritt 802 zwecks Abfrage, ob eine erneute Authentifizierung wegen Zeitablauf der Speicherung des *IDAKey* nötig sei. Ist das der Fall, dann kann zum Schritt 804 der zweiten Sub-Routine verzweigt werden. Unter der Voraussetzung, dass eine Eingabe (Schritt 803) der Geräte-ID und des Passwortes erfolgt, kann - in der gezeigten Weise - die erste Sub-Routine 700, d.h. ein Unterprozess nach Fig. 7 zur Geräte-ID-Authentifizierung ablaufen. Anderenfalls wird zum sechsten Schritt 806 der zweiten Sub-Routine 800 verzweigt, wenn keine erneute Authentifizierung wegen Zeitablauf der Speicherung des internen Verschlüsselungsschlüssels *IMDKey* nötig ist. Eine erneute Geräte-ID-Authentifizierung wird damit umgangen und im sechsten Schritt 806 der zweiten Sub-Routine 800 erfolgt ein Entschlüsseln der Daten D mittels des internen Verschlüsselungsschlüssels *IMDKey* zu den Klarschlüsseln *COMKey* und $IDAKey_1$. Im nachfolgenden siebenten Schritt 807 der zweiten Sub-Routine erfolgt ein Verschlüsseln des ersten Frankierbildschlüssels $IDAKey_1$ und weiterer Parameter, wie mindestens die Gerätekennung *g* des Frankiergeräts und die Schlüsselgenerationsnummer *i*, mittels des Kommunikationsschlüssels *COMKey* nach der Formel (11):

$$AES(COMKey, F(g, i, IDAKey_1)) \rightarrow D1 \qquad (11)$$

und ein Senden der Daten *D1* des mit einem Kommunikationsschlüssels *COMKey* verschlüsselten Frankierbildschlüssels $IDAKey_1$ und weiterer Parameter *g* und i, welche durch eine mathematische Funktion F miteinander verknüpft worden sind, wobei die mathematische Funktion F dem Datenzentrum des Postbeförderers bekannt ist.

[0071] Die Daten *D1* werden zum Datenzentrum des Postbeförderers übertragen und dort empfangen und entschlüsselt. Der Empfang des Frankierbildschlüssels $IDAKey_1$ und weiterer Parameter *g* und *i* wird bestätigt.
Im achten Schritt 808 der zweiten Sub-Routine 800 erfolgt ein Empfangen der Empfangsbestätigung des Kommunikationspartners. Im nachfolgenden neunten Schritt 809 der zweiten Sub-Routine 800 werden die Klarschlüsseln *COMKey* und $IDAKey_1$ mit zufälligen Daten überschrieben. Damit ist der Unterprozess des Sendens des ersten Frankierbildschlüssels $IDAKey_1$ im zehnten Schritt 810 der zweiten Sub-Routine 800 vollständig.
Vorzugsweise geht der erste Frankierbildschlüssel $IDAKey_1$ dem Datenzentrum 7 des Postbeförderers indirekt über das Datenzentrum 14 des Betreibers bzw. Hersteller des Frankiergeräts zu. Alternativ ist das Datenzentrum 7 des Postbeförderers der direkte Kommunikationspartner.

[0072] In der vorgenannten Berechnungs-Routine 600 erfolgt nach der Bildung eines Checkcodes M im Schritt 606 und nach dessen Verarbeitung im Schritt 608 ein Ableiten des nächsten Frankierbildschlüssels im Schritt 610. Die Reihenfolge kann auch umgedreht werden, indem zuerst ein Ableiten des nächsten Frankierbildschlüssels erfolgt und dann eine Bildung eines Checkcodes M und dessen Verarbeitung vorgenommen wird. Bei der Reihenfolge der Schritte bei einer Überprüfung der Frankierdaten in der Datenzentrale muss natürlich eine entsprechende Reihenfolge gewählt werden, so dass nach dem Abtasten des Frankierbildes oder einer Markierung des Poststückes bei der Erzeugung von neuen Frankierbild-schlüsseln wieder eine Synchronität erreicht wird.

[0073] Die vorgenannte Passwort-Wechsel-Routine 500 kann die Abfrage nach einem neuen Passwort nach anderen Kriterien erfolgen, als im Ausführungsbeispiel dargestellt wurde. Die Eingabe des neuen Passwortes selbst kann auf andere Weise erfolgen, als im Ausführungsbeispiel dargestellt wurde.

[0074] Die vorgenannten Routinen können den für die verschiedenen Länder unterschiedlichen Postvorschriften angepasst werden und sinngemäß verwendet werden.

[0075] Wenn in den vorgenannten Beispielen von Poststücken, Briefkuverten oder Frankierstreifen gesprochen wird, dann sollen andere Formen von Druckgütern nicht ausgeschlossen werden. Vielmehr sollen alle Poststücke mit eingeschlossen sein, die von Frankiervorrichtungen mit einem Frankierbild versehen werden können. Das Aufbringen eines Frankierbildes soll ein Aufbringen einer Markierung nicht ausschließen. Das Aufbringen eines Frankierbildes soll nicht auf ein Bedrucken eines Poststückes beschränkt bleiben, vielmehr sollen andere Formen des Aufbringens von mindestens einem Frankierbild oder einer Markierung nicht ausgeschlossen werden.

[0076] Es können weitere andere Ausführungen der Erfindung entwickelt bzw. eingesetzt werden, die vom gleichen Grundgedanken der Erfindung ausgehen und von den anliegenden Ansprüchen umfasst werden.

Patentansprüche

1. Frankierverfahren mit zentraler Portoerhebung im Datenzentrum eines Postbeförderers, mit Generierung eines

ersten Frankierbildschlüssels $IDAKey_1$ während einer Initialisierung des Frankiergeräts, mit Erzeugung eines Frankierbildes mittels des Frankiergeräts, und mit einer vom Frankiergerät entfernten Auswertung des Frankierbildes, **gekennzeichnet durch** die Schritte:

- Übermitteln des ersten Frankierbildschlüssels $IDAKey_1$ zur entfernten Auswertung von zu überprüfenden Frankierbildern auf Poststücken,
- Berechnung eines Frankierbilds vor der Erzeugung einer Frankierung,

wobei für jedes Frankierbild ein neuer Frankierbildschlüssel aus einem Vorgänger des Frankierbildschlüssels nach einem ersten Krypto-Algorithmus abgeleitet und wobei ein Integritäts-Checkcode *M* basierend auf dem neuen Frankierbildschlüssel, einer Schlüsselgenerationsnummer *i*, einer Gerätekennung *g* des Frankiergeräts und basierend auf einem zweiten Krypto-Algorithmus erzeugt wird, wobei das Frankierbild, mindestens die Gerätekennung *g* des Frankiergeräts, die Schlüsselgenerationsnummer *i* und dem Integritäts-Checkcode *M* aufweist,

- Befördern und Einliefern von Poststücken in ein Briefzentrum des Postbeförderers nach dem Frankieren, Abtasten und Prüfung von Frankierbildern beim Postbeförderer, wobei der Integritäts-Checkcode *M* kryptographisch verifiziert wird, indem ein Vergleichs-Integritäts-Checkcode zum Vergleich mit dem aufgedruckten Integritäts-Checkcode gebildet wird und wobei Gebühren zur zentralen Buchung erfaßt werden, welche dem Absender der Poststücke zeitlich entkoppelt von der Buchung am Ende der Abrechnungsperiode in Rechnung gestellt werden sowie
- Fehlerbehandlung beim Prüfen.

2. Verfahren, nach Anspruch 1, **gekennzeichnet durch** die Schritte:

- Datenübermittlung mindestens einer Gerätekennung *g* des Frankiergeräts, einer ersten Schlüsselgenerationsnummer i_1 und des ersten Schlüssels $IDAKey_1$ an ein entferntes Datenzentrum des Postbeförderers vor dem Ende der Initialisierung (400) des Frankiergeräts, und verschlüsselte interne Speicherung des generierten ersten Frankierbildschlüssels $IDAKey_1$ im flüchtigen Speicher des Frankiergeräts,
oder
Erzeugen eines nach einem ersten Krypto-Algorithmus abgeleiteten Frankierbildschlüssels $IDAKey_i$ und verschlüsselte interne Speicherung des abgeleiteten Frankierbildschlüssels $IDAKey_i$,
- Erkennen eines Frankierauftrags **durch** das Frankiergerät für ein zu bedruckendes Poststück und Start der Berechnung eines Frankierbildes mit Erzeugen eines Integritäts-Checkcodes *M* nach einem zweiten Krypto-Algorithmus, wobei das Erzeugen aus der Gerätekennung *g* des Frankiergeräts, der Schlüsselgenerationsnummer *i* und des ersten Frankierbildschlüssels $IDAKey_1$ oder eines abgeleiteten Frankierbildschlüssels $IDAKey_i$ erfolgt, wobei der verschlüsselt intern gespeicherte erste Frankierbildschlüssel oder abgeleitete Frankierbildschlüssel mittels eines Verschlüsselungsschlüssels *IMDKey* zu einem Klartextschlüssel $IDAKey_1$ oder $IDAKey_i$ entschlüsselt wird,
- Verarbeiten der Frankierbilddaten mit dem Integritäts-Checkcode *M*,
- Bedrucken des Poststücks mit einem Frankierbild, welches eine Markierung mit mindestens der Gerätekennung *g* des Frankiergeräts, der Schlüsselgenerationsnummer *i* und dem Integritäts-Checkcode *M* aufweist,
- schrittweises Verändern der Schlüsselgenerationsnummer i um einen festgelegten Zahlenwert *h,* Ableiten des nächsten Frankierbildschlüssels $IDAKey_{i \mp h}$ aus der aktuellen Schlüsselgenerationsnummer $i \mp$ h, Verschlüsselung mindestens des nächsten Frankierbildschlüssels $IDAKey_{i \mp h}$ und eines Kommunikationsschlüssels *COMKey* mittels des Verschlüsselungsschlüssels *IMDKey* und verschlüsselte interne Speicherung des nächsten Frankierbildschlüssels $IDAKey_{i \mp h}$ und des Kommunikationsschlüssels *COMKey* sowie Überschreiben der Klartextschlüssel *COMKey* und $IDAKey_{i \mp h}$ und dessen Vorgängers $IDAKey_i$ im flüchtigen Speicher des Frankiergeräts,
- Transportieren der vom Frankiergerät frankierten Poststücke zum Briefzentrum **durch** den Postbeförderer,
- Einliefern des Poststücks im Briefzentrum des Postbeförderers und Scannen des Frankierbilds und Auswerten der gescannten Daten mittels eines Prüfablaufs im Datenzentrum des Postbeförderers,

wobei der gescannte Integritäts-Checkcode *M* mit einem aktuellen Schlüssel kryptographisch verifiziert wird,

- zentrale Portoerhebung im Datenzentrum des Postbeförderers, wenn die Echtheit des Integritäts-Checkcodes *M* vorliegt, wobei eine Synchronität zwischen Frankiergerät und Datenzentrum hergestellt wird bzw.
- Durchführung einer Fehlerbehandlungsroutine, wenn die Echtheit des Integritäts-Checkcodes *M* nicht nachgewiesen wurde bzw. eine fehlerhafte Gerätekennung *g* des Frankiergeräts oder fehlerhafte Schlüsselgenera-

tionsnummer i vorliegt.

3. Verfahren, nach den Ansprüchen 1 und 2, **gekennzeichnet dadurch, dass** die Schlüsselgenerationsnummer i mit jeder Frankierung um den Wert $h = 1$ erhöht oder verringert wird.

4. Verfahren, nach den Ansprüchen 1 bis 3, **gekennzeichnet dadurch, dass** für eine nächste Schlüsselgenerationsnummer i + 1 das Ableiten des nächsten Frankierbildschlüssels $IDAKey_i + 1$ aus der aktuellen Schlüsselgenerationsnummer i und dem aktuellen Frankierbildschlüssel $IDAKey_i$ nach dem ersten Krypto-Algorithmus gemäß der Formel erfolgt:

$$IDAKey_{i+1} \leftarrow hash\,(\,i,\ IDAKey_i\,).$$

5. Verfahren, nach den Ansprüchen 1 bis 4, **gekennzeichnet durch, dass** ein hash-basierter Mitteilungs-Authentikationss-Code (HMAC) als erster Krypto-Algorithmus verwendet wird.

6. Verfahren, nach den Ansprüchen 1 bis 5, **gekennzeichnet dadurch, dass** das Erzeugen eines Integritäts-Checkcodes M nach einem zweiten Krypto-Algorithmus mittels eines geheimen kryptographischen Frankierbildschlüssels $IDAKey_i$ des Absenders, der Gerätekennung g des Frankiergeräts und deren aktuellen Schlüsselgenerationsnummer i nach der Formel:

$$M \leftarrow HMAC(\,IDAKey_i, (g \,||\, i))$$

erfolgt.

7. Verfahren, nach den Ansprüchen 1 bis 5, **gekennzeichnet dadurch, dass** das Erzeugen eines Integritäts-Checkcodes M nach einem zweiten Krypto-Algorithmus mittels eines geheimen kryptographischen Frankierbildschlüssels $IDAKey_i$ des Absenders, der Gerätekennung g des Frankiergeräts und deren aktuellen Schlüsselgenerationsnummer i nach der Formel:

$$M \leftarrow HMAC(\,IDAKey_i, f(g,\ i,\ IDAKey_i))$$

erfolgt.

8. Verfahren, nach einem der Ansprüche 1 bis 6 oder 7, **gekennzeichnet dadurch, dass** ein Auswerten der gescannten Daten mittels eines Prüfablaufs im Datenzentrum des Postbeförderers, eine Ermittlung der mathematischen Beziehung der abgetasteten Schlüsselgenerationsnummer $i \mp x$ zu der Kopie j der zuletzt verwendeten Schlüsselgenerationsnummer umfasst, wobei ein aktueller Frankierbildprüfschlüssel $IDAKey_j \mp h$ berechnet wird, der dem abgetasteten Frankierbildschlüssels entspricht, wenn die mathematische Beziehung gleich einer vorgegebenen mathematischen Beziehung $J = j + x$ mit $x = h \cdot z$ ist, wobei sich der Wert x der Veränderung der Kopie j der zuletzt verwendeten Schlüsselgenerationsnummer aus dem Produkt jedes einzelnen Schrittwertes h mit der Anzahl z an Veränderungen ergibt und wobei das Poststück einer Aussortierung und die abgetasteten Daten einer Fehlerbehandlung unterworfen werden, wenn die mathematische Beziehung der vorgegebenen mathematischen Beziehung nicht entspricht.

9. Verfahren, nach Anspruch 8, **gekennzeichnet durch, dass** das Poststück an den Absender zurückgesandt wird, wenn die mathematische Beziehung der abgetasteten Schlüsselgenerationsnummer $i \mp x$ zu der Kopie j der zuletzt verwendeten Schlüsselgenerationsnummer der vorgegebenen mathematischen Beziehung nicht entspricht und wenn der Absender des Poststücks benachrichtigt worden ist und einer Rücksendung zugestimmt hat.

10. Verfahren, nach Anspruch 8, **gekennzeichnet durch, dass** das Poststück zum Empfänger transportiert wird, wenn

die mathematische Beziehung der abgetasteten Schlüsselgenerationsnummer $i \mp x$ zu der Kopie j der zuletzt verwendeten Schlüsselgenerationsnummer der vorgegebenen mathematischen Beziehung nicht entspricht und wenn der Empfänger des Poststücks benachrichtigt worden ist und einer Zustellung zugestimmt hat.

11. Verfahren, nach einem der Ansprüche 1 bis 10, **gekennzeichnet dadurch, dass** die Weiterverarbeitung von abgetasteten Daten beim Postbeförderer in einer Routine (300) erfolgt, welche eine Dekodierung (301) der abgetasteten Daten, eine Ermittlung des jeweiligen Absenders (302), eine Ermittlung (303) der jeweiligen Portogebühr, eine Sicherheitsüberprüfung (304) jedes Frankierbildes und eine zentrale Buchung (306) der Portogebühr auf ein Konto des Absenders umfasst sowie dass ein Transport (4) und eine Auslieferung (5) von ordnungsgemäß frankierten Poststücken an die Empfänger oder Aussonderung von Poststücken im Briefzentrum erfolgt, wenn die Weiterverarbeitung der abgetasteten Daten in der Routine (300) nicht möglich ist, wobei

- die Ermittlung des jeweiligen Absenders (302) eine Suche nach der Gerätekennung g des Frankiergeräts in einer Datenbank des Briefzentrums oder Datenzentrums und nach der zugehörig gespeicherten Kopie j der zuletzt verwendeten Schlüsselgenerationsnummer umfasst, zu der ein zugehörig gespeicherter Frankierbildschlüssel existiert,
- die Sicherheitsüberprüfung (304) jedes Frankierbildes, eine Ermittlung der mathematischen Beziehung der abgetasteten Schlüsselgenerationsnummer $i \mp x$ zu der Kopie j der zuletzt verwendeten Schlüsselgenerationsnummer sowie eine kryptographische Verifizierung des Integritäts-Checkcodes M umfasst, wobei ein Frankierbildprüfschlüssel $IDAKey_J$ der dem aktuellen nachfolgenden Frankierbildschlüssel $IDAKey_{i \mp x}$ des Frankiergeräts entspricht, nach dem ersten Krypto-Algorithmus erzeugt, wobei letzterer entsprechend der Ermittlung der mathematischen Beziehung z-Mal angewendet wird sowie wobei Frankierbildprüfschlüssel $IDAKey_J$ zusammen mit der Kopie J der aktuell verwendeten Schlüsselgenerationsnummer $i \mp x$ und mit der Gerätekennung g zur Bildung eines Vergleichs-Integritäts-Checkcodes $Mref$ nach dem zweiten Krypto-Algorithmus verwendet wird.

12. Verfahren, nach Anspruch 1, **gekennzeichnet durch, dass** mindestens **durch** eine Passworteingabe die Sicherheit der Gerätekennung g gewährleistet wird.

13. Verfahren, nach Anspruch 12, **gekennzeichnet durch, dass** vor einem Berechnen eines Frankierbildes die Eingabe des bestehenden Passworts und der Gerätekennung g und dessen Authentizität abgefragt wird, wenn eine vorbestimmte Zeitdauer zur Speicherung des internen Verschlüsselungsschlüssels $IMDKey_k$ abgelaufen ist.

14. Verfahren, nach Anspruch 12, **gekennzeichnet durch, dass** vor der Berechnung eines Frankierbilds das bestehenden Passwort bedarfsweise gewechselt wird und vor einem Wechseln des bestehenden Passworts die Eingabe des bestehenden Passworts und der Gerätekennung g und dessen Authentizität abgefragt wird.

15. Verfahren, nach Anspruch 12, **gekennzeichnet durch, dass** die Sicherheit der Gerätekennung **durch** eine Kombination von Maßnahmen gewährleistet wird:

a) Passwort-Eingabe via Tastatur oder alternativ mittels RFID-Ausweis, Magnetkarte, Chipkarte, mobiles Gerät (Handy, Organizer) verbunden über persönliches Netzwerk (Bluetooth, USB, etc.) auf der Frankiergeräteseite,
b) Authentikation der Gerätekennung in jedem Frankierabdruck auf der Postbefördererseite, um die Verwendung falscher Gerätekennungen auszuschließen.
c) Einmal-Authentikation der Gerätekennung in jedem Frankierabdruck auf der Postbefördererseite, um die Wiederverwendung kopierter Authentikationen falscher Gerätekennungen auszuschließen.
d) Sicherung der Kommunikations-Verbindung mindestens zum Betreiber-Datenzentrum **durch** Verschlüsselung.
e) Verwaltung separate Benutzerkonten **durch** ein an sich bekanntes Betriebssystem eines Personalcomputers in Verbindung mit dem Einsatz von Multi-User-Frankiergeräten.

16. Verfahren, nach Anspruch 15, **gekennzeichnet durch, dass** über eine gesicherte Kommunikations-Verbindung ein generierter erster Frankierbildschlüssel $IDAKey_1$ während einer Initialisierung des Frankiergeräts zum Datenzentrum eines Betreibers und anschließend zum Datenzentrum des Postbeförderers übermittelt wird.

17. Postversandsystem mit zentraler Portoerhebung, mit einem Briefzentrum und einem Datenzentrum eines Postbeförderers, einem Datenzentrum eines Betreibers von einer Vielzahl an Frankiergeräten, wobei der Postbeförderer die vom Frankiergerät frankierten Poststücke zum Briefzentrum transportiert und wobei jedes Frankiergerät über

eine Kommunikationsverbindung via Netz und über eine Kommunikationsverbindung bedarfweise in Kontakt mit dem Betreiber-Datenzentrum steht, welches die Gerätekennung seiner Benutzer registriert und zusätzliche Dienste anbietet,
gekennzeichnet dadurch,

- **dass** das Frankiergerät ein Schlüsselgenerierungsmittel enthält, das für jedes nächste Frankierbild einen neuen Frankierbildschlüssel generiert,
- **dass** Kommunikationsmittel vorgesehen sind und über die Kommunikationsverbindung eine Synchronität zwischen Frankiergerät und Datenzentrum bedarfsweise hergestellt wird,
- **dass** Abtastmittel im Briefzentrum und erste Auswertemittel im Datenzentrum eines Postbeförderers vorgesehen sind, die kommunikativ miteinander verbunden sind, wobei durch die ersten Auswertemittel der Absender des Poststückes über eine in einer Datenbank gespeicherte Zuordnung der Gerätekennung zu einem Absender bestimmt und durch Portoberechnungsmittel die Portogebühr ermittelt wird,
- **dass** die Auswertemittel im Datenzentrum zweite Mittel zur Sicherheitsüberprüfung jedes abgetasteten Frankierbildes einschließen, welche dann, wenn sich zwischen der abgetasteten Schlüsselgenerationsnummer und ihrer berechneten Kopie und zwischen dem geheimen kryptographischen Frankierbildschlüssel und dem berechneten Frankierbildprüfschlüssel Synchronität herstellen lässt, einen Vergleichs-Integritäts-Checkcode im Datenzentrum berechnen, um den abgetasteten Integritäts-Checkcode kryptographisch zu verifizieren,
- **dass** Mittel zur Buchung der Portogebühren für Poststücke desselben Absenders auf ein separates Konto und zur Fehlerbehandlung im Datenzentrum des Postbeförderers vorgesehen sind, wobei die zentrale Portoerhebung dann durchgeführt wird, wenn die Echtheit des Integritäts-Checkcodes nachweislich vorliegt.

18. Postversandsystem, nach dem Anspruch 17, **gekennzeichnet dadurch, dass** die zweiten Mittel zur Sicherheitsüberprüfung so programmiert sind, dass eine Ermittlung der mathematischen Beziehung der abgetasteten Schlüsselgenerationsnummer zu der Kopie der zuletzt verwendeten Schlüsselgenerationsnummer erfolgt, wobei ein Frankierbildprüfschlüssel, der dem aktuellen nachfolgenden Frankierbildschlüssel des Frankiergeräts entspricht, nach dem ersten Krypto-Algorithmus erzeugt wird, wobei letzterer entsprechend der ermittelten mathematischen Beziehung z-Mal angewendet wird sowie wobei der Frankierbildprüfschlüssel zusammen mit der Kopie der aktuell verwendeten Schlüsselgenerationsnummer und mit der Gerätekennung zur Bildung eines Vergleichs-Integritäts-Checkcodes nach dem zweiten Krypto-Algorithmus verwendet wird.

19. Postversandsystem, nach dem Anspruch 17, **gekennzeichnet dadurch, dass** die Weiterverarbeitung von abgetasteten Daten beim Postbeförderer im Briefzentrum oder im Datenzentrum des Postbeförderers erfolgt.

20. Postversandsystem, nach dem Anspruch 17, **gekennzeichnet dadurch, dass** das Schlüsselgenerierungsmittel des Frankiergeräts programmiert sind, eine Berechnung unter Verwendung eines ersten und zweiten Krypto-Algorithmus vor dem Frankieren durchzuführen, wobei für ein erstes Frankierbild ein erster Integritäts-Checkcode basierend auf dem zweiten Krypto-Algorithmus erzeugt wird, wobei für jedes nachfolgende Frankierbild ein nachfolgender Frankierbildschlüssel aus einem Vorgänger des Frankierbildschlüssels nach dem ersten Krypto-Algorithmus abgeleitet und ein Integritäts-Checkcode erzeugt wird, basierend auf dem nachfolgenden Frankierbildschlüssel, einer Schlüsselgenerationsnummer, einer Gerätekennung des Frankiergeräts und basierend auf dem zweiten Krypto-Algorithmus.

21. Postversandsystem, nach den Ansprüchen 17 bis 19, **gekennzeichnet dadurch, dass** ein nicht-flüchtiger Speicher (101) für eine Passwortspeicherung auf einer unteren Ebene des Speicherschutzes, ein flüchtiger Speicher (102) für eine zeitgesteuerte Speicherung des intenen Verschlüsselungsschlüssels *IMDKey* in einer *IMDKey*-Datei auf einer mittleren Ebene des Speicherschutzes sowie dass ein flüchtiger Speicher (103) für eine verschlüsselte interne flüchtige Speicherung von Daten auf einer oberen Ebene des Speicherschutzes vorgesehen sind, wobei die Daten im flüchtigen Speicher (103) den Frankierbildschlüssel *IDAKey* und den Kommunikationsschlüssel *COMKey* in verschlüsselter Form enthalten.

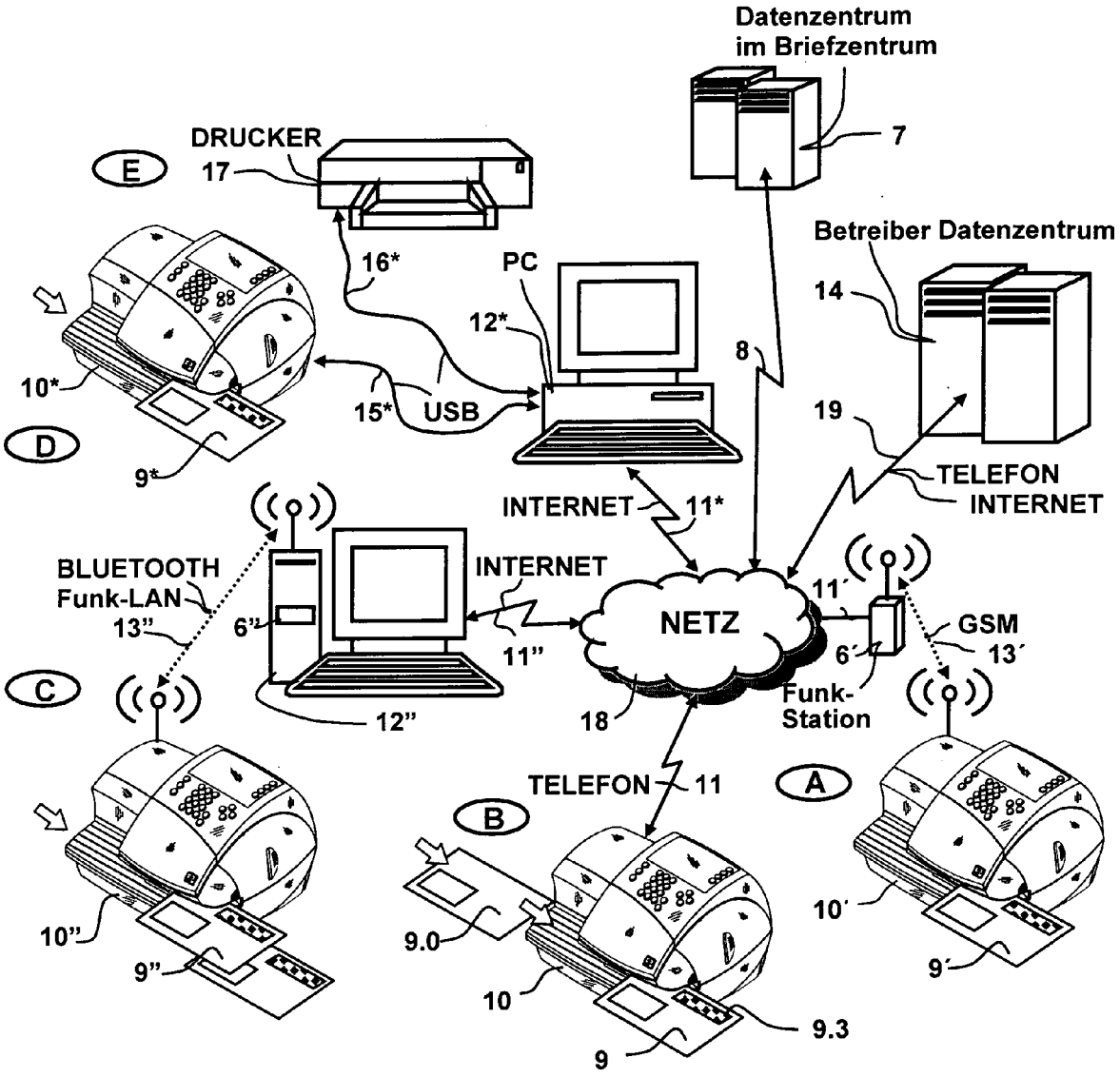
Datenzentrum
im Briefzentrum
7
DRUCKER
17
E
16*
PC
12*
Betreiber Datenzentrum
14
8
10*
15*
USB
19
D
9*
TELEFON
INTERNET
INTERNET
11*
BLUETOOTH
Funk-LAN
13"
INTERNET
6"
NETZ
11´
GSM
13´
6´
11"
C
Funk-
Station
18
12"
TELEFON
11
A
B
10"
9"
9.0
10´
9´
10
9.3
9

Fig. 1a

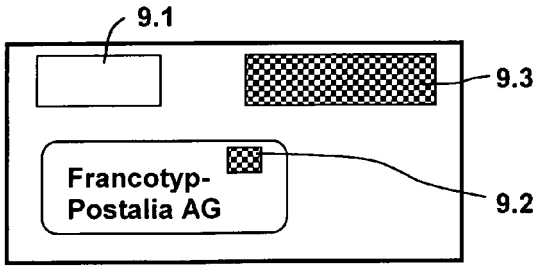
9.1
9.3
Francotyp-
Postalia AG
9.2

Fig. 1b

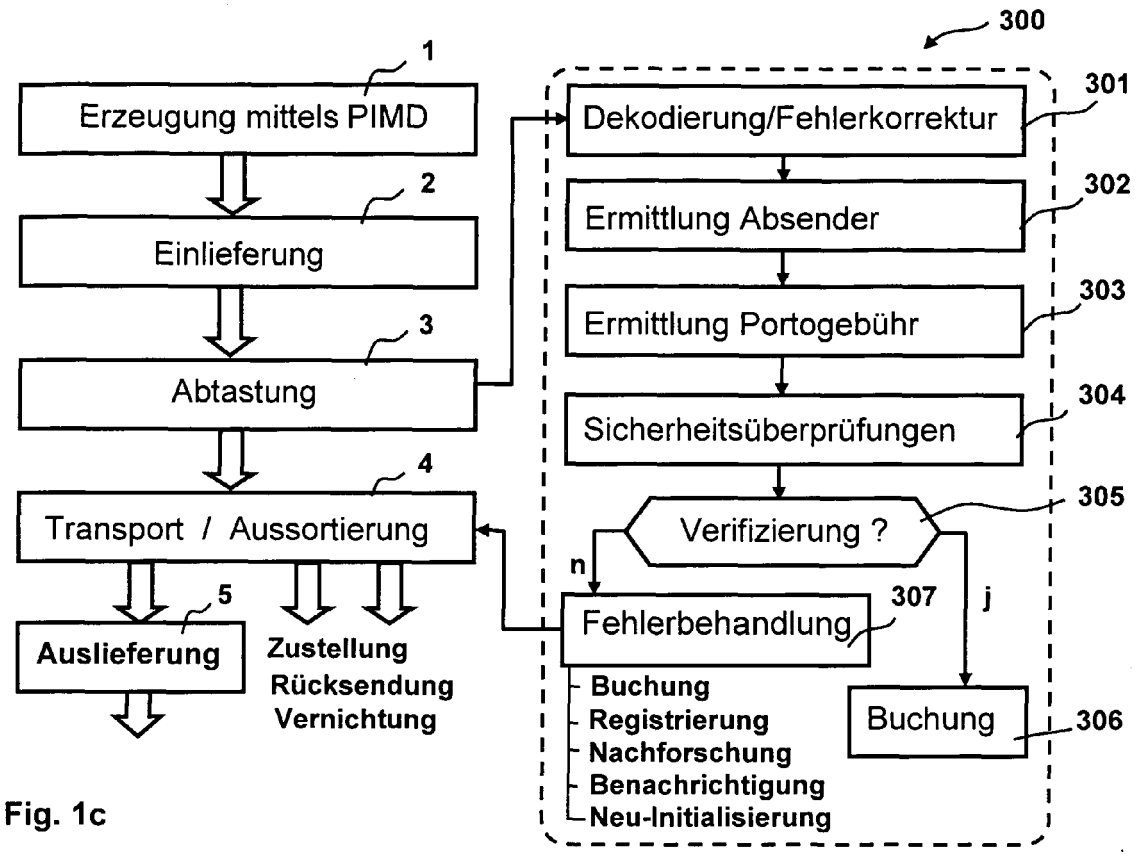
300
1
Erzeugung mittels PIMD
2
Einlieferung
3
Abtastung
4
Transport / Aussortierung
5
Auslieferung
Zustellung
Rücksendung
Vernichtung
301
Dekodierung/Fehlerkorrektur
302
Ermittlung Absender
303
Ermittlung Portogebühr
304
Sicherheitsüberprüfungen
305
Verifizierung ?
n
j
307
Fehlerbehandlung
Buchung
Registrierung
Nachforschung
Benachrichtigung
Neu-Initialisierung
Buchung
306

Fig. 1c

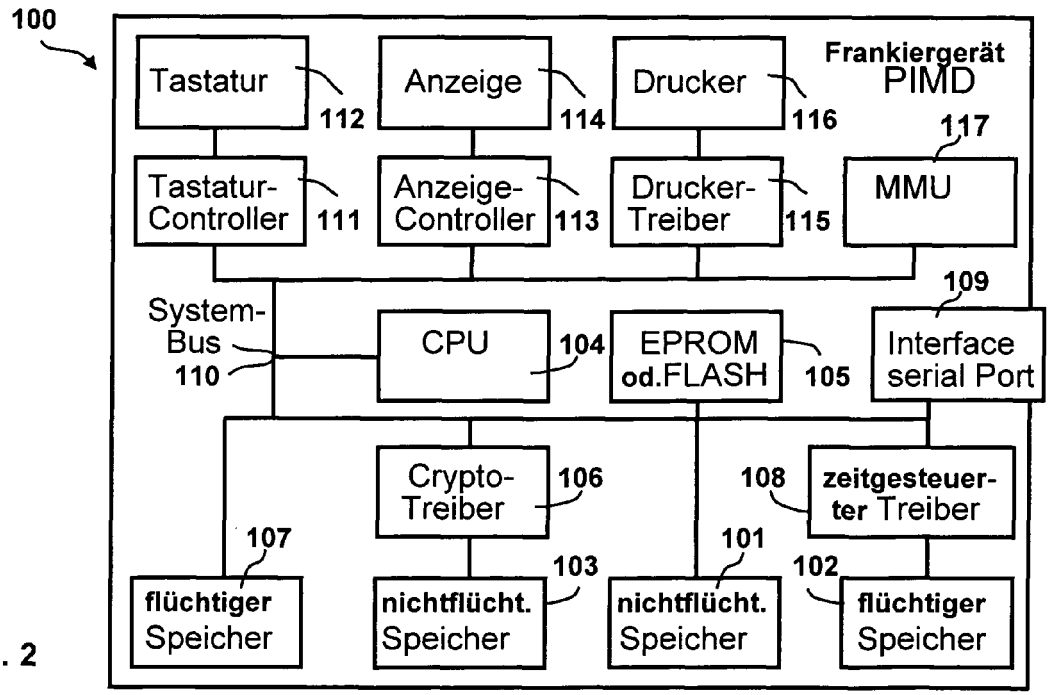
100
Frankiergerät
PIMD
Tastatur
112
Anzeige
114
Drucker
116
117
Tastatur-
Controller
111
Anzeige-
Controller
113
Drucker-
Treiber
115
MMU
109
System-
Bus
110
CPU
104
EPROM
od.FLASH
105
Interface
serial Port
Crypto-
Treiber
106
108
zeitgesteuer-
ter Treiber
107
flüchtiger
Speicher
103
nichtflücht.
Speicher
101
nichtflücht.
Speicher
102
flüchtiger
Speicher

Fig. 2

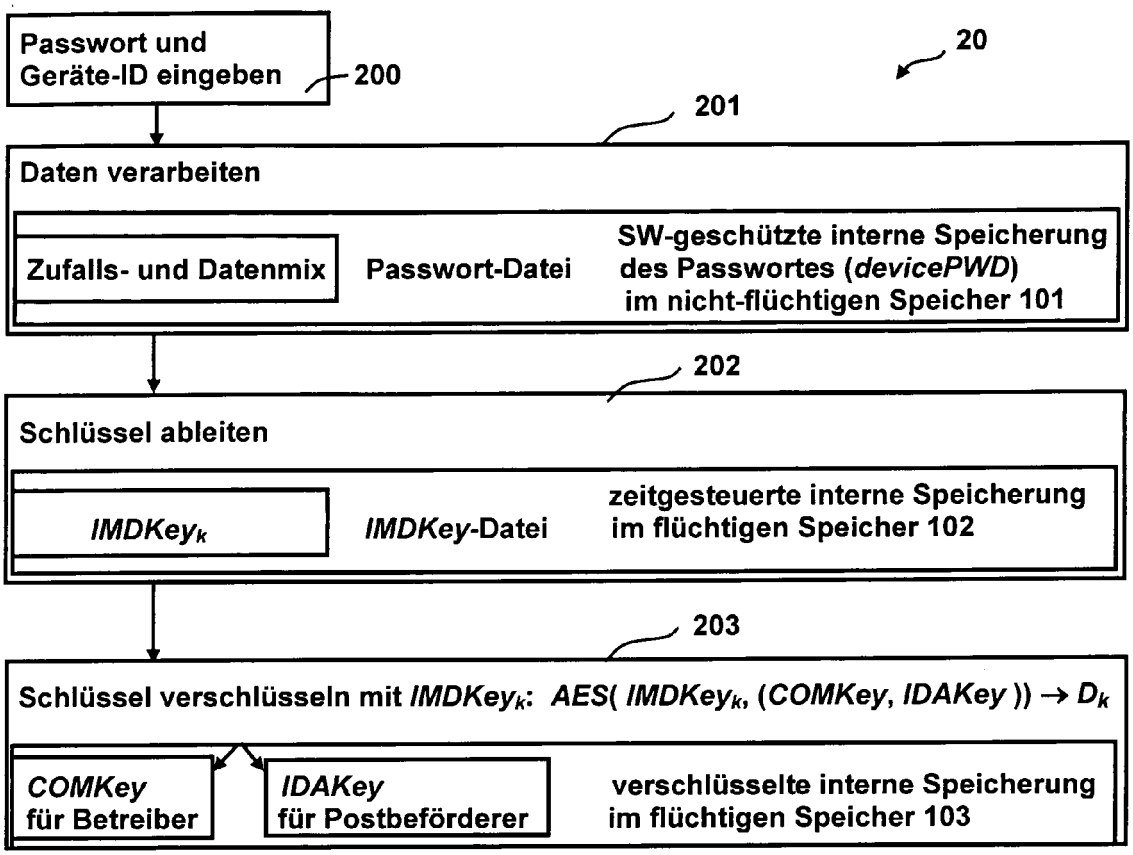
Passwort und
Geräte-ID eingeben
200
20
201
Daten verarbeiten
Zufalls- und Datenmix
Passwort-Datei
SW-geschützte interne Speicherung
des Passwortes (devicePWD)
im nicht-flüchtigen Speicher 101
202
Schlüssel ableiten
IMDKey_k
IMDKey-Datei
zeitgesteuerte interne Speicherung
im flüchtigen Speicher 102
203
Schlüssel verschlüsseln mit IMDKey_k: AES(IMDKey_k, (COMKey, IDAKey)) → D_k
COMKey
für Betreiber
IDAKey
für Postbeförderer
verschlüsselte interne Speicherung
im flüchtigen Speicher 103

Fig. 3

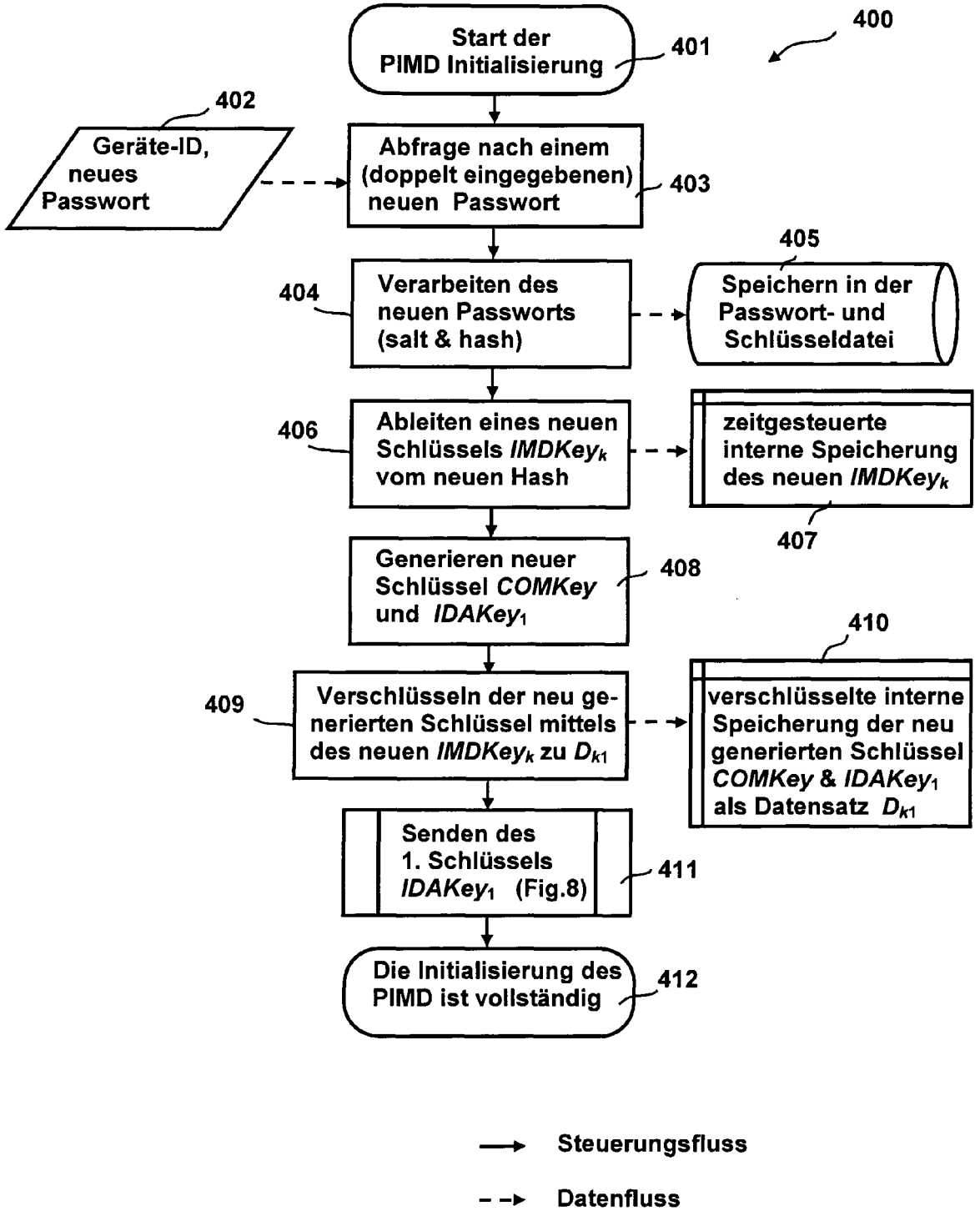
400
Start der PIMD Initialisierung
401
402
Geräte-ID, neues Passwort
Abfrage nach einem (doppelt eingegebenen) neuen Passwort
403
405
404
Verarbeiten des neuen Passworts (salt & hash)
Speichern in der Passwort- und Schlüsseldatei
406
Ableiten eines neuen Schlüssels IMDKey$_k$ vom neuen Hash
zeitgesteuerte interne Speicherung des neuen IMDKey$_k$
407
Generieren neuer Schlüssel COMKey und IDAKey$_1$
408
410
409
Verschlüsseln der neu generierten Schlüssel mittels des neuen IMDKey$_k$ zu D_{k1}
verschlüsselte interne Speicherung der neu generierten Schlüssel COMKey & IDAKey$_1$ als Datensatz D_{k1}
Senden des 1. Schlüssels IDAKey$_1$ (Fig.8)
411
Die Initialisierung des PIMD ist vollständig
412
Steuerungsfluss
Datenfluss

Fig. 4

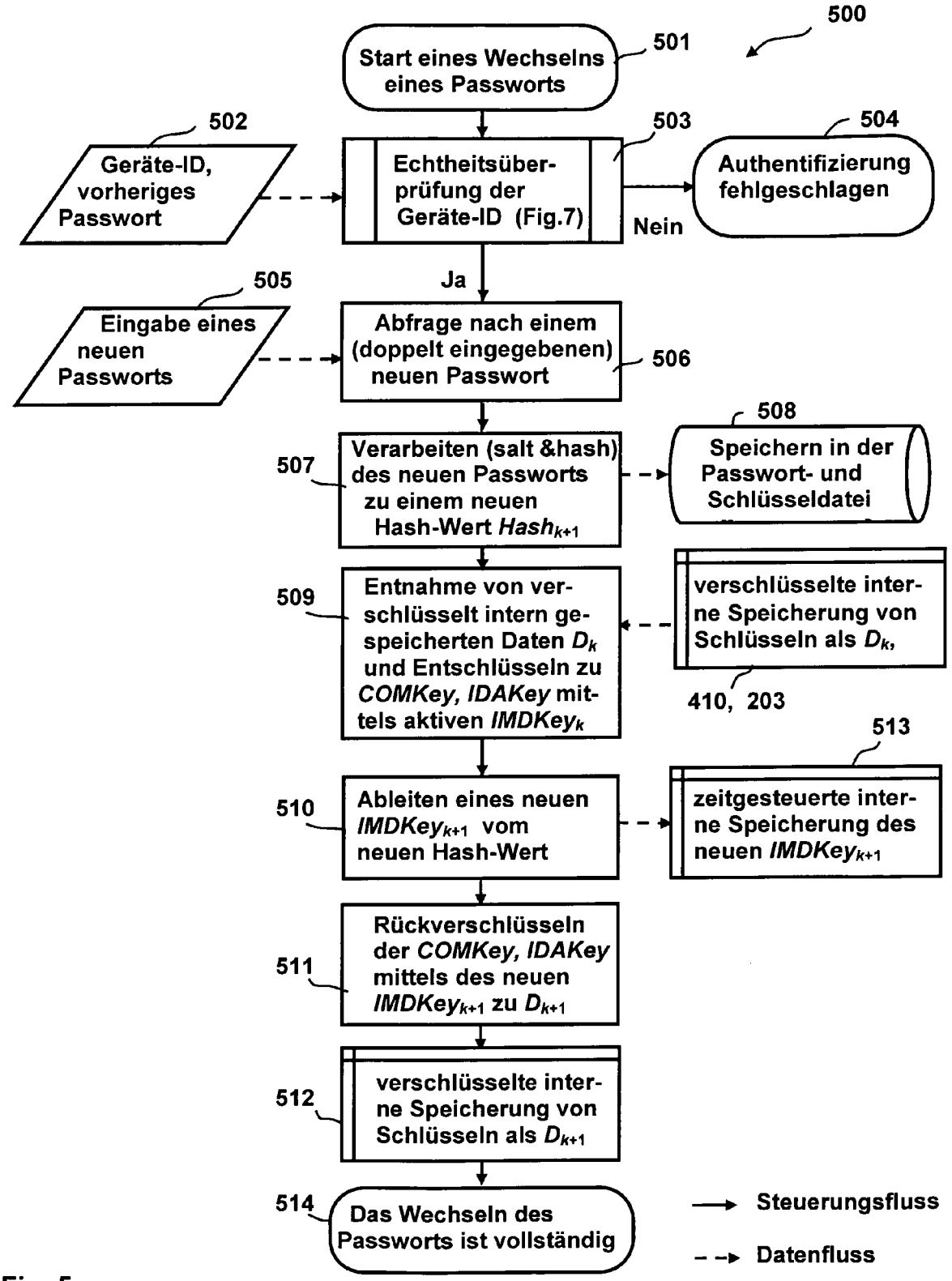
500
Start eines Wechselns eines Passworts
501
502
Geräte-ID, vorheriges Passwort
503
Echtheitsüberprüfung der Geräte-ID (Fig.7)
504
Authentifizierung fehlgeschlagen
Nein
Ja
505
Eingabe eines neuen Passworts
Abfrage nach einem (doppelt eingegebenen) neuen Passwort
506
508
Speichern in der Passwort- und Schlüsseldatei
507
Verarbeiten (salt &hash) des neuen Passworts zu einem neuen Hash-Wert $Hash_{k+1}$
509
Entnahme von verschlüsselt intern gespeicherten Daten D_k und Entschlüsseln zu *COMKey, IDAKey* mittels aktiven $IMDKey_k$
verschlüsselte interne Speicherung von Schlüsseln als D_k,
410, 203
513
510
Ableiten eines neuen $IMDKey_{k+1}$ vom neuen Hash-Wert
zeitgesteuerte interne Speicherung des neuen $IMDKey_{k+1}$
511
Rückverschlüsseln der *COMKey, IDAKey* mittels des neuen $IMDKey_{k+1}$ zu D_{k+1}
512
verschlüsselte interne Speicherung von Schlüsseln als D_{k+1}
514
Das Wechseln des Passworts ist vollständig
Steuerungsfluss
Datenfluss

Fig. 5

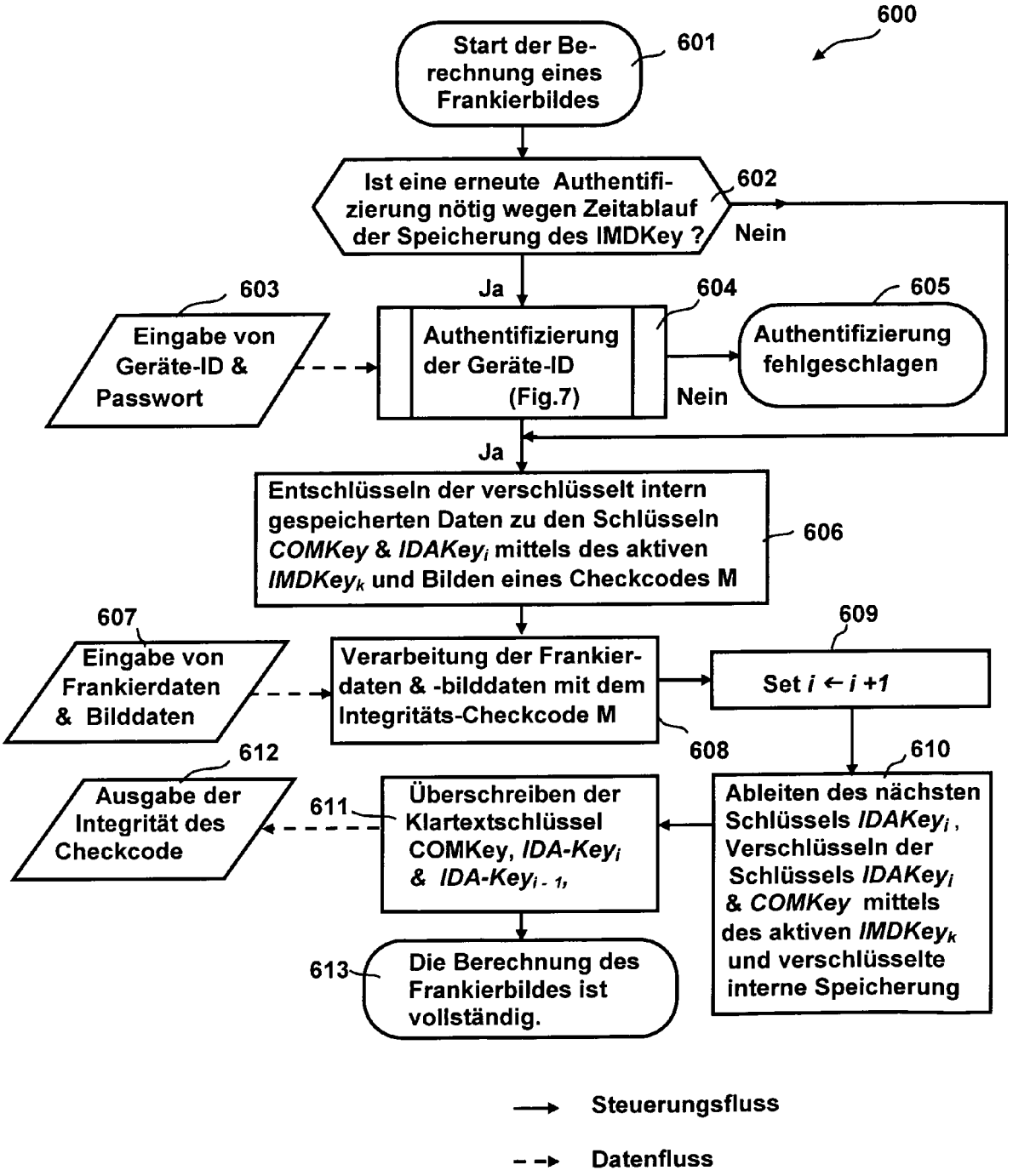
600
Start der Berechnung eines Frankierbildes
601
Ist eine erneute Authentifizierung nötig wegen Zeitablauf der Speicherung des IMDKey ?
602
Nein
Ja
603
Eingabe von Geräte-ID & Passwort
Authentifizierung der Geräte-ID (Fig.7)
604
Nein
Authentifizierung fehlgeschlagen
605
Ja
Entschlüsseln der verschlüsselt intern gespeicherten Daten zu den Schlüsseln COMKey & IDAKey$_i$ mittels des aktiven IMDKey$_k$ und Bilden eines Checkcodes M
606
607
Eingabe von Frankierdaten & Bilddaten
Verarbeitung der Frankierdaten & -bilddaten mit dem Integritäts-Checkcode M
608
609
Set $i \leftarrow i+1$
610
612
Ausgabe der Integrität des Checkcode
611
Überschreiben der Klartextschlüssel COMKey, IDA-Key$_i$ & IDA-Key$_{i-1}$,
Ableiten des nächsten Schlüssels IDAKey$_i$, Verschlüsseln der Schlüssels IDAKey$_i$ & COMKey mittels des aktiven IMDKey$_k$ und verschlüsselte interne Speicherung
613
Die Berechnung des Frankierbildes ist vollständig.
Steuerungsfluss
Datenfluss

Fig. 6

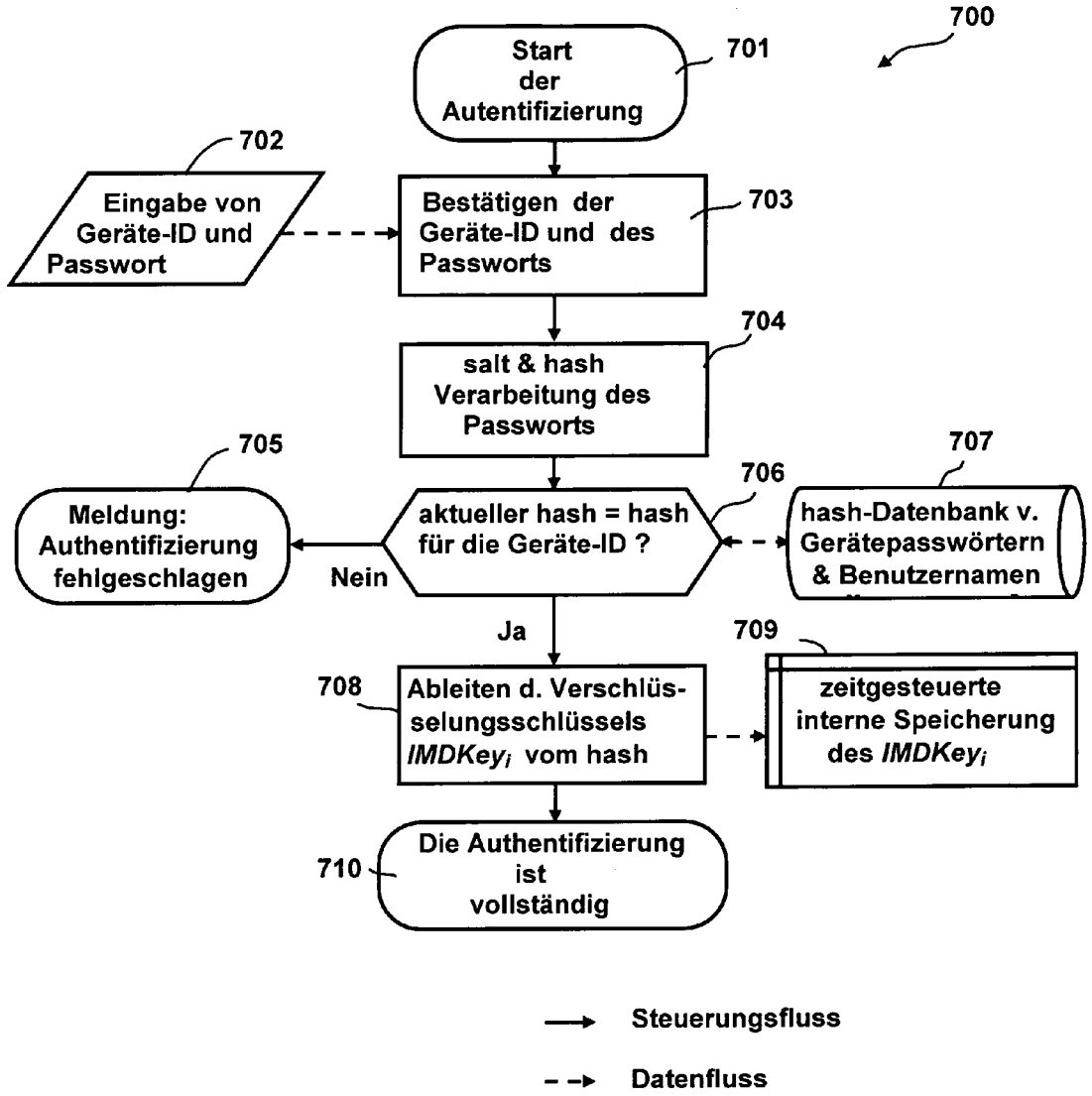
700
Start der Autentifizierung
701
702
Eingabe von Geräte-ID und Passwort
Bestätigen der Geräte-ID und des Passworts
703
704
salt & hash Verarbeitung des Passworts
705
707
706
Meldung: Authentifizierung fehlgeschlagen
Nein
aktueller hash = hash für die Geräte-ID ?
hash-Datenbank v. Gerätepasswörtern & Benutzernamen
Ja
709
708
Ableiten d. Verschlüsselungsschlüssels IMDKey$_i$ vom hash
zeitgesteuerte interne Speicherung des IMDKey$_i$
710
Die Authentifizierung ist vollständig
Steuerungsfluss
Datenfluss

Fig. 7

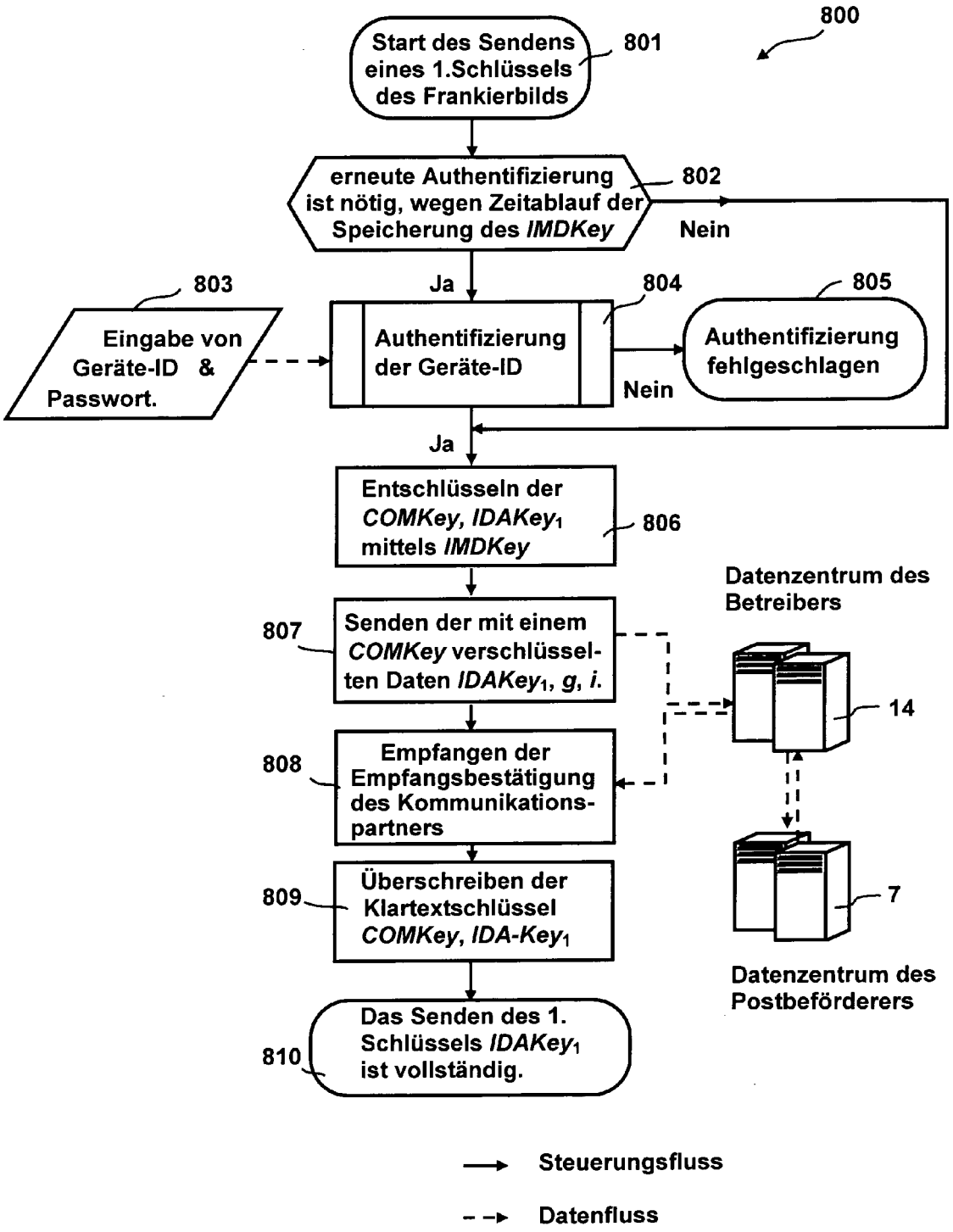
800
Start des Sendens eines 1.Schlüssels des Frankierbilds
801
erneute Authentifizierung ist nötig, wegen Zeitablauf der Speicherung des IMDKey
802
Nein
Ja
803
Eingabe von Geräte-ID & Passwort.
804
Authentifizierung der Geräte-ID
805
Authentifizierung fehlgeschlagen
Nein
Ja
Entschlüsseln der COMKey, IDAKey1 mittels IMDKey
806
Datenzentrum des Betreibers
807
Senden der mit einem COMKey verschlüsselten Daten IDAKey1, g, i.
14
808
Empfangen der Empfangsbestätigung des Kommunikationspartners
809
Überschreiben der Klartextschlüssel COMKey, IDA-Key1
7
Datenzentrum des Postbeförderers
810
Das Senden des 1. Schlüssels IDAKey1 ist vollständig.
Steuerungsfluss
Datenfluss

Fig. 8

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 08 01 7285

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
A	GB 2 211 144 A (PITNEY BOWES INC [US]) 28. Juni 1989 (1989-06-28) * Zusammenfassung * * Seite 1, Zeile 3 - Seite 2, Zeile 31 * * Seite 18, Zeile 17 - Seite 19, Zeile 1 * -----	1-21	INV. G07B17/00
A	WO 2004/029754 A (NEOPOST S A [FR]; LEON J P [US]) 8. April 2004 (2004-04-08) * Zusammenfassung * * Absatz [0036] - Absatz [0048] * * Absatz [0097] * -----	1-21	
A	WO 02/093316 A (INTELLIMARK TECHNOLOGIES INC [US]; HENDERSON VERLIN RAY [US]; JANOVICH) 21. November 2002 (2002-11-21) * Zusammenfassung * * Seite 2, Zeile 13 - Seite 4, Zeile 19 * -----	1-21	
A	WO 02/37736 A (PITNEY BOWES INC [US]) 10. Mai 2002 (2002-05-10) * Zusammenfassung * * Abbildungen 2b,3b,4b * * Seite 8, Zeile 4 - Seite 9, Zeile 26 * -----	1-21	

RECHERCHIERTE SACHGEBIETE (IPC)

G07B
G07F
G06F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	13. März 2009	Stenger, Michael

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

1

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 08 01 7285

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

13-03-2009

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
GB 2211144 A	28-06-1989	AU 2513288 A	29-06-1989
		CA 1295738 C	11-02-1992
		CH 678986 A5	29-11-1991
		DE 3841394 A1	29-06-1989
		FR 2625003 A1	23-06-1989
		IT 1224800 B	24-10-1990
		JP 1191994 A	02-08-1989
		SE 512619 C2	10-04-2000
		SE 8804235 A	23-11-1988
		US 4873645 A	10-10-1989
WO 2004029754 A	08-04-2004	AU 2003275216 A1	19-04-2004
		CA 2499923 A1	08-04-2004
		EP 1547022 A2	29-06-2005
		US 2004083189 A1	29-04-2004
WO 02093316 A	21-11-2002	EP 1402446 A2	31-03-2004
		JP 2004526389 T	26-08-2004
		US 2002188845 A1	12-12-2002
WO 0237736 A	10-05-2002	AU 1801102 A	15-05-2002
		CA 2441407 A1	10-05-2002
		EP 1410548 A2	21-04-2004
		US 6868407 B1	15-03-2005

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- DE 3840041 A1 **[0003]**
- US 7110576 B2 **[0007]**
- US 6801833 B2 **[0008]**
- US 5612889 A **[0009] [0010]**
- EP 710930 B1 **[0010]**
- EP 1058212 A1 **[0011]**

In der Beschreibung aufgeführte Nicht-Patentliteratur

- Electronic Postage Systems. **GERRIT BLEUMER.** Basic Cryptographic Mechanisms. Springer-Verlag, 2007, 91 **[0005]**
- **HENK C. A. VAN TILBORG.** Encyclopedia of Cryptography and Security. Springer-Verlag, 2005, 361-367 **[0029]**
- **HENK C. A. VAN TILBORG.** Encyclopedia of Cryptography and Security. Springer-Verlag, 2005, 256-264 **[0034]**
- **HENK C. A. VAN TILBORG.** Encyclopedia of Cryptography and Security. Springer-Verlag, 2005, 541 **[0059]**