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

(11) **EP 1 279 147 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
17.07.2013 Patentblatt 2013/29

(21) Anmeldenummer: **01935987.6**

(22) Anmeldetag: **24.04.2001**

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

(86) Internationale Anmeldenummer:
PCT/DE2001/001555

(87) Internationale Veröffentlichungsnummer:
WO 2001/082233 (01.11.2001 Gazette 2001/44)

(54) VERFAHREN ZUM VERSEHEN VON POSTSENDUNGEN MIT FREIMACHUNGSVERMERKEN

METHOD FOR PROVIDING POSTAL ITEMS WITH POSTAL PREPAYMENT IMPRESSIONS

PROCEDE SERVANT A POURVOIR DES ENVOIS POSTAUX DE MENTIONS D'AFFRANCHISSEMENT

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

(30) Priorität: **27.04.2000 DE 10020566**

(43) Veröffentlichungstag der Anmeldung:
29.01.2003 Patentblatt 2003/05

(73) Patentinhaber: **Deutsche Post AG**
53113 Bonn (DE)

(72) Erfinder:
- **MEYER, Bernd**
  53639 Königswinter (DE)
- **LANG, Jürgen**
  51429 Bergisch Gladbach (DE)

(74) Vertreter: **Jostarndt, Hans-Dieter**
Jostarndt Patentanwalts-AG
Brüsseler Ring 51
52074 Aachen (DE)

(56) Entgegenhaltungen:
EP-A- 0 376 573
EP-A- 0 550 226
EP-A- 0 854 446
WO-A-98/14907
WO-A-99/48053
DE-A- 3 126 785
US-A- 5 666 421

- **"Information Based Indicia Program Postal Security Device Specification" INFORMATION BASED INDICIA PROGRAM. POSTAL SECURITY DEVICE SPECIFICATION, 13. Juni 1996 (1996-06-13), Seiten 1-41, XP002137734**
- **SMID M E ET AL: "THE DATA ENCRYPTION STANDARD: PAST AND FUTURE" PROCEEDINGS OF THE IEEE, IEEE. NEW YORK, US, Bd. 76, Nr. 5, 1. Mai 1988 (1988-05-01), Seiten 550-559, XP000562387 ISSN: 0018-9219**

EP 1 279 147 B1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken, wobei ein Kundensystem von einem Wertübertragungszentrum über eine Datenleitung einen Gebührenbetrag lädt, wobei das Kundensystem ein Drucken von Freimachungsvermerken auf Postsendungen steuert und wobei das Wertübertragungszentrum ein Datenpaket an das Kundensystem sendet.

[0002] Ein gattungsgemäßes Verfahren ist aus der internationalen Patentanmeldung WO 98 14907 bekannt.

[0003] Ein weiteres Verfahren ist aus der Deutschen Patentschrift DE 31 26 785 C2 bekannt. Bei diesem verfahren erfolgt eine Erzeugung eines für eine Frankierung von Postsendungen bestimmten Nachladesignals in einem separaten Bereich eines von einem Postbeförderungsunternehmen betriebenen Wertübertragungszentrums.

[0004] Aus der internationalen Patentanmeldung WO 99/48053 geht ein Verfahren zum Verwalten von Lizenznummern hervor, die von einem "Postal Security Device (PSD)", das mit einem Computer verbunden ist, zur Erzeugung von kryptographisch abgesicherten elektronischen Frankiervermerken genutzt werden. Die Lizenznummern sind dabei jeweils mit einem Registersatz des PSD verknüpft. Sie werden von einem Postunternehmen ausgegeben und über den PSD-Hersteller an das PSD übertragen, wobei die Kommunikation zwischen dem PSD und dem Herstellersystem sowie zwischen dem Herstellersystem und dem Postunternehmen mittels digitaler Signaturen abgesichert wird. In die digitalen Frankiervermerke werden die Lizenznummer sowie weitere Informationen eingebracht und durch eine digitale Signatur abgesichert.

[0005] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Freimachen von Briefen zu schaffen, das sich sowohl zum Freimachen einzelner Briefe als auch zum Freimachen einer Vielzahl von Briefen eignet.

[0006] Erfindungsgemäß wird diese Aufgabe durch ein Verfahren nach dem Patentanspruch 1 gelöst.

[0007] Es ist insbesondere vorgesehen, dass in dem Kundensystem Daten erzeugt werden, die so verschlüsselt sind, dass das Wertübertragungszentrum diese entschlüsseln kann, dass die Daten von dem Kundensystem zu dem Wertübertragungszentrum gesendet werden und dass das Wertübertragungszentrum die Daten entschlüsselt und anschließend die Daten erneut mit einem dem Kundensystem nicht bekannten Schlüssel codiert und die so verschlüsselten Daten anschließend an das Kundensystem überträgt.

[0008] Das Kundensystem ist vorzugsweise so gestaltet, dass es nicht in der Lage ist, von dem Wertübertragungszentrum gesandte Daten vollständig zu entschlüsseln, jedoch ein Briefzentrum, in dem die Postsendungen auf eine korrekte Frankierung überprüft werden, diese Daten entschlüsseln kann.

[0009] Das Wertübertragungszentrum kann auf verschiedene Weisen gestaltet sein. Der Begriff Wertübertragungszentrum umfasst sowohl bekannte Wertübertragungszentren als auch neue Formen von Wertübertragungszentren.

[0010] Die Erfindung betrifft insbesondere solche Wertübertragungszentren, über die auf eine Datenkommunikationsleitung unmittelbar zugegriffen werden kann, wie an das Internet oder an Telefonleitungen angeschlossene Datenserver.

[0011] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die Verschlüsselung in dem Kundensystem unter Einsatz einer Zufallszahl erfolgt.

[0012] Es ist zweckmäßig, dass die Zufallszahl in einem Sicherungsmodul erzeugt wird, auf das ein Benutzer des Kundensystems keinen Zugriff hat.

[0013] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die Zufallszahl Zusammen mit einem von dem Wertübertragungszentrum ausgegebenen Sitzungsschlüssel und einem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt wird.

[0014] Es ist zweckmäßig, dass das Kundensystem die Daten mit einem privaten Schlüssel signiert.

[0015] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der private Schlüssel in dem Sicherungsmodul gespeichert ist.

[0016] Es ist zweckmäßig, dass die Daten mit jeder Anforderung eines Gebührenbetrages von dem Kundensystem an das Wertübertragungszentrum übertragen werden.

[0017] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass das Wertübertragungszentrum anhand der übermittelten Daten das Kundensystem identifiziert.

[0018] Es ist zweckmäßig, dass das Wertübertragungszentrum die von ihm verschlüsselten Daten an das Kundensystem schickt.

[0019] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die von dem Wertübertragungszentrum an das Kundensystem gesandten Daten einen ersten Bestandteil aufweisen, der von dem Kundensystem nicht entschlüsselt werden kann und dass die Daten ferner einen zweiten Anteil aufweisen, der von dem Kundensystem entschlüsselt werden kann.

[0020] Es ist zweckmäßig, dass der in dem Kundensystem entschlüsselbare Teil der Daten Informationen über die Identität des Kundensystems enthält.

[0021] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der von dem Kundensystem entschlüsselbare Anteil der Daten Informationen über die Höhe eines

Gebührenbetrages enthält.

[0022] Es ist zweckmäßig, dass ein Senden von Daten von dem Kundensystem an das Wertübertragungszentrum lediglich dann erfolgt, wenn in dem Kundensystem ein Betrag in einer Mindesthöhe geladen werden soll.

[0023] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass in dem Kundensystem ein Hash-Wert gebildet wird.

[0024] Es ist zweckmäßig, dass der Hash-Wert unter Einbeziehung von Angaben über Sendungsdaten gebildet wird.

[0025] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der Hash-Wert unter Einbeziehung einer zwischengespeicherten Zufallszahl gebildet wird.

[0026] Es ist zweckmäßig, dass der Hash-Wert unter Einbeziehung einer Ladevorgangsidentifikationsnummer gebildet wird.

[0027] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der Freimachungsvermerk logische Daten enthält.

[0028] Es ist zweckmäßig, dass der Freimachungsvermerk Informationen über Sendungsdaten enthält.

[0029] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die logischen Daten Informationen über die verschlüsselte Zufallszahl enthalten.

[0030] Es ist zweckmäßig, dass die logischen Daten Informationen über die verschlüsselte Ladevorgangsidentifikationsnummer enthalten.

[0031] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die logischen Daten Informationen über den Hash-Wert enthalten.

[0032] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der Freimachungsvermerk sowohl von dem Wertübertragungszentrum übertragene Informationen als auch von dem Dokumenthersteller eingegebene Daten enthält.

[0033] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszugestalten, dass der Freimachungsvermerk einen Hash-Wert enthält, der aus einer Kombination aus einem von dem Vorgabezentrum übertragenen Wert und von dem Dokumenthersteller eingegebenen Werten gebildet wird.

[0034] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass sie folgende Verfahrensschritte beinhalten: In dem Kundensystem oder in einem mit dem Kundensystem verbundenen Sicherungsmodul wird ein Geheimnis erzeugt und anschliessend zusammen mit Informationen über die Identität des Dokumentherstellers und/oder des von ihm eingesetzten Kundensystems an das Wertübertragungszentrum übermittelt.

[0035] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszugestalten, dass das Wertübertragungszentrum die verschlüsselte Zusatzzahl entschlüsselt und wieder derart verschlüsselt, dass nur das Briefzentrum diese entschlüsseln kann und anschliessend eine Ladeidentifikationsnummer erzeugt.

[0036] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass bei der Erzeugung der Ladeidentifikationsnummer die verschlüsselte Zufallszahl eingeht.

[0037] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszugestalten, dass die Ladeidentifikationsnummer an das Sicherungsmodul übertragen wird.

[0038] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass in dem Sicherungsmodul ein Hash-Wert aus der Ladeidentifikationsnummer und weiteren Daten gebildet wird.

[0039] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszugestalten, dass der Freimachungsvermerk so erzeugt wird, dass er den Hash-Wert enthält.

[0040] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die Gültigkeit von Freimachungsvermerken in dem Briefzentrum überprüft wird.

[0041] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszugestalten, dass die Prüfung in dem Briefzentrum durch eine Analyse von in dem Freimachungsvermerk enthaltenen Daten erfolgt.

[0042] Eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die Prüfungsstelle aus in dem Freimachungsvermerk enthaltenen Daten einen Hash-Wert bildet und überprüft, ob dieser Hash-Wert mit einem in dem Freimachungsvermerk enthaltenen Hash-Wert übereinstimmt und im Falle der Nichtübereinstimmung den Freimachungsvermerk als gefälscht registriert.

[0043] Weitere Vorteile, Besonderheiten und zweckmäßige Weiterbildungen der Erfindung ergeben sich aus der nachfolgenden Darstellung eines bevorzugten Ausführungsbeispiels anhand der Zeichnungen.

[0044] Von den Zeichnungen zeigt

Fig. 1 eine Prinzipdarstellung eineserfindungsgemäßen Verfahrens,

Fig. 2 die in Fig. 1 dargestellte Prinzipdarstellung mit einer Hervorhebung der bei einem Frankierungsvorgang beteiligten Parteien,

Fig. 3 Schnittstellen des in Fig. 1 und Fig. 2 dargestellten Frankierungssystems und

Fig. 4 eine Prinzipdarstellung von in dem Verfahren eingesetzten Sicherheitsmechanismen.

[0045] Das nachfolgende Ausführungsbeispiel beschreibt die Erfindung anhand eines vorgesehenen Einsatzes im Bereich der Deutschen Post AG. Es ist jedoch selbstverständlich gleichermaßen möglich, die Erfindung für eine Freimachung von anderen Dokumenten, insbesondere für einen Einsatz im Bereich von anderen Versandunternehmen, einzusetzen.

[0046] Die Erfindung stellt eine mögliche neue Form der Frankierung bereit, mit der Kunden unter Benutzung eines herkömmlichen PC mit Drucker und zusätzlicher Soft- und gegebenenfalls Hardware sowie eines Internet-Zugangs "digitale Freimachungsvermerke" auf Briefe, Postkarten etc. drucken können.

[0047] Eine Bezahlung zum Ausgleich des Wertes der von den Kunden ausgedruckten Frankierwerte kann auf verschiedene Weisen geschehen. Beispielsweise wird ein gespeichertes Guthaben verringert. Dieses Guthaben ist vorzugsweise digital gespeichert. Eine digitale Speicherung erfolgt beispielsweise auf einer speziellen Kundenkarte, einer standardisierten Geldkarte oder einem virtuellen Speicher, der sich beispielsweise in einem Computer des Benutzers befindet. Vorzugsweise wird der Guthabenbetrag geladen, bevor Ausdrucke von Frankierwerten erfolgen. Die Ladung des Guthabenbetrages erfolgt in einer besonders bevorzugten Ausführungsform in einem Lastschriftverfahren.

[0048] In Fig. 1 ist ein prinzipieller Ablauf einer erfindungsgemäßen Freimachung von Postsendungen gekennzeichnet. Das Verfahren beinhaltet mehrere Schritte, die vorzugsweise zu einem vollständigen Kreislauf ergänzt werden können. Dies ist zwar besonders zweckmäßig, jedoch nicht notwendig. Die nachfolgend dargestellte Zahl von acht Schritten ist gleichermaßen vorteilhaft, jedoch ebenfalls nicht notwendig.

1. Mit dem PC laden Kunden des Versandunternehmens (gegebenenfalls unter Verwendung zusätzlicher Soft/ Hardware, zum Beispiel Microprozessor-Chipkarte) über das Internet einen Wertbetrag.

2. Über den Wertbetrag erfolgt ein Inkasso, zum Beispiel durch Abbuchung vom Konto des Kunden.

3. Aus dem Wertbetrag, der beim Kunden in einer elektronischen Börse gespeichert ist, können so lange gültige Frankierwerte in beliebiger Höhe über den eigenen Drucker ausgedruckt werden, bis das Guthaben aufgebraucht ist.

4. Der vom Kunden aufgedruckte Freimachungsvermerk enthält lesbare Angaben sowie einen maschinenlesbaren Barcode, der von der Deutschen Post zur Prüfung der Gültigkeit herangezogen wird.

5. Die freigemachte Postsendung kann über die von der Deutschen Post bereitgestellten Möglichkeiten, zum Beispiel Briefkasten und Postfilialen, eingeliefert werden.

6. Der im Freimachungsvermerk angegebene Barcode, vorzugsweise 2D-Barcode, wird im Briefzentrum über eine Anschriftenlesemaschine gelesen. Während der Produktion erfolgt eine Gültigkeitsprüfung auf logischer Plausibilitätsbasis.

7. Die im Freimachungsvermerk gelesenen Daten werden unter anderem zur Entgeltsicherung an ein Hintergrundsystem übertragen.

8. Zwischen den geladenen Abrechnungsbeträgen und den produzierten Sendungen wird zur Erkennung von Missbrauch ein Abgleich vorgenommen.

[0049] Vorzugsweise sind an dem Frankierungsverfahren mehrere Parteien beteiligt, wobei eine besonders zweckmäßige Aufteilung der Parteien in Fig. 2 dargestellt ist.

[0050] Die dargestellten Parteien sind ein Kunde, ein Kundensystem und ein Versandunternehmen.

[0051] Das Kundensystem umfasst die Hard- und Software, die vom Kunden zur PC-Frankierung eingesetzt wird. Das Kundensystem regelt in Interaktion mit dem Kunden das Laden und Speichern der Abrechnungsbeträge und den Ausdruck des Freimachungsvermerks. Einzelheiten zum Kundensystem regeln die Zulassungsvoraussetzungen.

[0052] Das Versandunternehmen übernimmt die Produktion der Sendungen und führt die erforderliche Entgeltsiche-

rung durch. Ein Wertübertragungszentrum kann auf verschiedene Weise gestaltet sein.

- Der Betrieb eines eigenen Wertübertragungszentrums macht in Verbindung mit der Sicherheitsarchitektur der PC-Frankierung den Einsatz symmetrischer Verschlüsselungsverfahren im Freimachungsvermerk möglich. Hierdurch wird die erforderliche Prüfzeit der Gültigkeit eines Freimachungsvermerks erheblich reduziert. Erforderlich für den Einsatz eines symmetrischen Verfahrens ist der Betrieb des Wertübertragungszentrums und der Briefzentren durch dieselbe Organisation. Eine derart beschleunigte Produktion wäre bei Verwendung asymmetrischer Sicherheitselemente im Freimachungsvermerk nicht möglich.

- Realisierung aller erforderlichen Sicherheitsanforderungen, unter anderem zur Vermeidung von internen und externen Manipulationen:

  Anders als bei der Absenderfreistempelung erfolgt die Kommunikation über das offene und potentiell unsichere Internet. Angriffe auf die Kommunikationswege und die Internet-Server sowie interne Möglichkeiten der Manipulation erfordern höhere Sicherheitsvorkehrungen. Diese liegen in erster Linie im Interesse der Deutschen Post und deren Kunden.

[0053] Durch ein zentrales, durch das Versandunternehmen vorgegebenes, Management kryptographischer Schlüssel, ist eine Verbesserung der Sicherheit möglich. Die bei der Produktion im Briefzentrum relevanten Schlüssel können jederzeit durch die Deutsche Post ausgewechselt und Schlüssellängen verändert werden.

- Prüfungen zur Entgeltsicherung sind nach einem einheitlichen Prüfverfahren möglich und jederzeit durchführbar.

- Neue Vertragsteilnehmer und Änderungen in Verträgen können schnell allen erforderlichen Systemen des Versandunternehmens mitgeteilt werden.

[0054] Eine Entgeltsicherung erfolgt vorzugsweise unter Erfassung von Bestandteilen der Freimachungsvermerke.

[0055] Dazu werden Vereinbarungsdaten (Kunden-/Kundensystemdaten) aus einer zentralen Datenbank an das System übergeben, das für die Überprüfung der ordnungsgemäßen Entgeltsicherung erforderlich ist.

[0056] Den Umfang der zu speichernden Daten legt das Versandunternehmen, insbesondere der Betreiber des Postdienstes unter Beachtung von gesetzlichen Bestimmungen wie der Postdienstunternehmensdatenschutzverordnung (PDSV) fest. Grundsätzlich können danach alle Daten, die für das ordnungsgemäße Ermitteln, Abrechnen und Auswerten sowie zum Nachweis der Richtigkeit der Nachentgelte erforderlich sind, gespeichert werden. Grundsätzlich sind dies alle Sendungsinformationen ohne Empfängername und gegebenenfalls Hausnummer/Postfachnummer des Empfängers.

[0057] Ein Hintergrundsystem überprüft, ob in dem Kundensystem enthaltene Guthabenbeträge tatsächlich in Höhe von Gebührenbeträgen verringert werden, die als Freimachungsvermerke ausgedruckt werden.

[0058] Für eine Erfassung von Vereinbarungsdaten ist vorzugsweise ein Erfassungssystem vorgesehen.

[0059] Vereinbarungsdaten zur PC-Frankierung mit den jeweiligen Stammdaten der Kunden und des Kundensystems (z.B. Sicherungsmodul-ID) werden über eine beispielsweise auch zu anderen Freimachungsarten einsetzbare Datenbank bereitgestellt und gepflegt. Bei Einsatz einer bestehenden Freimachungsdatenbank wird beispielsweise ein separater Teilbereich zur PC-Frankierung in der Datenbank implementiert. Die Daten werden dem Wertübertragungszentrum und Entgeltsicherungssystem im Briefzentrum bereitgestellt. Es ist besonders zweckmäßig, dass das System Schnittstellen enthält, die einen Daten- und Informationsaustausch mit weiteren Systemen ermöglichen.

[0060] In Fig. 3 sind drei Schnittstellen dargestellt.

[0061] Die Schnittstellen sind mit "Freimachungsvermerk" und "Inkasso" bezeichnet. Über die Abrechnungsschnittstelle werden Abrechnungsdaten zwischen dem Kundensystem und dem Versanddienstleiter ausgetauscht. Beispielsweise kann über die Abrechnungsschnittstelle ein Geldbetrag geladen werden.

[0062] Die Freimachungsschnittstelle legt fest, wie Freimachungsvermerke gestaltet werden, damit sie in Brief-, beziehungsweise Frachtzentren gelesen und geprüft werden können.

[0063] Bei der in Fig. 3 dargestellten Implementation der Schnittstellen sind die Abrechnungsschnittstellen und die Inkassoschnittstelle voneinander getrennt. Es ist jedoch gleichfalls möglich, dass die Abrechnungsschnittstelle und die Inkassoschnittstelle zusammengefasst sind, beispielsweise bei einer Abrechnung über Geldkarten, Kreditkarten oder digitales Geld, insbesondere digitale Münzen. Die Inkassoschnittstelle legt fest, wie eine Abrechnung der über die Abrechnungsschnittstelle übermittelten Gebührenbeträge erfolgt. Die anderen Parameter des Frankierungsverfahrens hängen nicht von der gewählten Inkassoschnittstelle ab, jedoch wird durch eine effiziente Inkassoschnittstelle die Effizienz des Gesamtsystems erhöht. Bevorzugte Inkassomöglichkeiten sind Lastschriften und Rechnungen.

[0064] Nachfolgend wird dargestellt, wie durch anwendungsspezifische inhaltliche Sicherheitsanforderungen Sicher-

heitsziele des Frankierungsverfahrens erreicht werden.

[0065] Der Fokus dieses Konzeptes ist hierbei auf die technische Spezifikation der Sicherheitsanforderungen an das System gerichtet. Nicht sicherheitsrelevante Prozesse wie An-, Ab- und Ummelden von Kunden, die nicht über das Kundensystem erfolgen müssen, können separat festgelegt werden. Technische Prozesse zwischen dem Kundensystem und dem Kundensystemhersteller werden vorzugsweise so festgelegt, dass sie dem hier dargestellten Sicherheitsstandard entsprechen.

[0066] Durch das erfindungsgemäße Verfahren werden die nachfolgend genannten Sicherheitsziele erreicht.

- Phantasie- und Schmiermarken, also Freimachungsvermerke, die keine plausiblen Angaben zur Sendung enthalten oder aus anderen Gründen unleserlich sind, werden als ungültig erkannt.
- Dubletten, also exakte Kopien von gültigen Freimachungsvermerken mit plausiblen Angaben zur Sendung, können im Nachhinein erkannt werden.
- Eine Erhöhung des dem Kundensystem zur Verfügung stehenden Guthabenbetrages wird verhindert. Veränderungen des Guthabenbetrages sind auch im Nachhinein erkennbar und können vorzugsweise anhand einer Protokollliste auch im Nachhinein nachgewiesen werden.
- Unberechtigte Nutzungen werden erkannt und werden dem rechtmäßigen Nutzer im Falle einer unberechtigten Nutzung durch Dritte nicht angelastet.
- Hierzu zählt die missbräuchliche Verwertung rechtmäßig übertragener elektronischer Daten oder gültiger, rechtmäßig erzeugter Freimachungsvermerke ohne Wissen des rechtmäßigen Nutzers.
- Hierzu zählt die missbräuchliche Nutzung des Kundensystems durch Programmveränderungen.
- Hierzu zählt die unberechtigte Nutzung des Kundensystems durch fremde Softwareagenten über das Internet.
- Hierzu zählt das Ausforschen von PINs durch Angriffssoftware (trojanische Pferde).
- Hierzu zählen die Überlastungs-Angriffe (Denial-of-Service-Attacks, DoS), zum Beispiel durch Vortäuschen der Identität des Wertübertragungszentrums oder Manipulation des Ladevorgangs in der Art, dass Geld abgebucht, aber kein Guthaben angelegt wurde.
- Unberechtigtes Laden von Abrechnungsbeträgen wird durch technische Vorkehrungen im Wertübertragungszentrum unmöglich gemacht. Unberechtigtes Laden von Abrechnungsbeträgen könnte z.B. erfolgen durch:
- Vortäuschen der Identität des Post-Wertübertragungszentrums zur Erhöhung der eigenen Börse im Kundensystem durch den Kunden.
- Vortäuschen eines zertifizierten Kundensystems durch ein manipuliertes oder erfundenes Kundensystem derart, dass der Täter Kenntnis von sicherheitskritischen Geheimnissen des Sicherungsmoduls erlangt und daraufhin unbemerkt Fälschungen erstellen kann.
- Mitschneiden der ordnungsgemäßen Kommunikation zwischen einem Kundensystem und dem Wertübertragungszentrum und Wiederholung dieser Kommunikation in missbräuchlicher Absicht (Replay-Attacke).
- Manipulation der zwischen Kundensystem und Wertübertragungszentrum stattfindenden Kommunikation in Echtzeit (ein- und ausgehende Datenströme im Kundensystem) in der Weise, dass das Kundensystem von einem höheren geladenen Wertbetrag als das Wertübertragungszentrum ausgeht.
- Missbrauch von Kundenidentifikationsnummern in der Weise, dass Dritte auf Kosten eines Kunden Wertbeträge laden.
- Unvollständige Stornoabwicklung.

[0067] Die ersten beiden dieser Sicherheitsprobleme werden im Wesentlichen durch das Systemkonzept und die durch Maßnahmen im Gesamtsystem gelöst, die drei letzten werden vorzugsweise durch die Implementation von Soft-

und Hardware des Sicherungsmoduls gelöst.

[0068] Bevorzugte Ausgestaltungen einer die Sicherheitsstandards erhöhenden Hardware sind nachfolgend dargestellt:

- Grundlegende Eigenschaften der Hardware

  1. Alle Verschlüsselungen, Entschlüsselungen, Umschlüsselungen, Signaturberechnungen und kryptographischen Prüfungsprozeduren werden in gegen unberechtigte Zugriffe besonders geschützten Bereichen eines kryptographischen Sicherungsmoduls im Kundensystem durchgeführt. Die zugehörigen Schlüssel sind ebenfalls in solchen Sicherheitsbereichen abgelegt.

  2. Sicherheitsrelevante Daten und Abläufe (zum Beispiel Schlüssel, Programme) werden gegen unberechtigte Veränderungen und geheime Daten (zum Beispiel Schlüssel, PINs) gegen unberechtigtes Auslesen geschützt. Dies wird vorzugsweise durch folgende Maßnahmen gewährleistet:

- Bauart des Sicherungsmoduls, eventuell im Zusammenwirken mit Sicherheitsmechanismen der Software des Sicherungsmoduls,
- Laden von Programmen in Sicherungsmodule nur bei der Herstellung oder kryptographischer Absicherung des Ladevorgangs,
- kryptographische Absicherung des Ladens von sicherheitsrelevanten Daten, insbesondere von kryptographischen Schlüsseln.
- Auch vor dem Auslesen mittels Angriffen, die die Zerstörung des Moduls in Kauf nehmen, müssen geheime Daten in Sicherungsmodulen geschützt sein.

  a. Der Schutz von Daten und Programmen gegen Veränderung, beziehungsweise Auslesen in dem Sicherungsmodul muss so hoch sein, dass während der Lebensdauer des Moduls Angriffe mit vertretbarem Aufwand nicht möglich sind, wobei der für einen erfolgreichen Angriff nötige Aufwand gegen den hieraus zu ziehenden Nutzen abzuwägen ist.
  b. Unerwünschte Funktionen dürfen durch ein Sicherungsmodul nicht ausführbar sein.

- Unerwünschte Nebenfunktionen und zusätzliche Datenkanäle, insbesondere Schnittstellen, die ungewollt Informationen weitergeben (Side Channels), werden verhindert.

[0069] Durch die Konstruktion des Sicherungsmoduls wird sichergestellt, dass ein Angreifer Informationen über geheimzuhaltende Daten und Schlüssel nicht über Schnittstellen auslesen kann, die für andere Zwecke gedacht sind.

[0070] Das Vorliegen solcher Kanäle von Side Channels wird durch entsprechende Tests überprüft. Typische Möglichkeiten, die überprüft werden, sind:

1. Single Power Attack (SPA) und Differential Power Attack (DPA), die versuchen, aus Änderungen des Stromverbrauchs während kryptographischer Berechnungen auf geheime Daten zu schließen.
2. Timing Attacks, die versuchen, aus der Dauer kryptographischer Berechnungen auf geheime Daten zu schließen.

[0071] Bevorzugte Eigenschaften der Datenverarbeitung sind nachfolgend dargestellt:

- Ablaufkontrolle:

  Es ist besonders zweckmäßig, dass eine Ablaufkontrolle durchgeführt wird. Diese kann beispielsweise durch eine Zustandsmaschine, beispielsweise entsprechend dem Standard FIPS PUB 140-1, erfolgen. Dadurch wird sichergestellt, dass die Abläufe der spezifizierten Transaktionen und die hierbei verwendeten sicherheitsrelevanten Daten des Systems nicht manipuliert werden können.

[0072] Die beteiligten Instanzen, insbesondere der Benutzer, dürfen durch ein Sicherungsmodul über die Abläufe der Transaktionen nicht getäuscht werden.

[0073] Wenn beispielsweise der Vorgang des Ladens eines Wertbetrages in der Form mehrerer Teilvorgänge mit einzelnen Aufrufen des Sicherungsmoduls realisiert ist, muss die Ablaufkontrolle sicherstellen, dass diese Teilvorgänge nur in der zulässigen Reihenfolge ausgeführt werden.

[0074] Die Zustandsdaten, die für die Ablaufkontrolle verwendet werden, sind sicherheitsrelevant und werden daher vorzugsweise in einem gegen Manipulation gesicherten Bereich des Sicherungsmoduls gespeichert.

- Nachrichtenintegrität:

  1. Alle sicherheitsrelevanten Informationen in den Nachrichten werden vor und nach der Übertragung in den Komponenten des Systems mit geeigneten Verfahren gegen unberechtigte Veränderung geschützt.
  2. Veränderungen an sicherheitsrelevanten Informationen während der Übertragung zwischen Komponenten des chipkartengestützten Zahlungssystems werden erkannt. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen.
  3. Das unautorisierte Einspielen von Nachrichten wird erkannt. Entsprechende Reaktionen müssen auch auf wiedereingespielte Nachrichten erfolgen.

[0075] Dass unbefugte Veränderungen und das Wiedereinspielen von Nachrichten erkannt werden können, wird für die Standardnachrichten des Systems durch die Festlegungen des Systemkonzepts sichergestellt. Die Software des Sicherungsmoduls hat sicherzustellen, dass die Erkennung tatsächlich erfolgt und entsprechend reagiert wird. Für sicherheitsrelevante herstellerspezifische Nachrichten (etwa im Rahmen der Personalisierung der Wartung des Sicherungsmoduls) werden entsprechende geeignete Mechanismen festgelegt und angewendet.

[0076] Die für die Sicherung der Nachrichtenintegrität relevanten Informationen werden vorzugsweise in einem gegen Manipulation gesicherten Bereich des Sicherungsmoduls gespeichert. Solche Informationen sind insbesondere Identifikations- und Authentizitätsmerkmale, Sequenzzähler oder Gebührenbeträge.

- Geheimhaltung von PINs und kryptographischen Schlüsseln

  1. Obwohl die PIN außerhalb von gesicherten Bereichen nicht im Klartext übertragen werden sollte, wird vorzugsweise die Klartext-Übertragung bei der PC-Frankierung aus Gründen der Benutzerfreundlichkeit des Gesamtsystems und der Verwendung bestehender, ungesicherter Hardwarekomponenten im Kundensystem (Tastatur, Monitor) toleriert. Jedoch sind die lokalen Systemkomponenten, in denen die PINs im Klartext bearbeitet oder gespeichert werden, auf ein Minimum zu reduzieren. Eine ungesicherte Übertragung der PINs darf nicht erfolgen.
  2. Kryptographische Schlüssel dürfen auf elektronischen Übertragungswegen in ungesicherter Umgebung nie im Klartext übertragen werden. Werden sie in Systemkomponenten benutzt oder gespeichert, so müssen sie gegen unautorisiertes Auslesen und Verändern geschützt sein.
  3. Keine Systemkomponente darf eine Möglichkeit zur Bestimmung einer PIN aufgrund einer erschöpfenden Suche bieten.

- Protokollierung

  1. Innerhalb des Kundensystems werden alle Daten protokolliert, die für die Rekonstruktion der betreffenden Abläufe benötigt werden. Ferner werden auch Fehlerfälle protokolliert, die einen Manipulationsverdacht nahelegen.
  2. Gespeicherte Protokolldaten müssen gegen unberechtigte Veränderungen geschützt sein und authentisch an eine auswertende Instanz übertragen werden können.

- Verarbeitung anderer Anwendungen
  Werden in Sicherungsmodulen gleichzeitig andere Anwendungen verarbeitet, so darf dadurch die Sicherheit des PC-Frankierungssystems nicht beeinflusst werden.

[0077] Durch folgende Maßnahmen kann die Datensicherheit weiter erhöht werden:

- Löschen geheimer Daten aus temporären Speichern
- Sichere Implementation von herstellerspezifischen Funktionen (z.B. im Rahmen der Personalisierung); etwa Verwendung von Triple-DES oder einem sicheren symmetrischen Verfahren für Verschlüsselung von geheimen Personalisierungsdaten, Einbringung von Klartextschlüsseln in Form von geteilten Geheimnissen (z.B. Schlüsselhälften) nach dem Vier-Augen-Prinzip
- Es dürfen keine unsicheren Zusatzfunktionen existieren (etwa Verschlüsseln oder Entschlüsseln oder Signieren von frei wählbaren Daten mit Schlüsseln des Systems); es darf keine Funktionsvertauschung von Schlüsseln möglich sein.

Weitere Aspekte

[0078]

- Ausser den in den Kundensystemen eingesetzten Sicherungsmodulen sind auch weitere Sicherungsmodule zu untersuchen: Insbesondere sind die Sicherungsmodule der verschiedenen Zertifizierungsstellen (CAs) bei den Herstellern von Sicherungsmodulen zu untersuchen.
- Auch der PC-seitige Anteil der Kundensoftware ist hinsichtlich seiner sicherheitsrelevanten Aufgaben (z.B. PIN-Eingabe) zu untersuchen.
- Es ist vom Hersteller eines Kundensystems ein Verfahren vorzusehen, das die gesicherte Übermittlung der PIN von Sicherungsmodulen an die Benutzer garantiert (Beispielsweise PIN-Brief-Versendung). Ein solches Konzept ist auf Sicherheit und Einhaltung zu überprüfen.
- Sicherheit der Herstellerumgebung, insbesondere Schlüsseleinbringung etc.; Sicherheitsbeauftragte, allgemeiner: Zulassung der organisatorischen Sicherheitsmaßnahmen von Herstellern nach festgelegtem Verfahren. Im Einzelnen:

  Schlüsselmanagement

  1. Zur Verteilung, Verwaltung und eventuell zum turnusmäßigen Wechsel und zum Ersetzen von Schlüsseln sind Regelungen zu treffen.
  2. Schlüssel, für die der Verdacht auf Kompromittierung besteht, dürfen im gesamten System nicht mehr verwendet werden.

[0079] Bevorzugte Maßnahmen bei der Herstellung und Personalisierung von Sicherungsmodulen sind:

1. Die Herstellung und Personalisierung (Ersteinbringung geheimer Schlüssel, eventuell benutzerspezifischer Daten) von Sicherungsmodulen muss in einer Produktionsumgebung stattfinden, die verhindert, dass

   - Schlüssel bei der Personalisierung kompromittiert werden,
   - der Personalisierungsvorgang missbräuchlich oder unberechtigt durchgeführt wird,
   - unautorisierte Software oder Daten eingebracht werden können,
   - Sicherungsmodule entwendet werden.

2. Es muss sichergestellt sein, dass in das System keine unautorisierten Komponenten eingebracht werden können, die sicherheitsrelevante Funktionen ausführen.
3. Der Lebensweg aller Sicherungsmodule muss kontinuierlich aufgezeichnet werden.

Erläuterung:

[0080] Die Aufzeichnung des Lebenswegs eines Sicherungsmoduls umfasst:

- Herstellungs- und Personalisierungsdaten,
- räumlichen/zeitlichen Verbleib,
- Reparatur und Wartung,
- Ausserbetriebnahme,
- Verlust bzw. Diebstahl von das Sicherungsmodul enthaltenden Datenspeichern wie Dateien, Dongles, Krypto, Server oder Chipkarten
- Herstellungs- und Personalisierungsdaten,
- Einbringen neuer Anwendungen,
- Änderung von Anwendungen,
- Änderung von Schlüsseln,
- Ausserbetriebnahme,
- Verlust bzw. Diebstahl.

Sicherheitsarchitektur

[0081] Für die PC-Frankierung wird eine grundsätzliche Sicherheitsarchitektur vorgesehen, die die Vorteile verschiedener, bestehender Ansätze verbindet und mit einfachen Mitteln ein höheres Maß an Sicherheit bietet.

[0082] Die Sicherheitsarchitektur umfasst vorzugsweise im Wesentlichen drei Einheiten, die in einer bevorzugten Anordnung in Fig. 4 dargestellt sind:

- Ein Wertübertragungszentrum, in dem die Identität des Kunden und seines Kundensystems bekannt ist.
- Ein Sicherungsmodul, das die als nicht durch den Kunden manipulierbare Hard-/Software die Sicherheit im Kundensystem gewährleistet (z.B. Dongle oder Chipkarte bei Offline-Lösungen bzw. gleichwertige Server bei Online-Lösungen).
- Ein Briefzentrum, in dem die Gültigkeit der Freimachungsvermerke geprüft, beziehungsweise Manipulationen am Wertbetrag sowie am Freimachungsvermerk erkannt werden.

[0083] Die einzelnen Prozessschritte, die im Wertübertragungszentrum, Kundensystem und Briefzentrum erfolgen, sollen im Folgenden in Form einer Prinzipskizze dargestellt werden. Der genaue technische Kommunikationsprozess weicht hingegen von dieser prinzipiellen Darstellung ab (z.B. mehrere Kommunikationsschritte zur Erlangung einer hier dargestellten Übertragung). Insbesondere wird in dieser Darstellung eine vertrauliche und integere Kommunikation zwischen identifizierten und authentisierten Kommunikationspartnern vorausgesetzt.

Kundensystem

[0084]

1. Innerhalb des Sicherungsmoduls wird eine Zufallszahl erzeugt und zwischengespeichert, die dem Kunden nicht zur Kenntnis gelangt.

2. Innerhalb des Sicherungsmoduls wird die Zufallszahl zusammen mit einer eindeutigen Identifikationsnummer (Sicherungsmodul-ID) des Kundensystems, beziehungsweise des Sicherungsmoduls, derart kombiniert und verschlüsselt, dass nur das Wertübertragungszentrum in der Lage ist, eine Entschlüsselung durchzuführen.
In einer besonders bevorzugten Ausführungsform wird die Zufallszahl zusammen mit einem zuvor vom Wertübertragungszentrum ausgegebenen Sitzungsschlüssel und den Nutzdaten der Kommunikation (Beantragung der Einrichtung eines Abrechnungsbetrages) mit dem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt und mit dem privaten Schlüssel des Sicherungsmoduls digital signiert. Hierdurch wird vermieden, dass die Anfrage bei jedem Laden eines Abrechnungsbetrages dieselbe Gestalt hat und zum missbräuchlichen Laden von Abrechnungsbeträgen herangezogen werden kann (Replay-Attack).

3. Die kryptographisch behandelten Informationen aus dem Kundensystem werden an das Wertübertragungszentrum im Rahmen des Ladens eines Abrechnungsbetrages übertragen. Weder der Kunde noch Dritte können diese Informationen entschlüsseln.

[0085] In der Praxis wird die asymmetrische Verschlüsselung mit dem öffentlichen Schlüssel des Kommunikationspartners (Wertübertragungszentrum, beziehungsweise Sicherungsmodul) angewandt.

[0086] Bei der Möglichkeit eines vorhergehenden Austausches von Schlüsseln kommt eine symmetrische Verschlüsselung gleichfalls in Betracht.

Wertübertragungszentrum

[0087]

4. Im Wertübertragungszentrum wird unter anderem die Zufallszahl, die der Identifikationsnummer des Sicherungsmoduls (Sicherungsmodul-ID) zugeordnet werden kann, entschlüsselt.

5. Durch Anfrage in der Datenbank-Freimachung wird die Sicherungsmodul-ID ein Kunde der Deutschen Post zugeordnet.

6. Im Wertübertragungszentrum wird eine Ladevorgangsidentifikationsnummer gebildet, die Teile der Sicherungsmodul-ID, die Höhe eines Abrechnungsbetrages etc. beinhaltet. Die entschlüsselte Zufallszahl wird zusammen mit der Ladevorgangsidentifikationsnummer derart verschlüsselt, dass nur das Briefzentrum in der Lage ist, eine Entschlüsselung durchzuführen. Der Kunde ist hingegen nicht in der Lage, diese Informationen zu entschlüsseln. (Die Ladevorgangsidentifikationsnummer wird zusätzlich in einer vom Kundensystem entschlüsselbaren Form verschlüsselt). In der Praxis erfolgt die Verschlüsselung mit einem symmetrischen Schlüssel nach TDES, der ausschließlich

im Wertübertragungszentrum sowie in den Briefzentren vorhanden ist. Die Verwendung der symmetrischen Verschlüsselung an dieser Stelle ist begründet durch die Forderung schneller Entschlüsselungsverfahren durch die Produktion.

7. Die verschlüsselte Zufallszahl und die verschlüsselte Ladevorgangsidentifikationsnummer werden an das Kundensystem übertragen. Weder der Kunde noch Dritte können diese Informationen entschlüsseln. Durch die alleinige Verwaltung des posteigenen, vorzugsweise symmetrischen Schlüssels im Wertübertragungszentrum und in den Briefzentren kann der Schlüssel jederzeit ausgetauscht und Schlüssellängen können bei Bedarf geändert werden. Hierdurch wird auf einfache Weise eine hohe Manipulationssicherheit gewährleistet. In der Praxis wird die Ladevorgangsidentifikationsnummer dem Kunden zusätzlich in nicht verschlüsselter Form zur Verfügung gestellt.

Kundensystem

[0088]

8. Der Kunde erfasst im Rahmen der Erstellung eines Freimachungsvermerks die sendungsspezifischen Informationen oder Sendungsdaten (z.B. Porto, Sendungsart etc.), die in das Sicherungsmodul übertragen werden.

9. Innerhalb des Sicherungsmoduls wird ein Hash-Wert unter anderem aus folgenden Informationen gebildet

- Auszügen aus den Sendungsdaten (z.B. Porto, Sendungsart, Datum, PLZ etc.),
- der zwischengespeicherten Zufallszahl (die im Rahmen des Ladens eines Abrechnungsbetrages erzeugt wurde)
- und gegebenenfalls der Ladevorgangsidentifikationsnummer.

[0089] 10. In den Freimachungsvermerk werden unter anderem folgende Daten übernommen:

- Auszüge aus den Sendungsdaten im Klartext (z.B. Porto, Sendungsart, Datum, PLZ etc.),
- die verschlüsselte Zufallszahl und die verschlüsselte Ladevorgangsidentifikationsnummer aus dem Wertübertragungszentrum und
- der innerhalb des Sicherungsmoduls gebildete Hash-Wert aus Sendungsdaten, Zufallszahl und Ladevorgangsidentifikationsnummer.

Briefzentrum

[0090]

11. Im Briefzentrum werden zunächst die Sendungsdaten geprüft. Stimmen die in den Freimachungsvermerk übernommenen Sendungsdaten nicht mit der Sendung überein, so liegen entweder eine Falschfrankierung, eine Phantasie- oder eine Schmiermarke vor. Die Sendung ist der Entgeltsicherung zuzuführen.

12. Im Briefzentrum werden die Zufallszahl und die Ladevorgangsidentifikationsnummer, die im Rahmen des Abrechnungsbetrages an das Kundensystem übergeben wurden, entschlüsselt. Hierzu ist im Briefzentrum nur ein einziger (symmetrischer) Schlüssel erforderlich. Bei Verwendung von individuellen Schlüsseln wäre jedoch statt dessen eine Vielzahl von Schlüsseln einzusetzen.

13. Im Briefzentrum wird nach demselben Verfahren wie in dem Sicherungsmodul ein Hash-Wert aus folgenden Informationen gebildet:

- Auszügen aus den Sendungsdaten,
- der entschlüsselten Zufallszahl
- der entschlüsselten Ladevorgangsidentifikationsnummer.

14. Im Briefzentrum werden der selbstgebildete und der übertragene Hash-Wert verglichen. Stimmen beide überein, so wurde der übertragene Hash-Wert mit derselben Zufallszahl gebildet, die auch dem Wertübertragungszentrum im Rahmen des Ladens des Abrechnungsbetrages übermittelt wurde. Demnach handelt es sich sowohl um einen echten, gültigen Abrechnungsbetrag als auch um Sendungsdaten, die dem Sicherungsmodul bekanntgegeben

wurden (Gültigkeitsprüfung). Vom Aufwand her entsprechen die Entschlüsselung, die Bildung eines Hash-Wertes und der Vergleich von zwei Hash-Werten theoretisch dem einer Signaturprüfung. Aufgrund der symmetrischen Entschlüsselung entsteht jedoch gegenüber der Signaturprüfung ein zeitlicher Vorteil.

15. Über eine Gegenprüfung im Hintergrundsystem können im Nachhinein Abweichungen zwischen geladenen Abrechnungsbeträgen und Frankierbeträgen ermittelt werden (Überprüfung hinsichtlich Sendungsdubletten, Saldenbildung im Hintergrundsystem).

[0091] Die dargestellte grundsätzliche Sicherheitsarchitektur umfasst nicht die separat abgesicherte Verwaltung der Abrechnungsbeträge (Börsenfunktion), die Absicherung der Kommunikation zwischen Kundensystem und dem Wertübertragungszentrum, die gegenseitige Identifizierung von Kundensystem und Wertübertragungszentrum und die Initialisierung zur sicheren Betriebsaufnahme eines neuen Kundensystems.

[0092] Angriffe auf die Sicherheitsarchitektur Die beschriebene Sicherheitsarchitektur ist sicher gegenüber Angriffen durch Folgendes:

- Dritte können die im Internet mitgeschnittene (kopierte) erfolgreiche Kommunikation zwischen einem Kundensystem und dem Wertübertragungszentrum nicht zu betrügerischen Zwecken nutzen (Replay-Attacke).
- Dritte oder Kunden können gegenüber dem Wertübertragungszentrum nicht die Verwendung eines ordnungsgemäßen Kundensystems durch ein manipuliertes Kundensystem vortäuschen. Spiegelt ein Dritter oder ein Kunde die Übertragung einer Zufallszahl und einer Safe-Box-ID vor, die nicht innerhalb eines Sicherungsmoduls erzeugt wurden, sondern ihm bekannt sind, so scheitert das Laden der Abrechnüngsbeträge entweder an der separat durchgeführten Identifikation des rechtmäßigen Kunden durch Benutzername und Kennwort oder an der Kenntnis des privaten Schlüssels des Sicherungsmoduls, der dem Kunden unter keinen Umständen bekannt sein darf. (Deshalb ist der Initialisierungsprozess zur Schlüsselerzeugung in dem Sicherungsmodul und die Zertifizierung des öffentlichen Schlüssels durch den Kundensystemanbieter geeignet durchzuführen.)
- Dritte oder Kunden können nicht mit einem vorgetäuschten Wertübertragungszentrum gültige Abrechnungsbeträge in ein Kundensystem laden. Spiegelt ein Dritter oder ein Kunde die Funktionalität des Wertübertragungszentrums vor, so gelingt es diesem vorgespiegelten Wertübertragungszentrum nicht, eine verschlüsselte Ladevorgangsidentifikationsnummer zu erzeugen, die im Briefzentrum ordnungsgemäß entschlüsselt werden kann. Zudem kann das Zertifikat des öffentlichen Schlüssels des Wertübertragungszentrums nicht gefälscht werden.
- Kunden können nicht unter Umgehung des Wertübertragungszentrums einen Freimachungsvermerk erstellen, dessen Ladevorgangsidentifikationsnummer derart verschlüsselt ist, dass sie im Briefzentrum als gültig entschlüsselt werden könnte.

[0093] Zur Erhöhung der Datensicherheit, insbesondere beim Suchen, ist eine erschöpfende Anzahl von Zufallszahlen zur Hash-Wert-Bildung heranzuziehen.

- Die Länge der Zufallszahl ist daher möglichst gross und beträgt vorzugsweise mindestens 16 byte (128 bit).

Die eingesetzte Sicherheitsarchitektur ist durch die Möglichkeit, kundenspezifische Schlüssel einzusetzen, ohne dass es notwendig ist, in zur Entschlüsselung bestimmten Stellen, insbesondere Briefzentren, Schlüssel bereit zu halten, den bekannten Verfahren überlegen. Diese vorteilhafte Ausgestaltung ist ein wesentlicher Unterschied zu den bekannten Systemen nach dem Information-Based Indicia Program (IBIP).

Falls keine Signaturprüfung wie im Modell IBIP erfolgt, würde keine wesentlich höhere Sicherheit als bei der Absenderfreistempelung erzielt. Wird zudem die Tatsache bekannt, dass die digitalen Signaturen nicht geprüft werden, könnte dies zu einem Anstieg des Missbrauchs führen. Werden nämlich in missbräuchlicher Absicht alle Angaben, die zur Plausibilitätsprüfung herangezogen werden, gefälscht, ohne jedoch eine gültige Signatur anzufügen, so kann dieser Missbrauch auch bei erheblichem Umfang außerhalb von Stichproben nicht erkannt werden.

[0094] Vorteile der Sicherheitsarchitektur Folgende Merkmale zeichnen die beschriebene Sicherheitsarchitektur gegenüber dem IBIP-Modell der USA aus:

- Die eigentliche Sicherheit wird in den Systemen der Deutschen Post (Wertübertragungszentrum, Briefzentrum, Entgeltsicherungssystem) gewährleistet und ist damit vollständig im Einflussbereich der Deutschen Post.
- Es werden im Freimachungsvermerk keine Signaturen, sondern technisch gleichwertige und ebenso sichere (symmetrisch) verschlüsselte Daten und Hash-Werte angewandt. Hierzu wird im einfachsten Falle nur ein symmetrischer Schlüssel verwendet, der alleine im Einflussbereich der Deutschen Post liegt und somit leicht austauschbar ist.
- Im Briefzentrum ist eine Überprüfung aller Freimachungsmerkmale (nicht bloß stichprobenweise) möglich.
- Das Sicherheitskonzept basiert auf einem einfachen, in sich geschlossenen Prüfkreislauf, der in Einklang mit einem

hierauf angepaßten Hintergrundsystem steht.

- Das System macht selbst ansonsten kaum feststellbare Dubletten erkennbar.
- Ungültige Phantasiemarken sind mit diesem Verfahren mit hoher Genauigkeit erkennbar.
- Neben der Plausibilitätsprüfung kann bei allen Freimachungsvermerken eine Überprüfung der Ladevorgangsidentifikationsnummer in Echtzeit erfolgen.

Sendungsarten

[0095] Mit der PC-Frankierung können alle Produkte des Versendungsdienstleisters wie beispielsweise "Brief national" (einschließlich Zusatzleistungen) und "Direkt Marketing national" gemäß einer vorhergehenden Festlegung durch den Versendungsdienstleister freigemacht werden.

[0096] Ein Einsatz für andere Versandformen wie Paket- und Expresssendungen ist gleichermassen möglich.

[0097] Der Gebührenbetrag, der maximal über das Wertübertragungszentrum geladen werden kann, wird auf einen geeigneten Betrag festgelegt. Der Betrag kann je nach Anforderung des Kunden und dem Sicherheitsbedürfnis des Postdienstleisters gewählt werden. Während für einen Einsatz im Privatkundenbereich ein Gebührenbetrag von maximal mehreren hundert DM besonders zweckmäßig ist, werden für Einsätze bei Grosskunden wesentlich höhere Gebührenbeträge vorgesehen. Ein Betrag in der Grössenordnung von etwa DM 500,- eignet sich sowohl für anspruchsvolle Privathaushalte als auch für Freiberufler und kleinere Unternehmen. Der in der Börse gespeicherte Wert sollte vorzugsweise den doppelten Wertbetrag systemtechnisch nicht überschreiten.

[0098] Falschfrankierte Sendungen Falschfrankierte und nicht zur Beförderung geeignete, bereits bedruckte Schreiben, Umschläge etc. mit einem gültigen Freimachungsvermerk werden dem Kunden gutgeschrieben.

[0099] Durch geeignete Maßnahmen, beispielsweise durch eine Stempelung von in dem Briefzentrum eingehenden Sendungen, ist es möglich festzustellen, ob eine Sendung bereits befördert wurde. Hierdurch wird verhindert, dass Kunden bereits beförderte Sendungen vom Empfänger zurück erhalten und diese zur Gutschrift bei dem Postdientsbetreiber, beispielsweise der Deutschen Post AG, einreichen.

[0100] Die Rücksendung an eine zentrale Stelle des Versendungsdienstleisters, beispielsweise der Deutschen Post, ermöglicht ein hohes Maß an Entgeltsicherung durch Abgleich der Daten mit Abrechnungsbeträgen und die Kenntnis über die häufigsten Zusendungsgründe. Hierdurch besteht gegebenenfalls die Möglichkeit der Nachsteuerung durch Änderung der Einführungsvoraussetzungen mit dem Ziel der Reduzierung der Rücksendequote.

[0101] Gültigkeit von Freimachungswerten Vom Kunden gekaufte Abrechnungswerte sind aus Gründen der Entgeltsicherung beispielsweise nur 3 Monate gültig. Ein entsprechender Hinweis ist in der Vereinbarung mit dem Kunden aufzunehmen. Können Frankierwerte nicht innerhalb von 3 Monaten aufgebraucht werden, muss vom Kundensystem die Kontaktierung des Wertübertragungszentrums zu einer erneuten Herstellung von Freimachungsvermerken aufgenommen werden. Bei dieser Kontaktierung wird, wie beim ordentlichen Laden von Abrechnungsbeträgen, der Restbetrag eines alten Abrechnungsbetrages einem neu ausgegebenen Abrechnungsbetrag zugeschlagen und unter einer neuen Ladevorgangsidentifikationsnummer dem Kunden zur verfügung gestellt wird.

[0102] Besondere betriebliche Behandlung Grundsätzlich können die Freimachungsvermerke eine beliebige Form aufweisen, in der die in ihnen enthaltenen Informationen wiedergegeben werden können. Es ist jedoch zweckmässig, die Freimachungsvermerke so zu gestalten, dass sie wenigstens bereichsweise die Form von Barcodes aufweisen. Bei der dargestellten Lösung des 2D-Barcodes und der daraus resultierenden Entgeltsicherung sind folgende Besonderheiten in der Produktion zu berücksichtigen:

PC-frankierte Sendungen können über alle Einlieferungsmöglichkeiten, auch über Briefkasten, eingeliefert werden.

[0103] Durch die Festlegung von Zulassungsvoraussetzungen für Hersteller von für die Schnittstellen relevanten Bestandteilen des Frankierungssystems, insbesondere für Hersteller und/oder Betreiber von Kundensystemen, wird die Einhaltung der dargestellten Sicherheitsmaßnahmen weiter erhöht.

[0104] Übergeordnete Normen, Standards und Vorgaben International Postage Meter Approval Requirements (IPMAR)

[0105] Vorzugsweise finden die Vorschriften der aktuellsten Fassung des Dokuments International Postage Meter Approval Requirements (IPMAR), UPU S-30, ebenso Anwendung wie alle Normen und Standards, auf die in diesem Dokument verwiesen wird. Die Einhaltung aller dort genannten "Requirements" ist, soweit möglich, für das Kundensystem sinnvoll.

[0106] Digital Postage Marks: Applications, Security & Design Grundsätzlich finden die Vorschriften der aktuellen Fassung des Dokuments Digital Postage Marks: Applications, Security & Design (UPU: Technical Standards Manual) ebenso Anwendung wie alle Normen und Standards, auf die in diesem Dokument verwiesen wird. Die Einhaltung des

"normativen" Inhalts sowie die weitestgehende Beachtung des "informativen" Inhalts dieses Dokuments ist, soweit möglich, für das Kundensystem sinnvoll.

[0107] Vorzugsweise finden Regelungen und Bestimmungen des Versendungsdienstleistungsunternehmens gleichfalls Anwendung.

[0108] Durch eine Zulassung lediglich solcher Systeme, die alle gesetzlichen Bestimmungen ebenso erfüllen wie alle Normen und Standards des Versendungsdienstleisters, werden Datensicherheit und Zuverlässigkeit des Systems ebenso gewährleistet wie seine Benutzerfreundlichkeit.

Weitere Gesetze, Verordnungen, Richtlinien, Vorschriften Normen und Standards

[0109] Grundsätzlich finden alle Gesetze, Verordnungen, Richtlinien, Vorschriften, Normen und Standards der jeweils gültigen Fassung Anwendung, die zur Entwicklung und zum Betrieb eines technischen Kundensystems in der konkreten Ausprägung zu beachten sind.

Systemtechnische Interoperabilität

[0110] Die systemtechnische Interoperabilität bezieht sich auf die Funktionsfähigkeit der Schnittstellen des Kundensystems, beziehungsweise auf die Einhaltung der in den Schnittstellenbeschreibungen spezifizierten Vorgaben.

Schnittstelle Abrechnungsbetrag Kommunikationsweg, Protokolle

[0111] Die Kommunikation über die Schnittstelle Abrechnungsbetrag erfolgt vorzugsweise über das öffentliche Internet auf der Basis der Protokolle TCP/IP und HTTP. Der Datenaustausch kann optional per HTTP über SSL verschlüsselt werden (https). Hier dargestellt ist der Soll-Prozess einer erforderlichen Übertragung.

[0112] Der Datenaustausch erfolgt vorzugsweise, sofern möglich, über HTML- und XML-kodierte Dateien. Die textlichen und graphischen Inhalte der HTML-Seiten sind im Kundensystem darzustellen.

[0113] Es erscheint empfehlenswert, bei den Kommunikationsseiten auf eine bewährte HTML-Version zurückzugreifen und auf die Verwendung von Frames, eingebetteten Objekten (Applets, ActiveX etc.) und ggf. animierten GIFs zu verzichten.

Anmeldung zum Laden eines Abrechnungsbetrages (erste Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum)

[0114] Im Rahmen der ersten Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum werden das Zertifikat des Sicherungsmoduls sowie ein Aktionsindikator A unverschlüsselt und unsigniert übertragen.

[0115] Rückmeldung zur Anmeldung (erste Antwort vom Wertübertragungszentrum zum Sicherungsmodul) Die Rückmeldung des Wertübertragungszentrums enthält das eigene Zertifikat des Wertübertragungszentrums, einen verschlüsselten Sitzungsschlüssel und die digitale Signatur des verschlüsselten Sitzungsschlüssels.

Zweite Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum

[0116] Im Rahmen dieser Übertragung sendet das Sicherungsmodul den neu verschlüsselten Sitzungsschlüssel, die verschlüsselte Zufallszahl und den verschlüsselten Datensatz mit Nutzdaten (Höhe eines vorab geladenen Abrechnungsbetrages, Restwert des aktuellen Abrechnungsbetrages, aufsteigendes Register aller Abrechnungsbeträge, letzte Ladevorgangsidentifikationsnummer) an das Wertübertragungszentrum (alles asymmetrisch mit dem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt). Gleichzeitig sendet das Sicherungsmodul die digitale Signatur dieser verschlüsselten Daten an das Wertübertragungszentrum. Gleichzeitig kann das Kundensystem weitere, nicht verschlüsselte und nicht signierte Nutzungsprotokolle oder Nutzungsprofile an das Wertübertragungszentrum senden.

[0117] Es ist zweckmässig, dass die Nutzungsdaten in ein Nutzungsprotokoll eingetragen werden und dass das Nutzungsprotokoll und/oder die darin vermerkten Einträge digital signiert werden.

Zweite Antwort vom Wertübertragungszentrum zu dem Sicherungsmodul

[0118] Das Wertübertragungszentrum übermittelt die symmetrisch verschlüsselte Zufallszahl und die symmetrisch verschlüsselte Ladevorgangsidentifikationsnummer an das Sicherungsmodul. Außerdem übermittelt das Wertübertragungszentrum die mit dem öffentlichen Schlüssel des Sicherungsmoduls Ladevorgangsidentifikationsnummer, Login-Informationen für das Sicherungsmodul sowie einen neuen Sitzungsschlüssel an das Sicherungsmodul. Die gesamten übertragenen Daten werden zudem digital signiert.

Dritte Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum

[0119] Im Rahmen der dritten Übertragung werden von dem Sicherungsmodul der neue Sitzungsschlüssel, die neue Ladevorgangsidentifikationsnummer zusammen mit Nutzdaten zur Bestätigung der erfolgreichen Kommunikation allesamt in verschlüsselter und digital signierter Form an das Wertübertragungszentrum übertragen.

Dritte Antwort vom Wertübertragungszentrum an das Sicherungsmodul

[0120] Bei der dritten Antwort quittiert das Wertübertragungszentrum den Erfolg der Übertragung ohne Anwendung kryptographischer Verfahren.

Deinstallation

[0121] Die Möglichkeit einer Deinstallation des Kundensystems muss durch den Kunden möglich sein.

[0122] Die detaillierte, technische Beschreibung der Schnittstelle Abrechnungsbetrag erfolgt mit Konzeption des posteigenen Wertübertragungszentrums.

Nutzungsprotokoll und Nutzungsprofil

[0123] Im Kundensystem ist im Rahmen jeder Erzeugung eines Freimachungsvermerks ein Protokolleintrag zu erzeugen, der alle Angaben des jeweiligen Freimachungsvermerks - versehen mit einer digitalen Signatur des Sicherungsmoduls - enthalten muss. Weiterhin muss im Protokoll jeder Fehlerstatus des Sicherungsmoduls derart verzeichnet werden, dass die manuelle Löschung dieses Eintrags bei der Überprüfung bemerkt wird.

[0124] Das Nutzungsprofil enthält eine aufbereitete Zusammenfassung der Nutzungsdaten seit der letzten Kommunikation mit dem Wertübertragungszentrum.

[0125] Ist ein Kundensystem in eine beim Kunden befindliche und eine zentral (z.B. im Internet befindliche) Komponente aufgetrennt, so muss das Nutzungsprofil in der zentralen Komponente geführt werden.

Schnittstelle Freimachungsvermerk Bestandteile und Ausprägungen

[0126] Das Kundensystem muss in der Lage sein, PC-Freimachungsvermerke zu erzeugen, die exakt den Vorgaben der Deutschen Post, beziehungsweise dem Rahmen der gängigen CEN-und UPU-Standards entsprechen.

[0127] PC-Freimachungsvermerke bestehen vorzugsweise aus folgenden drei Elementen:

- Einem 2-dimensionalen Strichcode, Barcode oder Matrixcode, in dem sendungsspezifische Informationen in maschinenlesbarer Form dargestellt sind. (Zweck: Automatisierung in der Produktion und Entgeltsicherung der Deutschen Post.)
- Text in Klarschrift, der wichtige Teile der Strichcode-Information in lesbarer Form wiedergibt. (Zweck: Kontrollmöglichkeit für den Kunden sowie in der Produktion und Entgeltsicherung der Deutschen Post.)
- Eine den Versendungsdienstleister, beispielsweise die Deutsche Post, kennzeichnende Marke wie beispielsweise ein Posthorn.

Spezifikation des Dateninhaltes

[0128] Zweckmäßigerweise enthalten Strichcode und Klartext des PC-Freimachungsvermerks folgende Informationen:

Tabelle: Inhalt des PC-Freimachungsvermerks

		Im Strichcode	Im Klartext		Größe (Byte)	Typ	Anmerkung
1	PostUnternehmen	Ja	Nein		3	Binär	z.B.Deutsche Post
2	Freimachungsart	Ja	Nein		1	Binär	z.B. PC-Frankierung
3	Version und Version Preis/Produkt	Ja	Nein		1	Binär	

(fortgesetzt)

		Im Strichcode	Im Klartext		Größe (Byte)	Typ	Anmerkung
4	Krypto-Algorithmus-ID	Ja	Nein		1	Binär	z.B. TDES, 128 bit
5	Ladevorgangsidentifikationsnummer (verschlüsselt) - Hersteller - Modell - Serien-Nr. - lfd. Vorgabe - Betrag - Währung - Gültig bis - Redundanz	Ja			16	Binär	
6	Zufallszahl (verschlüsselt)	Ja	Nein		16	Binär	
7	lfd. Sendungs-Nr.	Ja	Ja		3	Binär	bezogen auf das Sicherungsmodul
8a	Produktart	Ja	Ja		2	Binär	einschl. Zusatzleistung - Im Klartext nur bei ermäßigten Sendungsarten (z.B. Infobrief)
8b	Versendungsform	Nein	Ja		-		Sendungsart bzw. gesonderte Versendungsform
9	Entgelt	Ja	Ja		2	Binär	Klartext in ASCII
10	Freimachungsdatum	Ja	Ja		3	Binär	
11	PLZ des Empfängers	Ja	Nein		3	Binär	
12	Straße/Postfach des Empfängers	Ja	Nein		6	ASCII	Ersten und letzten drei Stellen der Anschrift
13	Restwert des Wertbetrages	Ja	Nein		3	Binär	
14	Hash-Wert	Ja	Nein		20	Binär	SHA-1

[0129] Beschrieben wird hier nur der Inhalt des Freimachungsvermerks. Die Vorschriften des Versendungsdienstleisters für den Inhalt der Adressangaben behalten unverändert ihre Gültigkeit.

Spezifikation der physikalischen Ausprägung auf Papier (Layout)

[0130] Der Freimachungsvermerk ist vorteilhafterweise im Anschriftenfeld linksbündig oberhalb der Anschrift auf der Sendung angebracht.

[0131] Das Anschriftenfeld wird in der jeweils gültigen Fassung der Normen des Versendungsdienstleisters spezifiziert. So werden insbesondere folgende Freimachungen ermöglicht:

- Aufdruck auf den Briefumschlag,
- Aufdruck auf Klebeetiketten oder
- Verwendung von Fensterbriefumschlägen derart, dass der Aufdruck auf den Brief durch das Fenster vollständig

sichtbar ist.

[0132] Für die einzelnen Elemente des Freimachungsvermerks gilt vorzugsweise:

- Verwendet wird zunächst der Strichcode vom Type Data Matrix, dessen einzelne Bildpunkte eine Kantenlänge von mindestens 0,5 Millimeter aufweisen sollten. Im Hinblick auf lesetechnische Voraussetzungen sollte ein 2D-Barcode in Form der Data Matrix mit einer minimalen Pixelgröße von 0,5 mm bevorzugt zur Anwendung kommen. Eine ggf. zweckmäßige Option besteht darin, die Pixel-Größe auf 0,3 mm zu reduzieren.
  Bei einer Darstellungsgröße von 0,5 mm pro Pixel ergibt sich eine Kantenlänge des gesamten Barcodes von ca. 18 bis 20 mm, wenn alle Daten wie beschrieben eingehen. Falls es gelingt, Barcodes mit einer Pixelgröße von 0,3 mm in der ALM zu lesen, lässt sich, die Kantenlänge auf ca. 13 mm reduzieren.
  Eine nachträgliche Erweiterung der Spezifikationen auf die Verwendung eines anderen Barcodes (z.b. Aztec) bei gleichen Dateninhalten ist möglich.

[0133] Eine bevorzugte Ausführungsform des Layouts und der Positionierung der einzelnen Elemente des Freimachungsvermerks ist nachfolgend in Fig. 5 beispielhaft dargestellt.

[0134] Die "kritischste" Größe ist die Höhe des dargestellten Fensters eines Fensterbriefumschlags mit einer Größe von 45 mm x 90 mm. Hier dargestellt wird ein DataMatrix-Code mit einer Kantenlänge von ca. 13 mm, der bei Verwendung der vorgeschlagenen Datenfelder nur bei einer Pixelauflösung von 0,3 mm möglich ist. Ein Code mit einer Kantenlänge von 24 mm lässt bezüglich der zur Verfügung stehenden Höhe keinen ausreichenden Raum für Angaben zur Anschrift.

Druckqualität und Lesbarkeit

[0135] Verantwortlich für den einwandfreien Aufdruck des Freimachungsvermerks sind der Hersteller des Kundensystems im Rahmen des Zulassungsverfahrens sowie der Kunde im späteren Betrieb. Hierzu ist der Kunde durch geeignete Hinweise in einem Benutzerhandbuch und einem Hilfesystem hinzuweisen. Dies gilt insbesondere für das saubere Haften von Etiketten und das Verhindern des Verrutschens (von Teilen) des Freimachungsvermerks außerhalb des sichtbaren Bereichs von Fensterbriefumschlägen.

[0136] Die maschinelle Lesbarkeit von Freimachungsvermerken steht in Abhängigkeit von der verwendeten Druckauflösung und vom Kontrast. Sollen statt schwarz auch andere Farben zur Anwendung kommen, so ist mit einer geringeren Leserate zu rechnen. Es ist davon auszugehen, dass die geforderte Leserate bei einer im Drucker verwendeten Auflösung von 300 dpi ("dots per inch") bei hohem Druck-Kontrast gewährleistet werden kann; das entspricht etwa 120 Bildpunkten pro Zentimeter.

Testdrucke

[0137] Das Kundensystem muss in der Lage sein, Freimachungsvermerke zu produzieren, die in Ausprägung und Größe gültigen Freimachungsvermerken entsprechen, jedoch nicht für den Versand bestimmt sind, sondern für Kontrollausdrucke und der Drucker-Feinjustierung dienen.

[0138] Vorzugsweise ist das Kundensystem so gestaltet, dass die Testdrucke sich in einer für das Versendungsunternehmen erkennbaren Weise von tatsächlichen Freimachungsvermerken unterscheidet. Dazu wird beispielsweise in der Mitte des Freimachungsvermerks die Aufschrift "MUSTER - nicht versenden" angebracht. Mindestens zwei Drittel des Barcodes, sollen durch die Aufschrift oder anderweitig unkenntlich gemacht werden.

[0139] Neben echten (bezahlten) Freimachungsvermerken dürfen außer gesondert gekennzeichneten Testdrucken keine Nulldrucke hergestellt werden.

Anforderungen an das Kundensystem Basis-System Überblick und Funktionalität

[0140] Das Basis-System dient als Bindeglied zwischen den anderen Komponenten der PC-Frankierung, namentlich dem Wertübertragungszentrum, des Sicherungsmoduls, dem Drucker und dem Kunden. Es besteht aus einem oder mehreren Computersystemen, zum Beispiel PCs, die ggf. auch durch ein Netzwerk miteinander verbunden sein können.

[0141] Eine Darstellung des Gesamtsystems ist in Fig. 6 dargestellt.

[0142] Das Basis-System stellt auch die komfortable Benutzung des Gesamtsystems durch den Kunden sicher.

Anforderungen an den Aufbau und die Sicherheit

[0143] Das Basis-System verfügt vorzugsweise über vier Schnittstellen:

1. Über die beschriebene Schnittstelle Abrechnungsbetrag erfolgt die Kommunikation mit dem Wertübertragungszentrum.

2. Über eine Schnittstelle zum Sicherungsmodul werden alle Informationen ausgetauscht, die dem Sicherungsmodul bekanntgegeben werden müssen (Abrechnungsbetrag, beziehungsweise Ladevorgangsidentifikationsnummer, sendungsspezifische Daten zu einzelnen Frankierungen). Außerdem werden über diese Schnittstellen alle Daten mit dem Sicherungsmodul ausgetauscht (kryptographisch verarbeitete Daten).

3. Über eine Schnittstelle zum Drucker wird dieser angesteuert.

4. Über eine Schnittstelle zum Benutzer, beziehungsweise Kunden (Graphical User Interface, GUI), muss dieser alle relevanten Prozesse in Interaktion mit der größtmöglichen Ergonomie veranlassen können.

[0144] Im Basis-System sollten außerdem folgende Daten gespeichert und verarbeitet werden:

- Benutzerspezifische Einstellungen/Daten,
- detaillierte Nutzungsprotokolle und Nutzungsprofile,
- bei Verwendung von SSL: auswechselbare Zertifikate, mit denen die Gültigkeit der SSL-Zertifikate verifiziert werden können und
- alle relevanten Informationen über die Produkte und Preise des Versendungsdienstleisters.

Funktionsumfang und Abläufe

[0145] Das Basis-System unterstützt vorzugsweise folgende Abläufe:

- Erstinstallation mit Benutzerhilfe,
- Benutzeridentifikation, insbesondere gegenüber dem Sicherungsmodul; gegebenenfalls mit unterschiedlichen Berechtigungen für Laden von Abrechnungsbeträgen und Herstellung von Freimachungsvermerken,
- gegebenenfalls Administration mehrerer Benutzer,
- Unterstützung des Benutzers beim Laden von Abrechnungsbeträgen (hierbei Unterstützung der Wiedergabe von Informationen, die vom Wertübertragungszentrum in Form von HTML-kodierten Dateien gesandt werden),
- Unterstützung des Benutzers beim Auftreten von Problemen beim Laden von Abrechnungsbeträgen,
- für den Benutzer transparente Verwaltung des Wertbetrages (Kontoübersicht),
- Verwaltung von Nutzungsprotokollen, Aufbereitung von Nutzungsprofilen und Übertragung von Nutzungsprotokollen oder -profilen,
- Unterstützung des Benutzers bei der Erzeugung und beim Ausdruck des Freimachungsvermerks (Veranschaulichung eines Musters des zu druckenden Freimachungsvermerks auf dem Bildschirm - WYSIWYG),
- plausibilitätsgesicherte Entgeltberechnung gemäß Service-Information der Deutschen Post,
- elektronisches Hilfesystem,
- automatische Aktualisierung der relevanten Informationen über die Produkte und Preise der Deutschen Post bei Änderungen sowie Information des Kunden über die stattfindende und abgeschlossene Aktualisierung,
- technische Unterbindung des mehrfachen Ausdrucks ein- und desselben Freimachungsvermerks und
- De-Installation des Kundensystems.

Sicherungsmodul

Aufgabe und Sicherheitsniveau

Das Sicherungsmodul gewährleistet als "kryptographisches Modul" im Sinne der FIPS PUB 140, Security Requirements for Cryptographic Modules, die eigentliche Sicherheit des Kundensystems. Sie besteht aus Hardware, Software, Firmware oder einer Kombination hieraus und beherbergt die kryptographische Logik und die kryptographischen Prozesse, das heißt, die Verwaltung und Anwendung kryptographischer Verfahren sowie die manipulationssichere Speicherung des Wertbetrages. Die Anforderungen, denen das Sicherungsmodul genügen muss, werden

- bezüglich des Sicherheitsstandards durch geeignete Normen, wie beispielsweise FIPS PUB 140 definiert und
- bezüglich der Einhaltung von Post-Standards durch die an FIPS PUB 140 angelehnte UPU-Veröffentlichung "International Postage Meter Approval Requirements (IPMAR)" definiert.

[0146] Zur Einführung und zum Betrieb in einem Kundensystem muss ein Sicherungsmodul als Kryptographisches Modul nach FIPS PUB 140 - vorzugsweise nach Sicherheitsstufe 3 (Security Level 3) - im Rahmen des Einführungsverfahrens entsprechend zertifiziert werden.

Prozesse des Sicherungsmoduls

[0147] Das Sicherungsmodul sollte vorzugsweise zur Initialisierung und zur Kommunikation mit dem Wertübertragungszentrum und Deaktivierung neben üblichen Operationen im Wesentlichen folgende Prozesse unterstützen, die im hinteren Teil des Anhangs Technische Beschreibung Kundensystem detailliert beschrieben werden:

- Schlüsselerzeugung
- Ausgabe des öffentlichen Schlüssels
- Zertifikatspeicherung
- Signaturerzeugung
- Signaturprüfung
- Zertifikatprüfung
- Temporäre Zertifikatspeicherung
- Asymmetrische Verschlüsselung
- Asymmetrische Entschlüsselung
- Zufallszahlerzeugung
- Speicherung eines Sitzungsschlüssels
- Speicherung von zwei Ladevorgangsidentifikationsnummern
- Speicherung des aktuellen Registerwerts der Abrechnungsbeträge
- Speicherung des aufsteigenden Registerwerts
- Benutzeridentifikation
- Statusausgabe der Gültigkeit der Abrechnungsbeträge
- Statusausgabe des Registerwerts der Abrechnungsbeträge
- Hash-Bildung der sendungspezifischen Daten
- Verminderung der Registerwerte von geladenen Abrechnungsbeträgen
- Fehlerprotokollierung
- Selbsttest
- Deaktivierung

Testdrucke

[0148] Das Sicherungsmodul wird beim Testdruck nicht verwendet und daher auch nicht kontaktiert.

Drucker

[0149] Der Drucker kann nach Massgabe des Herstellers des Kundensystems entweder ein handelsüblicher Standarddrucker oder ein Spezialdrucker sein.

[0150] Die große Mehrzahl heutiger Laser- und Tintenstrahldrucker sollte prinzipiell für die PC-Frankierung geeignet sein. Empfohlen werden sollten Drucker mit einer Auflösung von wenigstens 300 dpi (dots per inch).

Prozesse innerhalb des Kundensystems Ablauf der Erzeugung von Freimachungsvermerken

[0151] Durch das Kundensystem führt der Kunde folgende Teilprozesse bei der Erzeugung von Freimachungsvermerken durch:

- Aufbau der Verbindung zum Sicherungsmodul: Über das Basis-System wird eine Verbindung zum Sicherungsmodul hergestellt.
- Identifikation des Benutzers: Der Benutzer identifiziert sich mit Passwort/PIN persönlich bei dem Sicherungsmodul und aktiviert diese somit.
- Eingabe der sendungsspezifischen Informationen: Der Kunde gibt, mit Unterstützung des Kundensystems, die erforderlichen sendungsspezifischen Informationen in das Basis-System ein, das die wesentlichen Daten an das Sicherungsmodul übergibt.
- Erzeugung des Freimachungsvermerks: Das Basis-System erzeugt aus den sendungsspezifischen Daten und den kryptographisch verarbeiteten Daten aus dem Sicherungsmodul einen Freimachungsvermerk.
- Protokollierung der Herstellung von Freimachungsvermerken: Jede erfolgreiche Rückübertragung wird in einem Nutzungsprotokoll des Basis-Systems festgehalten. Bei einer Aufteilung des Kundensystems in eine lokale Komponente beim Kunden und eine zentrale Komponente (z.B. im Internet) ist das Nutzungsprotokoll in der zentralen Komponente zu führen.

- Abbau der Kommunikationsbeziehung: Sind alle angeforderten Freimachungsvermerke hergestellt worden, so wird die Kommunikationsbeziehung wieder abgebaut. Bei erneuter Herstellung von Freimachungsvermerken ist die Benutzeridentifikation wieder - wie oben beschrieben - vorzunehmen.
- Testdrucke: Alternativ zu dieser Vorgehensweise ist es möglich, die Benutzerführung so weit fortschreiten zu lassen, dass ein Muster eines Freimachungsvermerks sowohl auf dem Bildschirm dargestellt (WYSIWYG) als auch als (nicht gültiger) Testdruck ausgedruckt werden kann. Erst in einem späten Stadium würde hierbei der oben genannte Prozess der Einbeziehung des Sicherungsmoduls erfolgen.

[0152] Der Einsatz des technischen Systems wird durch zweckmäßige organisatorische Maßnahmen flankiert, so dass ein technisch registrierbarer Mehrfachversand eines Freimachungsvermerkes auch als ein Verstoß gegen Geschäftsbedingungen des Versenders betrachtet wird.

[0153] Ferner ist es vorteilhaft, geeignete technische Parameter für den Ausdruck der Freimachungsvermerke vorzusehen, insbesondere bezüglich der Druckqualität, damit die Freimachungsvermerke in automatischen Erfassungseinrichtungen besser erfasst werden können.

[0154] Für eine Überprüfung der Systeme können geeignete Qualitätssicherungssysteme, insbesondere nach den Normen ISO 9001 ff. zugrunde gelegt werden.

Patentansprüche

1. Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken, wobei ein Kundensystem von einem Wertübertragungszentrum über eine Datenleitung einen Gebührenbetrag lädt, wobei das Kundensystem ein Drukken von Freimachungsvermerken auf Postsendungen steuert und wobei das Wertübertragungszentrum ein Datenpaket an das Kundensystem sendet,
   dadurch gekennzeichnet,

   - **dass** in einem Sicherungsmodul des Kundensystems, auf das der Kunde keinen Zugriff hat, eine Zufallszahl erzeugt und zwischengespeichert wird,
   - **dass** in dem Kundensystem die Zufallszahl enthaltende Daten so verschlüsselt werden, dass das wertübertragungszentrum diese entschlüsseln kann, und dass die Daten von dem Kundensystem an das Wertübertragungszentrum gesendet werden,
   - **dass** das Wertübertragungszentrum die Daten entschlüsselt und erneut mit einem dem Kundensystem nicht bekannten Schlüssel verschlüsselt und die so verschlüsselten Daten anschließend an das Kundensystem überträgt,
   - **dass** in dem Kundensystem unter Einbeziehung der zwischengespeicherten Zufallszahl ein Hash-Wert gebildet wird, und
   - **dass** der Frankiervermerk die verschlüsselte Zufallszahl aus dem Wertübertragungszentrum sowie den Hash-Wert enthält.

2. Verfahren nach Anspruch 1,
   dadurch gekennzeichnet,
   dass die Zufallszahl zusammen mit einem von dem wertübertragungszentrum ausgegebenen Sitzungsschlüssel und einem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt wird.

3. Verfahren nach Anspruch 1 oder 2,
   dadurch gekennzeichnet,
   dass das Kundensystem die Daten mit einem privaten Schlüssel signiert.

4. Verfahren nach Anspruch 3,
   dadurch gekennzeichnet,
   dass der private Schlüssel in dem Sicherungsmodul gespeichert ist.

5. verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
   dadurch gekennzeichnet,
   dass die Daten mit jeder Anforderung eines Gebührenbetrages von dem Kundensystem an das Wertübertragungszentrum übertragen werden.

6. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,

dadurch gekennzeichnet,
dass das Wertübertragungszentrum anhand der übermittelten Daten das Kundensystem identifiziert.

7. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass das Wertübertragungszentrum die von ihm verschlüsselten Daten an das Kundensystem schickt.

8. Verfahren nach Anspruch 7,
dadurch gekennzeichnet,
dass die von dem Wertübertragungszentrum an das Kundensystem gesandten Daten einen ersten Bestandteil aufweisen, der von dem Kundensystem nicht entschlüsselt werden kann und dass die Daten ferner einen zweiten Anteil aufweisen, der von dem Kundensystem entschlüsselt werden kann.

9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet,
dass der in dem vom Kundensystem entschlüsselbare Teil der Daten Informationen über die Identität des Kundensystems enthält.

10. verfahren nach einem oder beiden der Ansprüche 8 und 9, **dadurch gekennzeichnet,**
dass der von dem Kundensystem entschlüsselbare Anteil der Daten Informationen über die Höhe eines Gebührenbetrages enthält.

11. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass bei jeder Datenübertragung von dem wertübertragungszentrum zu dem Kundensystem ein Betrag übertragen wird, der zur Erstellung von mehreren Freimachungsvermerken ausreicht.

12. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass der Hash-Wert unter Einbeziehung von Angaben über Sendungsdaten gebildet wird.

13. Verfahren nach einem oder beiden der Ansprüche 1 und 12,
dadurch gekennzeichnet,
dass der Hash-Wert unter Einbeziehung der Ladevorgangsidentifikationsnummer gebildet wird.

14. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass der Freimachungsvermerk Informationen über Sendungsdaten enthält.

15. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass der Freimachungsvermerk sowohl von dem Wertübertragungszentrum übertragene Informationen als auch von dem Dokumenthersteller eingegebene Daten enthält.

16. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass der Freimachungsvermerk einen Hash-Wert enthält, der aus einer Kombination aus einem von dem vorgabezentrum übertragenen Wert und von dem Dokumenthersteller eingegebenen Wert gebildet wird.

17. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass es folgende Verfahrensschritte beinhaltet: In dem Kundensystem oder in einem mit dem Kundensystem verbundenen Sicherungsmodul wird ein Geheimnis erzeugt und anschliessend zusammen mit Informationen über die Identität des Dokumentherstellers und/oder des von ihm eingesetzten Kundensystems an das wertübertragungszentrum übermittelt.

18. Verfahren nach Anspruch 17,
dadurch gekennzeichnet,

dass das Wertübertragungszentrum die verschlüsselte Zusatzzahl entschlüsselt und anschliessend eine Ladeidentifikationsnummer erzeugt.

19. Verfahren nach Anspruch 18,
dadurch gekennzeichnet,
dass bei der Erzeugung der Ladeidentifikationsnummer die entschlüsselte Zufallszahl eingeht.

20. Verfahren nach Anspruch 18 oder 19,
dadurch gekennzeichnet,
dass die Ladeidentifikationsnummer an das Sicherungsmodul übertragen wird.

21. Verfahren nach Anspruch 20,
dadurch gekennzeichnet,
dass in dem Sicherungsmodul ein Hash-Wert aus der Ladeidentifikationsnummer und weiteren Daten gebildet wird.

22. Verfahren nach Anspruch 20,
dadurch gekennzeichnet,
dass der Freimachungsvermerk so erzeugt wird, dass er den Hash-Wert enthält.

23. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass die Gültigkeit von Freimachungsvermerken in dem Briefzentrum überprüft wird.

24. Verfahren nach Anspruch 20,
dadurch gekennzeichnet,
dass die Prüfung in dem Briefzentrum durch eine Analyse von in dem Freimachungsvermerk enthaltenen Daten erfolgt.

25. Verfahren nach einem oder beiden der Ansprüche 23 und 24,
dadurch gekennzeichnet,
dass die Prüfungsstelle aus in dem Freimachungsvermerk enthaltenen Daten einen Hash-Wert bildet und überprüft, ob dieser Hash-Wert mit einem in dem Freimachungsvermerk enthaltenen Hash-Wert übereinstimmt und im Falle der Nichtübereinstimmung den Freimachungsvermerk als gefälscht registriert.

26. Kundensystem zur Frankierung von Postsendungen, enthaltend Mittel zum Verschlüsseln von Daten und ein Sicherungsmodul, auf das der Benutzer des Kundensystems keinen Zugriff hat,
dadurch gekennzeichnet, dass es einen Datenausgang für eine Ausgabe der verschlüsselten Daten an ein Wertübertragungszentrum enthält, wobei die Daten eine in dem Sicherheitsmodul erzeugte Zufallszahl umfassen,
dass es einen Dateneingang für einen Empfang von durch das Wertübertragungszentrum anders verschlüsselten Daten enthält, welche die Zufallszahl enthalten,
wobei das Sicherungsmodul so gestaltet ist, dass es die von dem Wertübertragungszentrum empfangenen anders verschlüsselten Daten nicht vollständig entschlüsseln kann, dass das Kundensystem dazu ausgestaltet ist, unter Einbeziehung der zwischengespeicherten Zufallszahl einen Hash-Wert zu bilden und
dass der Frankiervermerk die verschlüsselte Zufallszahl und aus dem Wertübertragungszentrum sowie den Hash-Wert enthält.

Claims

1. A method for providing mailpieces with postage indicia, whereby a customer system loads a monetary amount from a value transfer center via a data line, whereby the customer system controls the printing of postage indicia onto mailpieces, and whereby the value transfer center transmits a data packet to the customer system,
characterized in that

- a random number is generated and temporarily stored in a security module of the customer system to which the customer has no access,
- the data containing the random number is encrypted in the customer system in such a way that the value transfer center is able to decrypt it, and **in that** the data is transmitted by the customer system to the value

transfer center,
- the value transfer center decrypts the data and then re-encrypts it with a key that is not known to the customer system and subsequently transmits the data thus encrypted to the customer system,
- a hash value is formed in the customer system, with the inclusion of the temporarily stored random number, and
- the postage indicium contains the encrypted random number from the value transfer center as well as the hash value.

2. The method according to claim 1,
characterized in that
the random number is encrypted together with a session key issued by the value transfer center and with a public key of the value transfer center.

3. The method according to claim 1 or 2,
characterized in that
the customer system signs the data with a private key.

4. The method according to claim 3,
characterized in that
the private key is stored in the security module.

5. The method according to one or more of the preceding claims,
characterized in that
the data is transmitted from the customer system to the value transfer center at the time of each request for a monetary amount.

6. The method according to one or more of the preceding claims,
characterized in that
the value transfer center identifies the customer system on the basis of the transmitted data.

7. The method according to one or more of the preceding claims,
characterized in that
the value transfer center transmits the data it has encrypted to the customer system.

8. The method according to claim 7,
characterized in that
the data transmitted by the value transfer center to the customer system has a first component that cannot be decrypted by the customer system, and **in that** the data also has a second component that can be decrypted by the customer system.

9. The method according to claim 8,
characterized in that
the part of the data that can be decrypted by the customer system contains information about the identity of the customer system.

10. The method according to one or both of claims 8 and 9,
characterized in that
the part of the data that can be decrypted by the customer system contains information about the actual monetary amount.

11. The method according to one of the preceding claims,
characterized in that,
during each data transfer from the value transfer center to the customer system, an amount is transferred that is sufficient to create several postage indicia.

12. The method according to claim 1,
characterized in that
the hash value is formed with the inclusion of information about mailing data.

13. The method according to one or both of claims 1 and 12,
characterized in that
the hash value is formed with the inclusion of the loading procedure identification number.

14. The method according to claim 1,
characterized in that
the postage indicium contains information about mailing data.

15. The method according to one or more of the preceding claims,
characterized in that
the postage indicium contains information transmitted by the value transfer center as well as data entered by the document producer.

16. The method according to one or more of the preceding claims,
characterized in that
the postage indicium contains a hash value that is formed on the basis of a combination of a value transferred by the specification center and of a value entered by the document producer.

17. The method according to one or more of the preceding claims,
characterized in that
it comprises the following process steps: in the customer system or in a security module connected to the customer system, a secret is generated and subsequently transmitted to the value transfer center, together with information about the identity of the document producer and/or of the customer system he/she is using.

18. The method according to claim 17,
characterized in that
the value transfer center decrypts the encrypted random number and subsequently generates a loading identification number.

19. The method according to claim 18,
characterized in that
the encrypted random number enters into the generation of the loading identification number.

20. The method according to claim 18 or 19,
characterized in that
the loading identification number is transmitted to the security module.

21. The method according to claim 20,
characterized in that,
in the security module, a hash value is formed on the basis of the loading identification number and additional data.

22. The method according to claim 20,
characterized in that
the postage indicium is created in such a way as to contain the hash value.

23. The method according to one or more of the preceding claims,
characterized in that
the validity of postage indicia is verified in the mail center.

24. The method according to claim 20,
characterized in that
the verification in the mail center is performed by an analysis of data contained in the postage indicium.

25. The method according to one or both of claims 23 and 24,
characterized in that
the verification station forms a hash value on the basis of data contained in the postage indicium and checks whether this hash value matches a hash value contained in the postage indicium and, if it does not match, then the postage indicium is registered as being forged.

26. A customer system for franking mailpieces, comprising means for the encryption of data and a security module to which the user of the customer system has no access,
characterized in that
it comprises a data output in order to output the encrypted data to a value transfer center, whereby the data comprises a random number generated in the security module,
in that it comprises a data input for receiving data that has been differently encrypted by the value transfer center and that contains the random number, whereby the security module is configured in such a way that it cannot completely decrypt the differently encrypted data received from the value transfer center,
in that the customer system is configured to form a hash value with the inclusion of the temporarily stored random number, and
in that the postage indicium contains the encrypted random number from the value transfer center as well as the hash value.

Revendications

1. Procédé servant à pouvoir des envois postaux de marques d'affranchissement, un système client chargeant un montant de taxe depuis un centre de transmission de valeurs via une ligne de données, le système client commandant une impression de marques d'affranchissement sur des envois postaux et le centre de transmission de valeurs envoyant un paquet de données au système client, **caractérisé en ce que** :

- un nombre aléatoire est généré et stocké temporairement dans un module de sécurisation du système client auquel le client n'a pas accès ;
- des données contenant le nombre aléatoire sont cryptées de manière telle, dans le système client, que le centre de transmission de valeurs peut les décrypter, et **en ce que** les données sont envoyées par le système client au centre de transmission de valeurs ;
- le centre de transmission de valeurs décrypte les données et les crypte de nouveau avec une clé non connue du système client et transmet ensuite les données ainsi cryptées au système client ;
- une valeur de hachage est formée dans le système client compte tenu du nombre aléatoire stocké temporairement ; et
- la marque d'affranchissement contient le nombre aléatoire crypté issu du centre de transmission de valeurs ainsi que la valeur de hachage.

2. Procédé selon la revendication 1, **caractérisé en ce que** le nombre aléatoire est crypté conjointement avec une clé de session émise par le centre de transmission de valeurs et une clé publique du centre de transmission de valeurs.

3. Procédé selon la revendication 1 ou 2, **caractérisé en ce que** le système client signe les données avec une clé privée.

4. Procédé selon la revendication 3, **caractérisé en ce que** la clé privée est stockée dans le module de sécurisation.

5. Procédé selon l'une ou plusieurs des revendications précédentes, **caractérisé en ce que** les données sont transmises du système client au centre de transmission de valeurs à chaque demande de montant de taxe.

6. Procédé selon l'une ou plusieurs des revendications précédentes, **caractérisé en ce que** le centre de transmission de valeurs identifie le système client à l'aide des données transmises.

7. Procédé selon l'une ou plusieurs des revendications précédentes, **caractérisé en ce que** le centre de transmission de valeurs envoie au système client les données qu'il a cryptées.

8. Procédé selon la revendication 7, **caractérisé en ce que** les données envoyées par le centre de transmission de valeurs au système client comportent une première composante qui ne peut pas être décryptée par le système client et **en ce que** les données comportent en outre une deuxième partie qui peut être décryptée par le système client.

9. Procédé selon la revendication 8, **caractérisé en ce que** la partie des données qui peut être décryptée par le système client contient des informations sur l'identité du système client.

10. Procédé selon l'une ou les deux revendications 8 et 9, **caractérisé en ce que** la partie des données qui peut être décryptée par le système client contient des informations sur la hauteur d'un montant de taxe.

11. Procédé selon l'une ou plusieurs des revendications précédentes, **caractérisé en ce qu'**est transmis du centre de transmission de valeurs au système client, à chaque transmission de données, un montant qui suffit pour créer plusieurs marques d'affranchissement.

12. Procédé selon la revendication 1, **caractérisé en ce que** la valeur de hachage est formée compte tenu d'indications relatives à des données d'envoi.

13. Procédé selon l'une ou les deux revendications 1 et 12, **caractérisé en ce que** la valeur de hachage est formée compte tenu du numéro d'identification de l'opération de chargement.

14. Procédé selon la revendication 1, **caractérisé en ce que** la marque d'affranchissement contient des informations sur des données d'envoi.

15. Procédé selon l'une ou plusieurs des revendications précédentes, **caractérisé en ce que** la marque d'affranchissement contient non seulement des informations transmises par le centre de transmission de valeurs, mais aussi des données introduites par le producteur de document.

16. Procédé selon l'une ou plusieurs des revendications précédentes, **caractérisé en ce que** la marque d'affranchissement contient une valeur de hachage qui est formée à partir d'une combinaison d'une valeur transmise par le centre de spécification et d'une valeur introduite par le producteur de document.

17. Procédé selon l'une ou plusieurs des revendications précédentes, **caractérisé en ce qu'**il comporte les étapes suivantes : un secret est généré dans le système client ou dans un module de sécurisation relié au système client et est ensuite transmis au centre de transmission de valeurs conjointement avec des informations sur l'identité du producteur de document et/ou du système client que celui-ci utilise.

18. Procédé selon la revendication 17, **caractérisé en ce que** le centre de transmission de valeurs décrypte le nombre aléatoire crypté, puis génère un numéro d'identification de chargement.

19. Procédé selon la revendication 18, **caractérisé en ce que** le nombre aléatoire décrypté intervient lors de la génération du numéro d'identification de chargement.

20. Procédé selon la revendication 18 ou 19, **caractérisé en ce que** le numéro d'identification de chargement est transmis au module de sécurisation.

21. Procédé selon la revendication 20, **caractérisé en ce qu'**est formée, dans le module de sécurisation, une valeur de hachage à partir du numéro d'identification de chargement et d'autres données.

22. Procédé selon la revendication 20, **caractérisé en ce que** la marque d'affranchissement est générée de manière telle qu'elle contient la valeur de hachage.

23. Procédé selon l'une ou plusieurs des revendications précédentes, **caractérisé en ce que** la validité de marques d'affranchissement est vérifiée dans le centre postal.

24. Procédé selon la revendication 20, **caractérisé en ce que** le contrôle s'effectue dans le centre postal par une analyse de données contenues dans la marque d'affranchissement.

25. Procédé selon l'une ou les deux revendications 23 et 24, **caractérisé en ce que** l'entité de contrôle forme une valeur de hachage à partir de données contenues dans la marque d'affranchissement et vérifie si cette valeur de hachage coïncide avec une valeur de hachage contenue dans la marque d'affranchissement et, en cas de non-coïncidence, enregistre la marque d'affranchissement comme étant falsifiée.

26. Système client pour affranchir des envois postaux, contenant des moyens pour crypter des données et un module de sécurisation auquel l'utilisateur du système client n'a pas accès, **caractérisé en ce qu'**il comporte une sortie de données pour envoyer les données cryptées à un centre de transmission de valeurs, les données comprenant un nombre aléatoire généré dans le module de sécurisation, **en ce qu'**il comporte une entrée de données pour recevoir des données cryptée différemment par le centre de transmission de valeurs, lesquelles contiennent le nombre aléatoire, le module de sécurisation étant configuré de manière telle qu'il ne peut pas décrypter entièrement les

données cryptées différemment par le centre de transmission de valeurs, **en ce que** le système client est configuré pour former une valeur de hachage compte tenu du nombre aléatoire stocké temporairement et **en ce que** la marque d'affranchissement contient le nombre aléatoire crypté issu du centre de transmission de valeurs ainsi que la valeur de hachage.

FIG 1

Der prinzipielle Kreislauf der PC-Frankierung PC-Frankierung

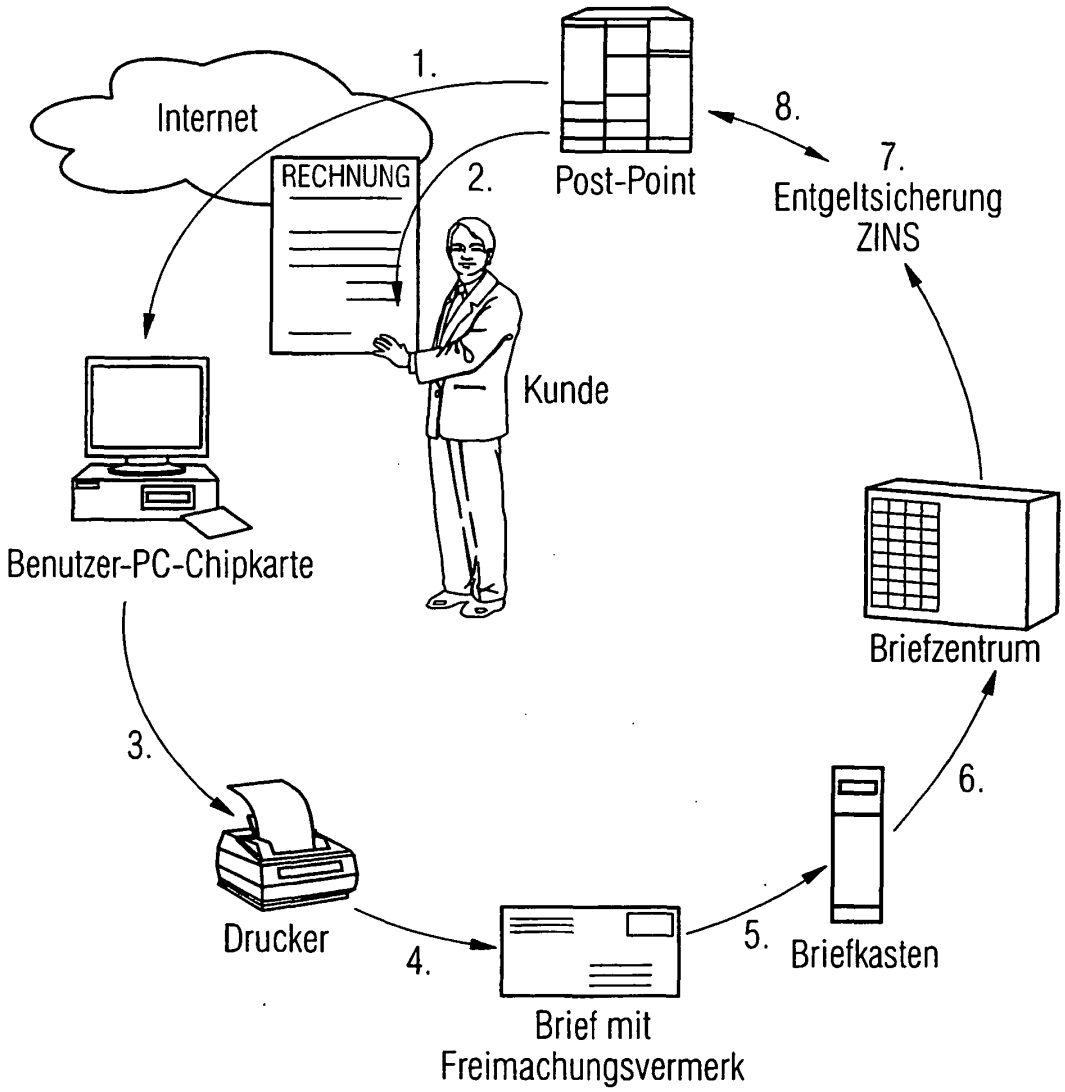


FIG 2

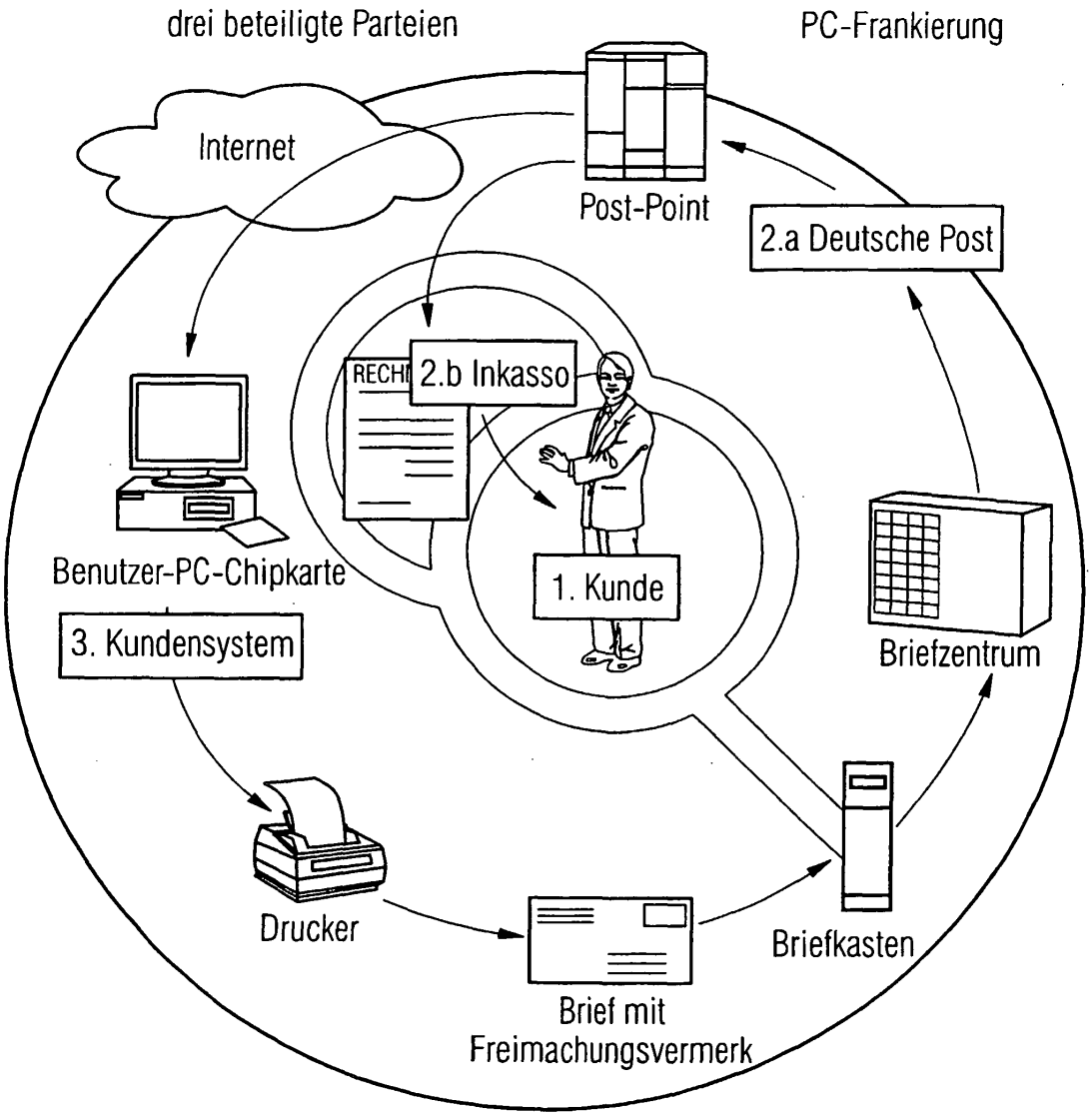

drei beteiligte Parteien
PC-Frankierung
Internet
Post-Point
2.a Deutsche Post
RECHN
2.b Inkasso
Benutzer-PC-Chipkarte
1. Kunde
3. Kundensystem
Briefzentrum
Drucker
Briefkasten
Brief mit
Freimachungsvermerk

FIG 3

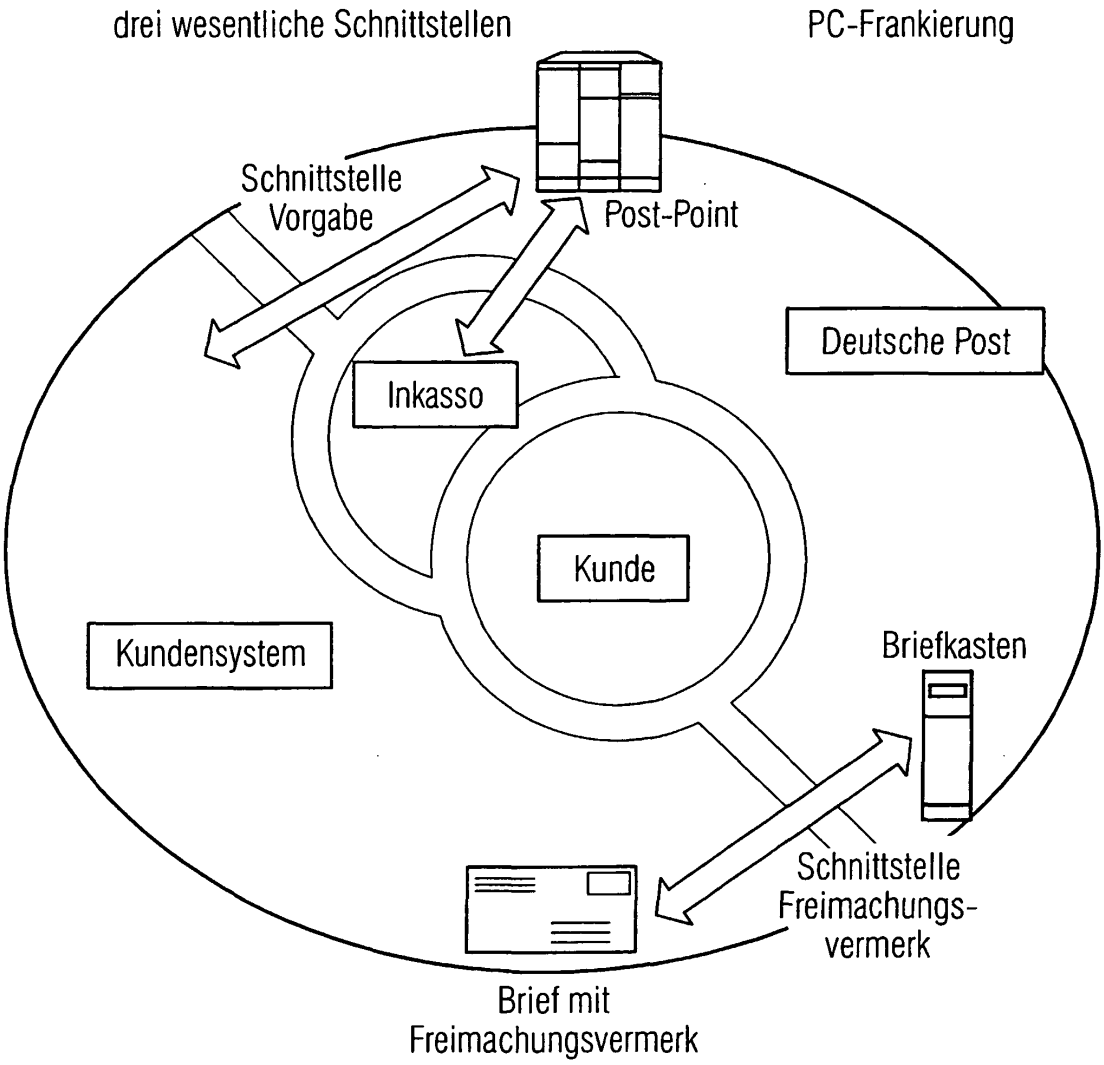
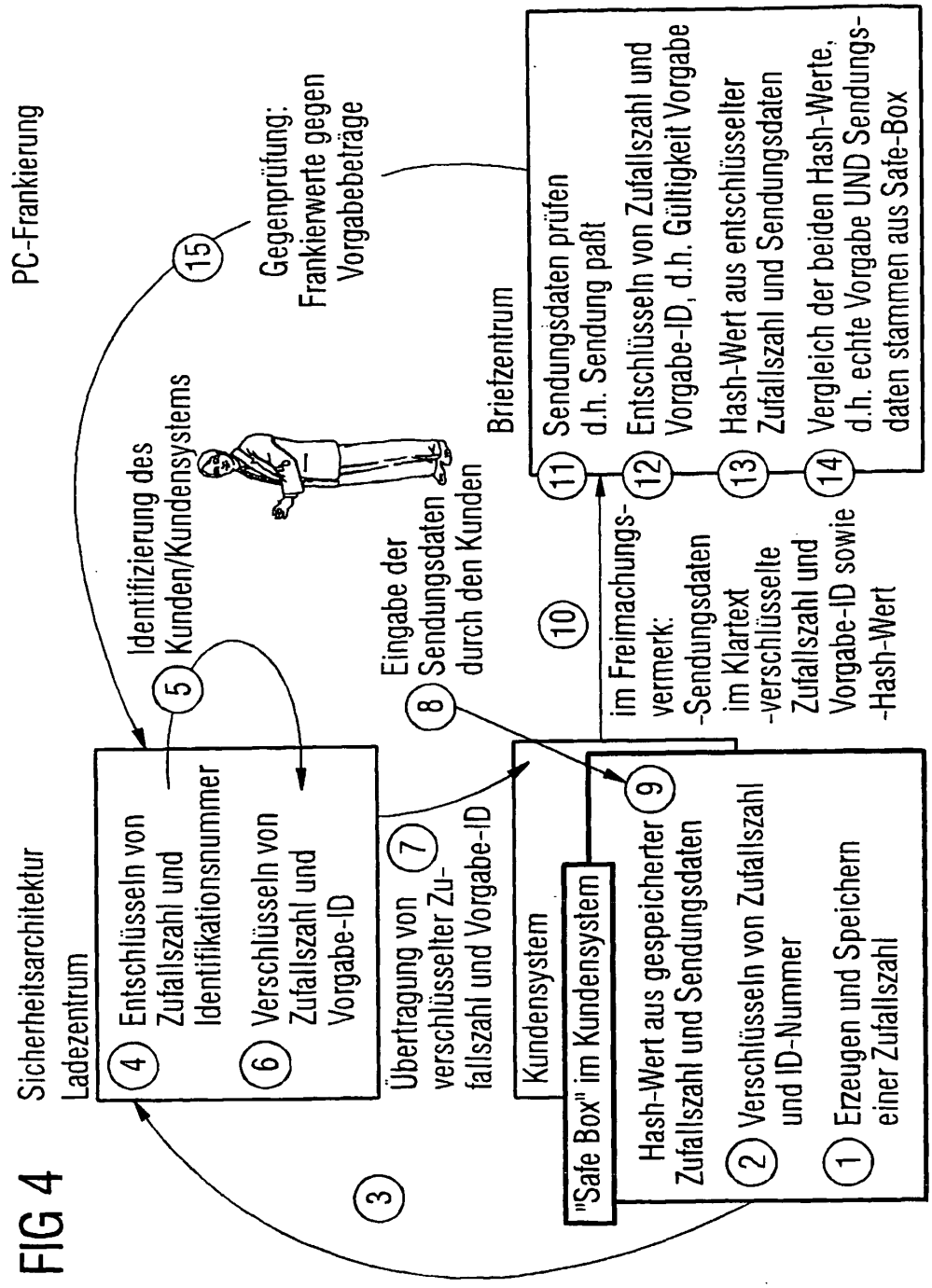

drei wesentliche Schnittstellen
PC-Frankierung
Schnittstelle
Vorgabe
Post-Point
Deutsche Post
Inkasso
Kunde
Kundensystem
Briefkasten
Schnittstelle
Freimachungs-
vermerk
Brief mit
Freimachungsvermerk

FIG 4


PC-Frankierung
Sicherheitsarchitektur
Ladezentrum
Briefzentrum
Kundensystem
"Safe Box" im Kundensystem
1 Erzeugen und Speichern einer Zufallszahl
2 Verschlüsseln von Zufallszahl und ID-Nummer
3
4 Entschlüsseln von Zufallszahl und Identifikationsnummer
5 Identifizierung des Kunden/Kundensystems
6 Verschlüsseln von Zufallszahl und Vorgabe-ID
7 Übertragung von verschlüsselter Zufallszahl und Vorgabe-ID
8 Eingabe der Sendungsdaten durch den Kunden
9 Hash-Wert aus gespeicherter Zufallszahl und Sendungsdaten
10 im Freimachungsvermerk:
-Sendungsdaten im Klartext
-verschlüsselte Zufallszahl und Vorgabe-ID sowie -Hash-Wert
11 Sendungsdaten prüfen d.h. Sendung paßt
12 Entschlüsseln von Zufallszahl und Vorgabe-ID, d.h. Gültigkeit Vorgabe
13 Hash-Wert aus entschlüsselter Zufallszahl und Sendungsdaten
14 Vergleich der beiden Hash-Werte, d.h. echte Vorgabe UND Sendungsdaten stammen aus Safe-Box
15 Gegenprüfung: Frankierwerte gegen Vorgabebeträge

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

- WO 9814907 A **[0002]**
- DE 3126785 C2 **[0003]**
- WO 9948053 A **[0004]**