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

(11) **EP 2 131 330 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
09.12.2009 Patentblatt 2009/50

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

(21) Anmeldenummer: **09005922.1**

(22) Anmeldetag: **29.04.2009**

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

(30) Priorität: **02.06.2008 DE 102008026273**

(71) Anmelder: **Deutsche Post AG**
53113 Bonn (DE)

(72) Erfinder: **Rakow, Matthias**
12205 Berlin (DE)

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

(54) Einlieferungsstation für Postsendungen und Verfahren zum Einliefern von Postsendungen

(57) Die Erfindung betrifft eine Einlieferungsstation (10) zum Einliefern und Frankieren von Postsendungen (20), die wenigstens eine Waage (30) zur Bestimmung des Gewichts einer Postsendung (20), wenigstens ein Dimensionsmessgerät (40) zur Bestimmung der Abmessungen einer Postsendung (20), eine Recheneinheit (50) zur Bestimmung des Portoentgelts für eine Postsendung (20) und eine Frankiereinheit (60) zur Aufbringung eines Frankiervermerks auf die Postsendung (20) umfasst, wobei die Recheneinheit (50) Zugriff auf Messtoleranzen der Waage (30) und des Dimensionsmessgerätes (40) hat.

Die Einlieferungsstation zeichnet sich dadurch aus, dass die Einlieferungsstation (10) ein Messmodul (52) mit einem Mittel zum Empfangen von Messwerten von der Waage (30) und/oder dem Dimensionsmessgerät (40) aufweist und dass das Messmodul (52) und/oder eine Komponente des Messmoduls (52) mit einer TPM-Einheit verbindbar ist.

Die Erfindung betrifft ferner ein Verfahren zum Einliefern und frankieren von Postsendungen.

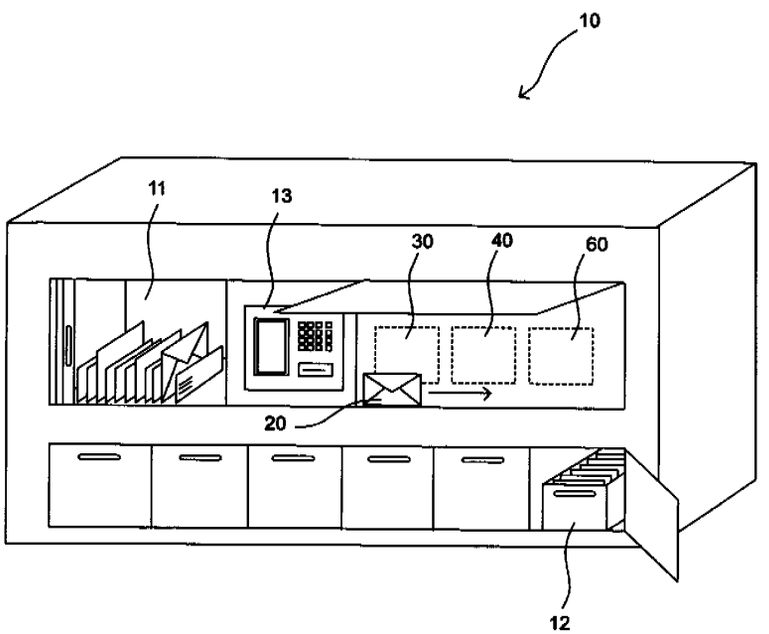

Fig. 11

EP 2 131 330 A1

Beschreibung

[0001] Die Erfindung betrifft eine Einlieferungsstation für Postsendungen und ein Verfahren zum Einliefern von Postsendungen.

[0002] Insbesondere betrifft die Erfindung eine Einlieferungsstation, beziehungsweise ein Verfahren, bei dem Postsendungen frankiert werden.

[0003] Neben der Aufbringung von Postwertzeichen wie Briefmarken ist es auf dem Gebiet der Freimachung von Postsendungen bekannt, Frankiermaschinen einzusetzen, welche von einem Nutzer dazu verwendet werden können, größere Mengen von Postsendungen mit einem Freimachungsvermerk zu versehen. Die Anschaffung einer Frankiermaschine wird jedoch insbesondere von Kunden mit geringem oder unregelmäßigem Aufkommen an zu frankierenden Postsendungen oftmals vermieden.

[0004] Kunden können ferner eine größere Menge von unfrankierten Postsendungen in einer Filiale eines Transport- und Zustelldienstes abgeben. Das Zustelluntemehmen führt eine Frankierung der Sendungen durch, wobei ebenfalls Frankiermaschinen zum Einsatz kommen können. Dabei sind die Kunden jedoch für die Einlieferung von Sendungen an festgelegte Öffnungszeiten von Filialen des Zustellunternehmens gebunden.

[0005] Im postalischen Bereich besteht daher der Bedarf nach einer Einlieferungsstation für Postsendungen, in welche Kunden größere Mengen unfrankierter Postsendungen einliefern können, wobei die Vorrichtung die Sendungen automatisch frankiert. Die Vorrichtung könnte in öffentlichen Bereichen aufgestellt werden, um Kunden einen 24-Stundenbetrieb zu gewährleisten. Dabei setzt eine derartige Vorrichtung ein Verfahren zur automatischen Ermittlung eines für eine Sendung erforderlichen Portobetrages bzw. Portoentgelts voraus.

[0006] Eine solche Einlieferungsstation für Briefsendungen ist beispielsweise aus der deutschen Offenlegungsschrift DE 10 2005 006 005 A1 bekannt. Die Druckschrift offenbart eine Einlieferungsstation für Postsendungen, bei der eine Postsendung von einem Annahmemittel in ein für einen Kunden unzugängliches Gehäuse überführt wird. Innerhalb des Gehäuses werden durch Messeinrichtungen Messwerte für Gewicht, Länge, Breite und Höhe der Postsendung ermittelt. Zu den so ermittelten Messwerten werden die Negativtoleranzen der einzelnen Messeinrichtungen addiert und die Beträge der Positivtoleranzen subtrahiert, um angepasste Messwerte zu erhalten. Diese angepassten Messwerte werden mit Wertebereichen einer Referenzliste verglichen, wobei die Referenzliste Wertebereichen der angepassten Messwerte verschiedene Portobeträge zuordnet und eine Ergebnisliste mit den Portobeträgen erzeugt wird, die den ermittelten angepassten Messwerten zugeordnet sind. Der kleinste Portobetrag der Ergebnisliste wird ermittelt und als erforderliches Portoentgelt für die betreffende Postsendung festgelegt. Daraufhin wird ein Freimachungsvermerk auf die Postsendung aufgebracht, wobei der Freimachungsvermerk den ermittelten Portobetrag enthält. Durch diese Vorgehensweise wird sichergestellt, dass ein Kunde nie einen zu hohen Portobetrag entrichten muss. Dies ist eine wesentliche Voraussetzung für die Zulassung einer solchen Einlieferungsstation, wenn diese öffentlich aufgestellt wird.

[0007] Für Messgeräte wie beispielsweise Waagen, Tankzapfsäulen und auch Einlieferungsstationen zum Frankieren von Postsendungen besteht die Notwendigkeit, diese gemäß nationaler Eichgesetze eichen zu lassen, um eichpflichtige Messungen damit durchführen zu können. Die Eichung setzt in den meisten Fällen eine Bauartzulassung voraus, das heißt, ein typisches Exemplar des betreffenden Messgerätes muss von der zuständigen Behörde zugelassen werden. In der Bundesrepublik Deutschland ist die dafür zuständige Behörde beispielsweise die Physikalisch Technische Bundesanstalt (PTB).

[0008] Die Behörde prüft üblicherweise die Zulassungsunterlagen und ein Mustergerät nach den Vorschriften der jeweiligen Eichordnung. Wesentliche Aspekte sind hierbei die Messrichtigkeit und Messbeständigkeit. Es müssen insbesondere die geltenden Anforderungen und Fehlergrenzen eingehalten werden. Die Zulassungsprüfung beinhaltet messtechnische, technische und administrative Prüfungen. Bei den technischen Prüfungen, zu denen auch Softwareprüfungen gehören, wird untersucht, ob die Bedien-, Anzeige- und Abdruckfunktionen den Anforderungen genügen und das Gerät ausreichend gegen Bedienungsfehler und Manipulationen geschützt ist. Da Einlieferungsstationen zum Frankieren von Postsendungen üblicherweise computergesteuert sind, ist somit auch eine Zulassung und Eichung von Softwarekomponenten erforderlich.

[0009] War die Zulassungsprüfung erfolgreich, erhält der Antragsteller von der zuständigen Behörde einen Zulassungsschein und ein Zulassungszeichen, das auf allen Messgeräten an sichtbarer Stelle aufgebracht werden muss. Hat die Geräte-Bauart eine Zulassung erhalten, so muss anschließend jedes einzelne Gerät von der zuständigen Eichbehörde geeicht werden, bevor es beispielsweise im geschäftlichen Verkehr eingesetzt werden darf.

[0010] Insbesondere im Bereich der Prüfung und Eichung von Software liegen ferner Empfehlungen der WELMEC (Western European Legal Metrology Cooperation) vor, bei der es sich um eine europäische Zusammenarbeit im gesetzlichen Messwesen handelt. Als gesetzliches Messwesen wird die Gesamtheit der technischen und administrativen Verfahren bezeichnet, die von den öffentlichen Behörden rechtlich verbindlich festgelegt wurden, um die Qualität der im Rahmen gewerblicher Geschäfte und amtlicher Kontrollen bzw. in den Bereichen Gesundheitsfürsorge, Sicherheit usw. vorgenommenen Messungen zu garantieren. Dabei werden Empfehlungen für die Ausführung von eichpflichtiger Software und die Verarbeitung eichpflichtiger Messwerte und Parameter angegeben.

[0011] Soll eine Einlieferungsstation zur Einlieferung und Frankierung von Postsendungen geeicht werden, besteht die Möglichkeit, alle Komponenten der Anlage und die Software in ihrer Gesamtheit prüfen und eichen zu lassen. Dies hat jedoch den Nachteil, dass Änderungen an der Vorrichtung und/oder der Software mit einer erneuten Prüfung durch eine Zulassungsbehörde verbunden sind. Eine Veränderung des der Software zugrunde liegenden Betriebssystems oder sonstiger nicht eichrelevanter Parameter kann daher in diesem Fall nicht von einem Administrator durchgeführt werden. Da eine Einlieferungsstation Komponenten im Hardware- und Softwarebereich umfassen kann, die nicht eichpflichtig sind, besteht jedoch die Möglichkeit, eichpflichtige von nicht-eichpflichtigen Komponenten zu trennen. Dadurch können die nicht-eichpflichtigen Komponenten frei verändert werden, ohne dass eine erneute Zulassung oder Eichung der gesamten Anordnung erforderlich ist. Das deutsche Gebrauchsmuster DE 296 13 903 U1 offenbart dazu beispielsweise eine Anordnung zur Qualitätssicherung komplexer elektronischer Messeinrichtungen, die sowohl eichpflichtige als auch nicht-eichpflichtige Komponenten aufweisen.

[0012] Ferner sind aus der deutschen Offenlegungsschrift DE 195 27 293 A1 ein Verfahren und eine Vorrichtung zur sicheren Messung und Verarbeitung von Messdaten im Bereich der Abgasuntersuchung bekannt. Damit ein Computer, der an ein Messmodul angeschlossen ist, nicht zusammen mit dem Messmodul geeicht werden muss, was zu einer Einschränkung des zunächst offenen PC-Systems führen würde, schlägt die Druckschrift vor, dass Messwerte über eine geeignete Schnittstelle zu einem PC übertragen werden. Der PC muss dabei nicht geeicht werden, sondern kann auch für andere Anwendungen zur freien Verfügung stehen.

[0013] Es ist wünschenswert, eine Einlieferungsstation für Postsendungen bereitzustellen, die flexibel eingesetzt werden kann.

[0014] Erfindungsgemäß wird diese Aufgabe durch eine Einlieferungsstation mit den Merkmalen des unabhängigen Anspruches 1 gelöst. Vorteilhafte Weiterbildungen der Einlieferungsstation ergeben sich aus den Unteransprüchen 2 bis 9. Die Aufgabe wird ferner durch ein Verfahren nach Anspruch 10 gelöst. Vorteilhafte Ausführungsformen des Verfahrens ergeben sich aus den Unteransprüchen 11 bis 13.

[0015] Die Erfindung beinhaltet eine Einlieferungsstation zum Frankieren von Postsendungen, die wenigstens eine Waage zur Bestimmung des Gewichts einer Postsendung, wenigstens ein Dimensionsmessgerät zur Bestimmung der Abmessungen einer Postsendung, eine Recheneinheit zur Bestimmung des Portoentgelts für eine Postsendung und eine Frankiereinheit zur Aufbringung eines Frankiervermerks auf die Postsendung umfasst, wobei die Recheneinheit Zugriff auf Messtoleranzen der Waage und des Dimensionsmessgerätes hat.

[0016] Erfindungsgemäß wird diese Einlieferungsstation so ausgestaltet, dass sie ein Messmodul mit einem Mittel zum Empfangen von Messwerten von der Waage und/oder dem Dimensionsmessgerät aufweist und dass das Messmodul und/oder eine Komponente des Messmoduls mit einer TPM-Einheit verbindbar ist.

[0017] Die Erfindung beinhaltet eine TPM-Einheit zum Kalibrieren und/oder Eichen von Software.

[0018] Bei der TPM-Einheit handelt es sich beispielsweise um ein Modul, das sicherstellt, dass nur zugelassene Software/Hardware versendet werden kann.

[0019] In einer besonders bevorzugten Ausführungsform der Erfindung handelt es sich bei der TPM-Einheit um derartiges Modul, das in der vorliegenden Anmeldung auch als TPM (Trusted Platform Module) bezeichnet wird.

[0020] Das Merkmal "Trusted" beinhaltet mehrere Bedeutungen und umfasst insbesondere einen englischen Begriff, der besagt, dass sichergestellt und/oder vorausgesetzt wird, dass ein entsprechend ausgestattetes Modul sich entsprechend vorgebbarer Merkmale verhält.

[0021] Beispielsweise bedeutet dies bei einer Waage, dass sichergestellt wird, auf welche Weise Messwerte ermittelt werden und dass auch eine sichere, nicht abänderbare Übermittlung der Messwerte sicher gestellt wird.

[0022] Eine entsprechende Sicherheit wird auch bei den anderen mit einer TPM-Einheit ausgestatteten Bestandteilen der Einlieferungsstation, insbesondere einzelner, mehrerer oder sämtlicher für eine Frankierung relevanten Modulen bzw. Komponenten, beispielsweise einer Größenmesseinrichtung gewährleistet.

[0023] Die Waage und/oder die Größenmesseinrichtung sind besonders bevorzugte Module, bei denen ein Kalibrieren und/oder Eichen mittels einer TPM-Einheit erfolgt.

[0024] Durch die TPM-Einheit wird sichergestellt, dass nur genehmigte, vorzugsweise geeichte Software in dem System verwendet wird.

[0025] Durch eine hierzu berechtigte Instanz erfolgt eine Eichung der Software. Das Ergebnis der Eichung wird protokolliert und dokumentiert. Die Ergebnisse der Protokollierung werden in einem elektronischen Speicher vermerkt und sind somit jederzeit abrufbar.

[0026] Die Eichung der Software ist Grundlage für eine Genehmigung für den Einsatz der Software.

[0027] Genehmigte Software kann für einen Einsatz in dem erfindungsgemäßen System zugelassen werden.

[0028] Durch eine Überprüfungseinheit wird sichergestellt, dass nur die zugelassene, das heißt genehmigte und/oder geeichte Software in dem Einlieferungssystem eingesetzt wird.

[0029] Ferner existieren Überprüfungseinheiten der Echtheit von in den Modulen eingesetzten TPM-Einheiten.

[0030] Mit der TPM-Einheit kann sichergestellt werden, dass nur die genehmigte ("geeichte") Software in einem System verwendet wird.

[0031] Die TPM-Einheit könnte dabei verhindern, dass nicht-geeichte Software verwendet werden kann.

[0032] Zweckmäßigerweise erfolgt eine möglichst regelmäßige Prüfung des Systems. Hierbei wird insbesondere die Funktionsfähigkeit der Überprüfungskomponenten geprüft. Hiermit wird sichergestellt, dass Überprüfungskomponenten eingesetzt werden, die ausschließlich einen Einsatz von zuvor genehmigter und/oder geeichter Software sicherstellen.

[0033] Zum Ändern von Einstellungen der TPM-Einheit, z. B. um neue Software freizugeben, kann ein autorisierter Nutzer auf die TPM-Einheit zugreifen.

[0034] Weiterbildungen der Erfindung zeichnen sich dadurch aus, dass eine Schnittstelle für ein Zusammenwirken zwischen geeichter und ungeeichter Software vorgesehen ist.

[0035] Die Schnittstelle ist so beschaffen, dass Veränderungen der geeichten Software durch geeignete Zugriffsrechte/Managementsysteme nur durch besonders autorisierte Benutzer erfolgen kann.

[0036] Änderungen der mit der geeichten Software zusammenwirkenden ungeeichten Software sind hiervon unabhängig vornehmbar.

[0037] Dies hat den Vorteil, dass Updates, beispielsweise Service-Updates zur Integration neuer Funktionen der Einlieferungsstation, vorzugsweise für das Erstellen von Benachrichtigungen oder die Dokumentation von Einschreiben variabel geändert werden können, während eine Integrität und Authentizität der gesicherten geeichten Software weiterhin sichergestellt wird.

[0038] In einer Weiterbildung der Erfindung werden bestimmte Funktionen der geeichten TPM-Module, insbesondere von TPM-Software -Modulen und andere Funktionen von "freier" (gleich ungeeichter) Software durchgeführt.

[0039] Die freie Software ist beliebig änderbar, so dass beispielsweise Masken für nichteichrelevante Aufgaben ohne neue Eichung des Gesamtsystems angepasst werden können.

[0040] Eichrelevante Funktionen des Systems, insbesondere Funktionen, die eine Überprüfung von für eine Entgeltabrechnung relevanten Parameter wie Sendungsgröße und/oder Sendungsgewicht beinhalten, werden von geeichten Software-Modulen durchgeführt.

[0041] Die Einlieferungsstation enthält wenigstens eine Überprüfungseinheit zur Überprüfung der Echtheit der geeichten Software-Module. Zweckmäßigerweise wird von dieser Überprüfungsseinheit überprüft, ob das Software-Modul mit einer elektronischen Bestätigung eines Eichvermerks (elektronischer Eichvermerk) versehen ist.

[0042] Gemäß einer Weiterbildung der Erfindung werden die geeichten Software-Module in ein Framework eingebettet. Das Framework enthält vorgebbare Anforderungen für einen Einsatz von Software-Modulen einschließlich Informationen über Funktionen, die ausschließlich von den geeichten Software-Modulen vorgenommen werden dürfen, beispielsweise alle Prozesse, welche eine Entgeltabrechnung der Postsendungen ermöglichen beziehungsweise zumindest unterstützen.

[0043] Es ist besonders vorteilhaft, das Messmodul und/oder einzelne, mehrere oder sämtliche seiner Komponenten so auszugestalten, dass sie eine Signatur erzeugen können.

[0044] In einer bevorzugten Ausführungsform der Erfindung handelt es sich bei der TPM-Einheit um eine miniaturisierte elektronische Schaltung - nachfolgend vereinfachend als "Chip" bezeichnet.

[0045] Insbesondere ist es vorteilhaft, die TPM-Einheit in ein System - insbesondere das Einlieferungssystem - einzubinden, wobei eine feste Einbindung hierbei im Kontext der Erfindung auch als Framework bezeichnet wird.

[0046] Gemäß einer Weiterbildung der Erfindung ist der Chip passiv, das heißt, er ist so gestaltet, dass er weder den Bootvorgang noch den Betrieb des Systems beeinflussen kann.

[0047] Dies hat den Vorteil, dass ein erhöhter Schutz vor Manipulationen gewährleistet wird.

[0048] Es ist jedoch alternativ gleichfalls möglich, dass der Chip aktiv ist und den Bootvorgang und/oder den Betrieb des Systems direkt beeinflussen kann.

[0049] Eine bevorzugte Weiterbildung der Erfindung sieht vor, dass die TPM-Einheit eine eindeutige Kennung enthält und ihre Identifizierung ermöglicht.

[0050] Zusätzlich ist es möglich, dass ein System, das eine Komponente oder ein Modul, das die TMP-Einheit enthält, durch die eindeutige Kennung der TPM-Einheit identifiziert wird.

[0051] Durch die TPM-Einheit können mehrfache Funktionen realisiert werden.

[0052] Insbesondere ist es möglich, eine Versiegelung (sealing) vorzunehmen.

[0053] Eine derartige Versiegelung stellt eine zweckmäßige Weiterentwicklung der Erfindung dar. Es ist besonders vorteilhaft, dass die TPM-Einheit die Versiegelung unter Einsatz eines Hash-Wertes durchführt.

[0054] Durch das Bilden des Hash-Wertes aus der System-Konfiguration (Hard- und Software) können Daten an eine eindeutig identifizierbare TPM-Einheit verknüpft werden. Hierbei erfolgt eine Verschlüsselung mittels des Hash-Wertes.

[0055] Bei einer Weiterbildung der Erfindung erfolgt die Verschlüsselung so, dass eine Entschlüsselung nur dann gelingt, wenn der gleiche Hash-Wert wieder ermittelt wird. Eine Sicherheitsüberprüfung erfolgt dadurch, dass die Hash-Werte verglichen werden. Nur diejenigen Hash-Werte, die vollständig übereinstimmen, zeigen an, dass das System (insbesondere das Einlieferungssystem) unverändert blieb.

[0056] Eine Weiterbildung der Erfindung beinhaltet auch einen Schutz eines oder mehrerer kryptographischer Schlüssel.

[0057] Kryptographische Schlüssel werden vorzugsweise innerhalb der TPM-Einheit erzeugt, benutzt und sicher abgelegt. Dies erhöht den Schutz gegen externe Attacken, und zwar sowohl gegen softwarebezogene Angriffe als auch gegen hardwarebezogene Angriffe.

[0058] Zur weiteren Erhöhung des Schutzes vor hardwarebezogenen Angriffen ist es zweckmäßig, die TPM-Einheiten so herzustellen, dass die in ihnen enthaltenen Daten bei einer äußeren Einwirkung - insbesondere einer mechanischen Einwirkung - gelöscht werden.

[0059] Es ist besonders vorteilhaft, unter Einbeziehung der Einlieferungsstation erzeugte Frankiervermerke zu beglaubigen.

[0060] Die Integration einer Beglaubigungsfunktion in die TPM-Einheit beziehungsweise in mehrere der TPM-Einheiten ermöglicht einen zuverlässigen Nachweis der Echtheit von entgeltrelevanten Messwerten und/oder Frankiervermerken, die im Bereich der Einlieferungsstation erzeugt wurden.

[0061] Ferner ist es möglich, die Funktionsfähigkeit und/oder Echtheit der Einlieferungsstation beziehungsweise der in ihr enthaltenen Komponenten durch die vorgenommene Beglaubigung nachzuweisen.

[0062] Eine Weiterentwicklung der Erfindung beinhaltet, dass der kryptographische Schlüssel ein privater Schlüssel eines asymetrischen Verschlüsselungssystems ist und dass die Signatur mit diesem privaten Schlüssel erzeugt wird, wobei der private Schlüssel selbst durch die TPM-Einheit erzeugbar ist.

[0063] Insbesondere ist es vorteilhaft, dass der private Schlüssel in der TPM-Einheit, insbesondere in einem TPM-Chip integriert ist.

[0064] Hierbei ist es ferner vorteilhaft, dass die TPM-Einheit, insbesondere der TPM-Chip, fest in die Recheneinheit eingebaut ist.

[0065] Eine Weiterentwicklung der Erfindung beinhaltet, dass ein Zugriff auf den privaten Schlüssel in die TPM-Einheit durch ein Passwort geschützt ist.

[0066] Weitere Vorteile, Besonderheiten und zweckmäßige Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Darstellung bevorzugter Ausführungsbeispiele anhand der Abbildungen.

Von den Abbildungen zeigt:

[0067]

Fig. 1 eine Architekturübersicht eines erfindungsgemäßen Systems;

Fig. 2 Verfahrensschritte für eine Erstinitialisierung eines erfingungsgemäßen Systems;

Fig. 3 bevorzugte Verfahrensschritte zur Anforderung und/oder Übernahme von Sicherheitsdaten;

Fig. 4 eine Prüfung einer Gültigkeit von Sicherheitsinformationen

Fig. 5 Verfahrensschritte zur Erzeugung eines auf eine Postsendung aufbringbaren Matrixcodes;

Fig. 6 Verfahrensschritte zu einer Überprüfung von Authentifizierungsdaten

Fig. 7 Verfahrensschritte zum Schließen eines Crypto-Stores;

Fig. 8 eine erfindungsgemäße Schlüsselhierarchie;

Fig. 9 eine Prinzipdarstellung eines erfindungsgemäßen TCG Software-Stacks;

Fig. 10 ein bevorzugter Aufbau einer erfindungsgemäßen TPM-Einheit und

Fig. 11 ein Ausführungsbeispiel einer erfindungsgemäßen Einlieferungsstation.

[0068] Die Erfindung beinhaltet eine Einlieferungsstation zum Frankieren von Postsendungen, die wenigstens eine Waage zur Bestimmung des Gewichts einer Postsendung und wenigstens ein Dimensionsmessgerät zur Bestimmung der Abmessungen einer Postsendung aufweist. Ferner ist eine Recheneinheit zur Bestimmung des Portoentgelts für eine Postsendung und eine Frankiereinheit zur Aufbringung eines Frankiervermerks auf die Postsendung vorgesehen. Die Recheneinheit hat dabei Zugriff auf Messtoleranzen der Waage und des Dimensionsmessgerätes.

[0069] Erfindungsgemäß wird ein System zur Einlieferung und/oder sonstigen Bearbeitung von Postsendungen bereitgestellt, das an verschiedene Anforderungen angepasst werden kann.

[0070] Es ist möglich, erfindungsgemäße Einlieferungsstationen auf vielfältige Weise auszuführen.

[0071] Insbesondere handelt es sich bei der Einlieferungsstation um einen Selbstbedienungsautomaten, an dem Kunden Postsendungen wie Brief- oder Paketsendungen anliefern können.

[0072] Vorzugsweise ist der Selbstbedienungsautomat so ausgestaltbar, dass eine Einbeziehung sowohl von registrierten Kunden als auch von nicht registrierten Kunden möglich ist.

[0073] Bei einer Ausgestaltung der Einlieferungsstation für eine Bearbeitung von Postsendungen registrierter Kunden ist es zweckmäßig, dass die Kunden sich auf geeignete Weise - beispielsweise über eine Kundenkarte - identifizieren, so dass die durch die Einlieferungsstation erbrachten Leistungen auf einfache Weise bei dem Kunden abgerechnet werden können.

[0074] Zu den Leistungen der Einlieferungsstation zählt beispielsweise die Frankierung von Postsendungen.

[0075] In einer besonders bevorzugten Ausführungsform der Erfindung ermittelt die Einlieferungsstation vollautomatisch entgeltrelevante Angaben von Sendungen - beispielsweise durch eine vollautomatische Ermittlung von Format und/oder Gewicht der Sendung.

[0076] In einer besonders bevorzugten Ausführungsform der Erfindung druckt die Einlieferungsstation beziehungsweise ein Bestandteil der Einlieferungsstation einen Frankiervermerk und/oder weitere sendungsrelevante Angaben auf die Sendung (Post- oder Paketsendung) auf.

[0077] Bei einer Integration geeigneter Abrechnungsverfahren ist es möglich, eine Nutzung der Einlieferungsstation durch nicht-registrierte Kunden zu ermöglichen.

[0078] Je nach Ausführungsform der Einlieferungsstation ist es möglich, zusätzlich zu den Brief- oder Paketsendungen auch Warensendungen zu bearbeiten und Zusatzfunktionen, beispielsweise Postzustellungsaufträge, Einschreiben, Nachnahmesendung, Anschriftenüberprüfungen oder Benachrichtigungsfunktionen ... durchzuführen/abzurechnen.

[0079] Bei der nachfolgenden Darstellung bevorzugter Ausführungsformen der Erfindung werden die nachfolgend genannten Abkürzungen und Definitionen eingesetzt:

Abkürzungen und Definitionen

Abkürzung	Beschreibung
CSP	Cryptography Service Provider
CryptoString	Kryptographische Bytefolge aus dem Postage-Point zur Einbringung in den Matrixcode eines jeden Labeldrucks
EPOS	Elektronischer Postschalter Schaltersystem der Postfilialen ("Kasse der Deutschen Post")
gB	Geschützter Bereich auf einem EPOS-Frontend Gerät, der von der Cryptostore.dll verwaltet wird (auch Cryptostore oder Cryptostore-Datei genannt)
m_{secret}	Bei der Schlüsselinformation handelt es sich um den vom Postage-Point stammenden Zahlenwert m_{secret} mit einer Länge von 16 Byte, der dem geschützten Bereich in nochmals verschlüsselter Form als $(m_{secret})_{meter}$ zur Verfügung gestellt wird
P_{meter}	Öffentlicher Schlüssel Einer der beiden Schlüssel eines Schlüsselpaares. Mit dem öffentlichen Schlüssel werden Informationen verschlüsselt und Unterschriften verifiziert. Mit Hilfe des öffentlichen Schlüssels einer Person kann niemand an den entsprechenden privaten Schlüssel gelangen.
PKCS	Public-Key Cryptography Standard PKCS sind eine Reihe von Spezifikationen, die von der Firma RSA Data PKCS Security herausgegeben werden. Diese Papiere beschäftigen sich mit Themen der Anwendung von asymmetrischen Verschlüsselungsverfahren wie RSA. Solche Anwendungen sind z.B. die Erzeugung und Verwendung von digitalen Signaturen und den zugehörigen Zertifikaten.
Postage-ID	16 Byte verschlüsselte Identifikation mit folgendem Inhalt: Hersteller Modell Gerätenummer Lfd. Nr. Postage-ID Key-Phase Währung Portobonitätslimit Gültigkeitsdatum Reserve
PP	Postage-Point Der Postage Point stellt das zentrale Back-Office-System für die Frankierung dar und fungiert als Schnittstelle zu den betroffenen Frontend-Systemen der Deutschen Post. Es werden Sicherheitsinformationen generiert und zur Verfügung gestellt. Über das Interface PostagePoint können sich registrierte Clients / Benutzer beim Postage Point anmelden (login) und die für sie freigegebenen Dienste (Services) in Anspruch nehmen.

(fortgesetzt)

Abkürzung	Beschreibung
S_{meter}	Privater Schlüssel Der geheime Teil eines Schlüsselpaares, mit dem Informationen unterschrieben und entschlüsselt werden. Der private Schlüssel eines Benutzers sollte geheim gehalten werden und nur diesem bekannt sein.
RSA-Schlüssel	Abkürzung von RSA Data Security Steht für die Firmenchefs Ron Rivest, Adi Shamir und Len Adleman und bezieht sich auf den von ihnen erfundenen Algorithmus. Der RSA-Algorithmus wird in der Kryptographie mit öffentlichen Schlüsseln verwendet. Seine Funktionsweise beruht auf der Tatsache, dass zwei große Primzahlen zwar leicht miteinander zu multiplizieren sind, aber das Produkt nur schwer wieder in sie zu zerlegen ist.
TCG	Trusted Computing Group
TMS	Transaktions-Management-System IT-System in das alle Transaktionen, die an den Frontends erzeugt werden, hineinlaufen und verarbeitet werden, um anschließend an Umsysteme weitergegeben zu werden
TPM	Trusted Platform Module
TSS	TCG Software Stack
VGA	Vorgangsart
XML	eXtensible Markup Language

[0080] Der Begriff TCG beinhaltet Implementierungen entsprechend der Trusted Computing Group, ebenso wie Systemkomponenten oder Trusted Computing Platforms, welche entsprechend den Standards der Trusted Computing Group gestaltet sind.

[0081] Eine Weiterbildung der Erfindung beinhaltet einen Einsatz eines Cryptostores.

[0082] Vorzugsweise ist der Cryptostore so ausgebildet, dass er wenigstens ein TPM-Element enthält und/oder an das TPM-Element angepasst werden kann.

[0083] Der (TPM-)angepasste Cryptostore ist die Umsetzung des so genannten "geschützten Bereiches" (gB). Der geschützte Bereich ist das Kernstück der kryptographischen Filialfreimachung mit EPOS (VGA 1114 und VGA1158). Zur Gewährleistung hoher Fälschungssicherheit werden die Freimachungslabel mit maschinenlesbaren Matrixcodes versehen. Diese Matrixcodes enthalten kryptographische Elemente, die ausschließlich über den geschützten Bereich realisiert werden. Diese kryptographischen Elemente werden von dem geschützten Bereich vor dem Ausdruck des Freimachungslabels unter Verwendung hinterlegter Sicherheitsinformationen individuell errechnet und in den Matrixcode eingebracht. Die Bereitstellung der Sicherheitsinformationen erfolgt durch den PostagePoint (PP). TMS wird als Transportschicht genutzt.

[0084] Fig. 1 beinhaltet eine Übersicht, auf der die beteiligten Systeme für die Anforderung und Übernahme der Sicherheitsinformationen gezeigt werden.

[0085] Hierbei werden Sicherheitsanforderungen des für die Erzeugung des digitalen Freimachungsvermerkes bei EPOS (Matrix-Code) erfüllt.

[0086] Der angepasste Cryptostore ist weiterhin als Carbon Basisdienst verwendbar. Die Schnittstellen zu EPOS FE V31.x und Carbon V 4.x sowie die Schnittstelle vom Cryptostore zum PostagePoint (über TPM) bleiben unverändert.

[0087] Die Anpassung des Cryptostore erfolgt derart, dass auch ein Betrieb ohne TPM Unterstützung auf EPOS FE Clients mit Windows NT möglich ist. Der TPMangepasste Cryptostore verhält sich auf Windows NT EPOS FE Clients wie die Vor-Version vom Cryptostore ohne TPM Anpassung.

[0088] In einer besonders bevorzugten Ausführungsform der Erfindung wird mindestens eine Einlieferungsstation mit dem Trusted Platform Module (TPM)ausgestattet, der mittels kryptographischer Verfahren die Integrität sowohl der Software-Datenstrukturen als auch der Hardware messen kann und diese Werte nachprüfbar abspeichert. Das Betriebssystem des Computers, aber auch geeignete Anwendungsprogramme können dann diese Messwerte überprüfen und damit entscheiden, ob die Hard- oder Software-Konfiguration gegebenenfalls verändert wurde und darauf entsprechend reagieren. Dies kann von einer Warnung an den Benutzer bis zum Programmabbruch führen.

[0089] Insbesondere ist es zweckmäßig, die Einlieferungsstation mit einem Betriebssystem auszustatten, das die in dem vorangegangen Absatz dargestellten Integritätsprüfungen veranlasst und gegebenenfalls auch auswertet.

[0090] Eine derartige Ausführungsform ist auch mit einer lediglich passiv wirkenden TPM-Einheit durchführbar.

[0091] Es ist besonders zweckmäßig, die Einlieferunsstation so auszustatten, dass sie eine an die TPM-Einheit, beziehungsweise die TPM-Einheiten angepasste Systemstruktur aufweist.

[0092] Insbesondere wird hierbei eine Sicherheitsplattform bereitgestellt, bei der die sicherheitsrelevanten Prozesse bereits auf der untersten Ebene der Plattform erfolgen.

[0093] Es ist besonders zweckmäßig, durch die TPM-Einheit oder mehrere der TPM-Einheiten eine geschlossene Sicherheitskette zu realisieren.

[0094] Die TPM-Einheit wirkt hierbei als Hardware-Sicherheits-Referenz und stellt die Wurzel ("Root of Trust") der gesamten Sicherheitskette dar.

[0095] Vorteilhafterweise wird zu einem möglichst frühen Zeitpunkt überprüft, ob sich die Signatur und damit die Konfiguration der Einlieferungsstation verändert hat. Somit ist es möglich, durch eine Prüfung der Signatur sicherzustellen, dass keine Änderungen der Einliefungsstation, zumindest keine Änderung von geeichten Prozessen an relevanten Bestandteilen der Einliefungsstation erfolgten.

[0096] Änderungen von Betriebsparametern der Einlieferungsstation führen zu einer Veränderung der Signatur und können daher durch Prüfung der Signatur ermittelt werden.

[0097] Auf entsprechende Weise wird überprüft, ob eine der Komponenten entfernt und/oder ersetzt wurde.

[0098] Ähnliche Überprüfungsmechanismen mit Hilfe der TPM-Einheit verifizieren dann nacheinander die Korrektheit (Unverändertheit gleich Integrität) einzelner oder mehrerer Komponenten, beispielsweise des BIOS, des Bootblocks und des Bootens selbst, sowie die jeweils nächst höheren Schichten beim Starten des Betriebssystems. Während des ganzen Startvorgangs, aber auch später, ist damit der Sicherheits- und Vertrauenszustand des Systems über den TPM abfragbar.

Damit kann aber auch eine kompromittierte Plattform sicher von anderen identifiziert werden und der Datenaustausch auf das angemessene Maß eingeschränkt werden. Trusted-Computing-Systeme können die Voraussetzung schaffen, dass eine wesentliche Weiterentwicklung moderner, vernetzter Plattform-Strukturen auch unter dem Gesichtspunkt der Sicherheit und des gegenseitigen Vertrauens erst möglich wird.

[0099] Kernstück einer erfindungsgemäßen Trusted Computing Base ist die TPM-Einheit. Diese TPM-Einheit ist beispielsweise eine zusätzliche Hardware-Komponente, die einzelne oder mehrere kryptographische Funktionen bereitstellt, die für die Labelfreimachung mit EPOS genutzt werden sollen.

[0100] Im Gegensatz zum "ursprünglichen" Cryptostore werden die Sicherheitsdaten hardwareseitig vom TPM gespeichert und kryptographische Berechnungen ausschließlich von ihm durchgeführt. Damit ist sichergestellt, dass die Sicherheitsinformationen nicht von Unberechtigten ausgelesen und verändert werden können und dass kontrollierbare Algorithmen den Berechnungen zugrunde liegen

[0101] Alle Verschlüsselungen, Entschlüsselungen und andere sicherheitsrelevanten Prozesse sowie die Registerverwaltung werden gegen unberechtigte Zugriffe von der TPM -Einheit geschützt. Ohne TPM bzw. mit dem TPM eines anderen Rechners ist kein Zugriff auf die Daten möglich.

[0102] Die in Fig. 1 dargestellte Architekturübersicht zeigt eine Integration eines Cryptostores mit wenigstens einer TPM-Einheit in ein Bearbeitungssystem.

Beschreibung Cryptostore

[0103] Der Cryptostore dient zur Ablage von sicherheitsrelevanten Daten für die digitale Freimachung. Der Cryptostore ist als dll-Bibliothek als Carbon-Basisdienst ausgeführt (angebotene Schnittstelle, bleibt unverändert). Der Cryptostore nutzt Schnittstellen vom TPM (neue Schnittstelle) und EPOS/TMS zum PostagePoint (Nutzung der Schnittstellen bleibt unverändert). Folgende Funktionalitäten werden realisiert:

- Verwaltung des geschützten Bereiches
- Generierung RSA-Schlüsselpaar
- Erzeugung der signierten Lizenz
- Verschlüsselte Speicherung von Daten
- Update der Ladungsdaten
- Erzeugen des Hashcodes für den Matrixcode
- Behandlung des Bytestrings (Öffnen der Cryptostore-Datei)

[0104] Zweckmäßigerweise werden geeignete Schnittstellen für einen Einsatz des erfindungsgemäßen Systems bereitgestellt.

[0105] Nachfolgend werden zunächst Komponenten einer Schnittstelle zwischen dem Cryptostore zu EPOS/Carbon bereitgestellt. Hierbei können bekannte Schnittstellen (Signatur und Dateninhalte) eingesetzt werden.

[0106] Zweckmäßigerweise ist der Cryptostore an den Einsatz der TPM-Einheiten angepasst.

[0107] Insbesondere ist es zweckmäßig, hierbei die folgenden Funktionen einzusetzen:

AddTruncatedHashValue	ref byte	Berechnet den Hashcode für den

	[]matrixCode	Matrixcode.
CloseStore	-	Schließt die CryptoStore-Instanz.
CreateNewKeyPair	-	Erzeugt ein neues Schlüsselpaar.
CreateStore	string eposDeviceNumber, string riposteGroupId, string riposteNodeId, string filePath1, string filePath2)	Erzeugt eine neue CryptoStore-Instanz.
GetEPOSDeviceNumber	out string eposDeviceNumber	Gibt die in der Meter-ID gespeicherte Gerätenummer zurück.
GetRiposteGroupId	out string riposteGroupId	Gibt die Riposte-Group-ID zurück.
GetRiposteNodeId	out string riposteNodeId	Gibt die Riposte-Node-ID zurück.
GetSignedLicenseAsBase64EncodedXML	out string base64String	Gibt die signierte Lizenz als XML-Datei kodiert in base64 zurück.
IsNewLoadDataRequestRecommended	-	Gibt Werte größer 0 zurück, wenn eine signierte Lizenz zum Postagepoint gesendet werden sollte, um neue Ladedaten anzufordern.
OpenStore	string filePathReadWrite, string filePathWrite	Diese Methode ist im Normalfall zum Öffnen des CryptoStores zu verwenden. Es wird nur vom ersten Pfadnamen gelesen. Änderungen werden aber unter beiden Pfaden gespeichert.
SetLoadDataAsBase64EncodedXML	string base64String	Übergibt die Ladedaten als base64-kodierte XML-Datei.
UpdateRiposteIds	string riposteGroupId, string riposteNodeId	Aktualisiert Riposte-Daten und erzeugt neues Schlüsselpaar und neue Lizenz.

Tabelle 1: Schnittstelle Cryptostore zu EPOS/Carbon

[0108] Zweckmäßige Verfahrensschritte für eine Erstinitialisierung sind in Fig. 2 dargstellt.

[0109] In nachfolgenden Verfahrensschritten erfolgt eine Anforderung und/oder Übernahme von Sicherheitsdaten.

[0110] Bevorzugte Verfahrensschritte für eine Anforderung und Übernahme der Sicherheitsdaten sind in Fig. 3 dargestellt.

[0111] Die Begriffe "Sicherheitsdaten" und "Sicherheitsinformationen" sind jeweils in ihrer weitest möglichen Bedeutung gemeint. Für das Fachgebiet der Erfindung ist es klar, dass die Ausführungen zu den Sicherheitsdaten sich auch

auf die Sicherheitsinformationen beziehen und das umgekehrt die Ausführungen zu den Sicherheitsinformationen auch auf die Sicherheitsdaten beziehen.

[0112] Unter Einbeziehung der Sicherheitsdaten/Sicherheitsinformationen ist es möglich, einen Frankiervermerk, beispielsweise als Matrixcode bereitzustellen.

[0113] Bevorzugte Verfahrensschritte für die Erzeugung des als Frankiervermerk einsetzbaren Matrixcodes sind in Fig. 5 dargestellt.

[0114] Im Bedarfsfall und/oder innerhalb vorgebbarer Prüfungszeiträume erfolgt die - beispielhaft in Fig. 6 dargestellte - Prüfung der Authentifizierungsdaten.

[0115] In dieser Anmeldung wird eine besonders bevorzugte Ausführungsform eines erfindungsgemäßen Cryptostores nachfolgend als EPOS FE-Cryptostore bezeichnet.

[0116] Verfahrensschritte zur Prüfung von Authentifizierungsdaten im EPOS FE-Cryptostore sind in Fig. 6 dargestellt.

[0117] Fig. 7 zeigt Verfahrensschritte zum Schließen des Cryptostores.

[0118] **Aufrufe CryptoStore -> Cryptography Service Provider (CSP) / MSCAPI**

ErstInitialisierung

Nr.	Aufruf EPOS->CS	Aufrufe im CS	Aufruf CS->.NET Cryptograpy /MSCAPI
1	**OpenStore(** string filePathReadWrite, string filePathWrite)	_internalStore = new InternalStore(filePathReadWrite) und Für InternalStore: ... new FileStream	Wenn Windows XP identifiziert worden ist, wird die Initialisierung derart vorgenommen, dass der TPM CSP genutzt wird. Wenn Windows NT identifiziert worden ist, wird der ein nicht TPM-basierter CSP weiter genutzt.
2a	int **CreateStore(** string eposDeviceNumber, string riposteGroupId, string riposteNodeId, string filePath1, string filePath2)	_internalStore = new InternalStore(eposDeviceNumber, riposteGroupId, riposteNodeId); ->a. NewStore() -> RNG.GetBytes **->_registryValue.PutValue(keyData);**	Wenn Windows XP identifiziert worden ist, wird die Initialisierung derart vorgenommen, dass der TPM CSP genutzt wird. Wenn Windows NT identifiziert worden ist, wird der bisherige non-TPM CSP weiter genutzt. RNG.GetBytes(keyData) wobei: RandomNumberGenerator RNG = new RNGCryptoServiceProvider(); Und: namespace System.Security.Cryptography { [ComVisible(true)] public sealed class RNGCryptoServiceProvider :

			RandomNumberGenerator ... }

2b		->b. InitMailingSequence
		->_store.WriteData(..);
		->
		Store.Change/WriteData(..)
		-> Store.
		encryptAES128CBCwithSalt(..)
		
		-> ...
			void Store.addData(string id, byte[] data) {
			// New salt
			byte[] salt = generateSalt();
			byte[] ciphertext = encryptAES128CBCwithSalt(_localKey, salt, _localIV, data);
			
			byte[] Store.encryptAES128CBCwithSalt(..) {
			...
			Rijndael cipher = Rijndael.Create();
			cipher.KeySize = 128;
			cipher.Mode = CipherMode.CBC;
			...
			System.Security.Cryptography.CryptoStream cs = new CryptoStream(cm,cipher.CreateEncryptor(..),..);
			cs.Write(..);
			...

2h		-> h. CreateNewKeyPair(); ->RSAKeyPair.Create(	RSAKeyPair Create(..) {

		GetSerialNumber(), keyGeneration); - >SetPendingRSAKeyPair(newPair) -> SetRSAKeyPair(..) -> _store.WriteData(..) siehe 2b.	... CspParameters cspParameters = .. cspParameters.Flags = CspProviderFlags.UseMachineKeyStore; **System.Security.Cryptography.RSA rsa = getRsaCsp(1024);** RSAKeyPair keyPair = new RSAKeyPair(.., rsa);

Tabelle 2: Erstinitialisierung

Tabelle 3: Anforderung/Übernahme der Sicherheitsdaten

Anforderung/Übernahme der Sicherheitsdaten			
Nr	**Aufruf EPOS->CS**	**Aufrufe Im CS**	**Aufruf CS->.NET Cryptograpy / MSCAPI**

1	int IsNewLoadDataRequestRecommended( )	_intemalStore.IsNewLoadDataRequestRecommended() ->.. ... ->
		GetDaysBeforeEndOfValidity() -> _store.ReadData(DAYS_BEFORE_END_OF_VALIDITY)
			byte[] Store.ReadData(string id){
			// CCurrently only Rijndael128-CBC is supported
			plaintext= decryptAES128CBCwithSalt(_localKey,salt,_localIV,data);

2	GetSignedLicenseAsBase64EncodedX eAsXML() ML()	_internalStore.GetSignedLicens -> GetPendingLicense() ..-> GetLicense(PENDING_LICENSE) -> store.ReadData(PENDING_LIC ENSE) -> GetActiveLicense () ..-> GetLicense(ACTIVE_ LICENSE) -> store.ReadData (ACTIVE LICENSE) -> new SignedLicenseMessage()	Siehe 4.5.2 Nr. 1 (store.ReadData)

3	int SetLoadDataAsBase 64EncodedXML(stri ng base64String)	_internalStore.SetLoadDataAsXML(xmlData) // jdi: get from xmlData/msg: newPostageId, encryptedMSecret,cryptoStr
		-> new MSecret (GetActiveRSAKeyPair (), encryptedMSecret); -> GetRSAKeyPair(ACTIVE_KEY PAIR) -> _store.ReadData (ACTIVE_KEY PAIR) -> SetMSecret(mSecret) -> _store.WriteData(M_SECRET, mSecret.Bytes)
			Siehe 4.5.2 Nr. 1 (store.ReadData) Und
			Siehe 4.5.1 Nr. 2b (store.WriteData)

Tabelle 4: Prüfung Gültigkeit der Sicherheitsinformationen

Prüfung Gültigkeit der Sicherheitsinformationen			
Nr.	**Aufruf EPOS->CS**	**Aufrufe Im CS**	**Aufruf CS->.NET Cryptograpy / MSCAPI**
1	int GetPostageId(out byte[] postageId)	_ internalStore.GetPostageIdAsBytes() -> _store.ReadData (POSTAGE_ID)	Siehe 4.5.2 Nr. 1 (store.ReadData)

Tabelle 5: Generierung Matrixcode

Generierung Matrixcode			
Nr	**Aufruf EPOS->CS**	**Aufrufe Im CS**	**Aufruf CS->.NET Cryptograpy / MSCAPI**
1	int AddTruncatedHashV alue(ref byte[] matrixCodeBytes)	AddUpdateRegister(matrixCode. Value) AddTotalRegister (matrixCode.V alue) GetSerialNumber() IncrementMailingSequence() GetMSecret() -> _store.ReadData(M_SEC RET)	Siehe 4.5.2 Nr. 1 (store.ReadData)
2		matrixCode.ComputeTruncated HashValue(postageId, mSecret)	SHA1 sha1 = new SHA1 CryptoServiceProvider() sha1.ComputeHash(bytesToHa sh)

Tabelle 6: Prüfung Authentifizierungsdaten EPOS FE - Cryptostore

Prüfung Authentifizierungsdaten EPOS FE - Cryptostore			
Nr.	**Aufruf EPOS->CS**	**Aufrufe Im CS**	**Aufruf CS->.NET Cryptograpy / MSCAPI**
1	int GetEPOSDeviceNu mber (out string eposDeviceNumber)	_store.ReadData(SERIAL_NU MBER)	Siehe 4.5.2 Nr. 1 (store.ReadData)
2	string GetRiposteGroupId()	_store.ReadData(SERIAL_NU MBER)	Siehe 4.5.2 Nr. 1 (store.ReadData)
3	string GetRiposteNodeId()	_store.ReadData(SERIAL_NU MBER)	Siehe 4.5.2 Nr. 1 (store.ReadData)
4	int UpdateRipostelds(st ring riposteGroupId, string riposteNodeId)	_store.WriteData(id, UTF8.GetBytes(value) CreateNewKeyPair()	Siehe 4.5.1 Nr. 2b (store.WriteData)

Tabelle 7: Schließen Cryptostores

Schließen Cryptostore			
Nr	**Aufruf EPOS->CS**	**Aufrufe Im CS**	**Aufruf CS->.NET Cryptograpy / MSCAPI**
1	int CloseStore()	internalStore.Dispose()	

[0119] Bevorzugte Verfahrensschritte zur Verwendung des TPM-Elements sind nachfolgend dargestellt.

[0120] Beim Initialisieren (Open / Create Store) des Cryptostores wird geprüft, ob der Cryptostore unter Windows NT oder Windows XP genutzt wird. Wird der Cryptostore unter Windows NT genutzt, wird **kein TPM** verwendet, d.h. der Cryptostore verwendet den Software Cryptography Service Provider und verhält sich wie bisher. Wird der Cryptostore unter Windows XP genutzt, **wird TPM verwendet,** d.h. der entsprechende TPM Hardware CSP genutzt.
Damit die bisherige Cryptostore-Implementierung TPM verwendet werden kann, wird anstatt des bisher genutzten Software Cryptography Service Provider (CSP) der zum TPM Chip mitgelieferte TPM-Hardware CSP verwendet bzw. referenziert. Aus Sicherheitsgründen wird der Providername und -type fest im Code verankert:

```
CSP_ProviderName = "Infineon TPM Platform Cryptographic Provider";
CSP_ProviderType = 12;
```

[0121] Voraussetzungen sind:

- Installation Infineon TPM Professional Package V2.0.2 und
- Initialisierung TPM Chip (Take_Ownership).
  Durch Verwendung des TPM-CSP wird den Anforderungen des Auftraggebers, die erweiterte Sicherung des Cryptostores durch Verwendung des TPM, entsprochen.

[0122] Das TPM wird für folgende Funktionen und zu sichernden Daten genutzt:

- **TPM gesicherte Speicherung des Cryptostores**

[0123] Durch das TPM wird mittels des TPM-Hardware Storage Root Key per RSA (2048) ein persistenter Cryptostore Storage Key als RSA-Objekt erzeugt, mit dem der Cryptostore Daten verschlüsselt, auf der Festplatte ablegt.
[0124] Hierdurch sind alle Daten, die sich im Cryptostore befinden, nur in Kombination mit der TPM-Hardware (genauer: dessen eindeutigen Storage
[0125] Root Key) verwendbar. Durch diesen Mechanismus sind insbesondere folgende Daten ohne TPM- Hardware nicht mehr verwendbar.
[0126] Daten des geschützten Bereiches (des bisherigen non-TPM Cryptostore).
Diese sind:

- ○ Das Schlüsselpaar S_{meter} / P_{meter}
- ○ Sicherheitsinformationen vom PostagePoint (m_{secret}, Postage-ID, CryptoString)
- ○ Aufsteigende Register (Gesamt und seit letzter Ladung)
- ○ Laufende Sendungsnummer
- ○ Riposte GroupID/-NodeID, FE Gerätekennung
- ○ Meter-ID
- **Hashwertbildung**

[0127] Ein Hash-Wert wird durch direkte Verwendung der TPM-CSP nach SHA-1 gebildet (Input: postalische Inhalte Matrixcode, Postage-ID, m_{secret}). m_{secret} wird dazu entschlüsselt der Methode übergeben. Im Matrixcode werden die ersten vier Bytes des Hash-Wertes verwendet.
[0128] Eine bevorzugte Schlüsselhierarchie ist in Fig. 8 dargestellt. Durch das TPM-Element verschlüsselte und/oder gesicherte Daten werden auf einem geeigneten Speichermedium, beispielsweise einer Festplatte permanent und persistent gespeichert.
[0129] Die Anwendung EPOS implementiert die Funktionalität zum Ansprechen des TPM über die Service Provider Schnittstelle (siehe Architektur-Abbildung, TCG). Der TCG Software Stack (TSS) ist Teil einer TCG konformen Plattform und stellt Funktionen zur Verfügung, die von erweiterten Betriebssystemen und Applikationen verwendet werden können. Der TCG Service Provider wird durch den Basisdienst ‚CryptoStore' aus EPOS heraus angesteuert.
[0130] Der Basisdienst wird auf der Grundlage von Carbon 4.0 und .Net 2.0 implementiert. Die Anlage 8.1 zeigt die vollständige Softwarearchitektur des TPM.
Für die konkrete Entscheidung, welche Implementierung / Bibliothek für die Anbindung des TPM zu verwenden ist, ist in Hinblick auf die Lizenzierung zu prüfen, welche Tools/Implementierung der TPM-Test-Hardware schon beiliegen, und ob die in Frage kommenden TPM Bibliotheken die Funktionen zur Verfügung stellen, die für die o. g. Umsetzung der angepassten Cryptostore benötigt werden.

Fehlerbehandlung / Logging

[0131] Der CryptoStore schreibt Infonachrichten in ein InfoLog (TracingLevel.InfoLog) als Information (LoggingEntryType.Information) unter dem Switch EPOS.CryptoStore. Ein erfolgreiches Anlegen des Cryptostores unter TPM wird folgendermaßen geloggt:
TraceInfo("Neuer Sicherer Bereich wurde mittels TPM erzeugt für Gerät \"" + eposDeviceNumber + "\" mit Riposte Group ID \""+ riposteGroupId + "\" und " + " Node ID \"" + riposteNodeId + "\".");
[0132] Das erfolgreiche Öffnen mittels TPM:
TraceInfo("Sicherer Bereich wurde mittels TPM geöffnet von Datei " + _filePath1 + ".");
[0133] Die sich im Fehlerfall ergebenden Ausnahmen werden in das InfoExceptionLog (TracingLevel.InfoExceptionLog) als Error (LoggingEntryType.Error) unter dem Switch EPOS.CryptoStore geschrieben. Zusätzlich gibt die jeweilige Methode einen negativen Retumcode zurück. Bei TPM Fehlersituationen wird der Code -6 (Fehler bei den Argumenten) an EPOS zurückgegeben.
Hinweis: Für Aktivitäten am TPM gibt es keinen direkten Logging-Mechanismus. Einzig auf Transport Ebene gibt es einen optionalen Logging-Mechanismus für den allerdings geprüft werden muss, ob die vorliegende Kombination aus Hardware/ TPM-Treiber diesen unterstützt. Für das Projekt DigiMarke_TPM ist eine Verwendung nicht vorgesehen.

Schutz Cryptostore.dll

[0134] .NET-Lösungen lassen sich nicht nur disassemblieren, sondern auch dekompilieren. Ohne besondere Schutzmaßnahmen wird quasi der Sourcecode mitgeliefert. Microsoft liefert mit dem Visual Studio .NET ein Werkzeug zum "Verschleiern" einer DLL, die Dotfuscator Community Edition. Aufgrund seiner Funktionsbeschränktheit ist seitens des Auftraggebers zu prüfen, ob ein anderes, leistungsfähigeres, Tool genutzt werden soll.
Bis zur Entscheidung wird die Dotfuscator Community Edition genutzt.
[0135] Eine für einen Einsatz der Erfindung geeignete Entwicklungsumgebung enthält beispielsweise einzelne, mehrere oder sämtliche der folgenden Komponenten:
[0136] Software

- VSS für Versionsverwaltung
- Visual Studio .NET 2005
- Carbon 4.0
- Cryptostore.dll mit entsprechendem Testrahmen
- TPM-Bibliotheken / Suites: Infineon TPM Professional Package 2.0 Hardware
- Neues Filial Frontend-Gerät von Wincor Nixdorf

[0137] Eine Prinzipdarstellung eines bevorzugten erfindungsgemäßen Software-Stacks entsprechend der TCG-Spezifikation ist in Fig. 9 dargestellt.
[0138] Eine Prinzipdarstellung eines inneren Aufbaus einer TCG-Einheit ist in Fig. 10 dargestellt.
[0139] Die TPM-Einheit weist vorzugsweise eine funktionale Einheit, einen nicht flüchtigen Speicher und einen flüchtigen Speicher auf.
[0140] Die funktionale Einheit enthält vorzugsweise Komponenten, welche mit anderen Bestandteilen des Systems wechselwirken können, beispielsweise einen
[0141] Zufallszahlgenerator, einen Hash-Wert-Generator, einen RSA-Schlüsselgenerator und/oder ein Mittel zur Ver- und Entschlüsselung - beispielsweise anhand der RSA-Spezifikation.
[0142] Der nicht flüchtige Speicher enthält vorzugsweise solche Schlüsselinformationen bzw. Schlüssel, die nicht verändert werden sollen, beispielsweise einen Endorsement Key, einen Storage Root Key oder eine Owner Auth Secret-Key.

Nachrichtenformate zwischen EPOS (CryptoStore) und PostagePoint

Allgemeine Festiegungen

[0143] Die Nachrichten sind vorzugsweise als XML-Dokumente formatiert.
Die XML-Dokumente werden vom Postage-Point bzw. dem sicheren Bereich generiert und verarbeitet und sind ohne Änderungen von dazwischen liegenden Softwaremodulen und Softwareprodukten zu übertragen.
Werden die XML-Dokumente als Dateien gespeichert, ist das folgende Format für den Dateinamen zu verwenden. Es ist in Augmented Backus Naur Form (ABNF) spezifiziert. Ein Beispiel für Ladedaten ist LD-12345-123-2003-05-27.xml.

file-name = descriptor "-" riposte-group-id "-" riposte-node-id

year "-" month "-" day extension

descriptor = 2CHAR

riposte-group-id = *DIGIT

riposte-node-id = *DIGIT

year = 4DIGIT

month = 2DIGIT

day = 2DIGIT

extension = ".xml"

Signierte Lizenz

XML-Dokument

[0144] Das XML-Dokument für die signierte Lizenz besteht aus dem Root-Element signed-license-message.

[0145] Es enthält ein Element signed-license in dessen Attribut das Binärformat der signierten Lizenz in Base64-Kodierung gespeichert ist. Im Anhang A sind die verwendete XML-Schemadefinition sowie die DTD-Definition angegeben.

Hier ein Beispiel mit gekürztem Base64-Wert.

```
<?xml version="1.0" encoding="utf-8"?>
<signed-license-message>
<signed-license
value="AAAAFAAAAAHxAXTnAgEAAQEAOXc...Zc2yGW53DQTJhY=" />
</signed-license-message>
```

[0146] Als Abkürzung im Dateinamen ist SL zu verwenden. Ein Beispiel für einen Dateinamen ist SL-12345-123-2003-05-27.xml

Binärformat

[0147] Das Binärformat der signierten Lizenz besteht aus den Lizenzdaten auf die eine Signatur folgt. Das Signaturformat ist PKCS#1 Version 1.5. Zur Signatur wird der in der Nachricht enthaltene öffentliche Schlüssel verwendet.

[0148] Die Lizenzdaten bestehen aus Nachrichtensegmenten, die mit einem Segmentkopf versehen sind. Der Segmentkopf besteht aus zwei vorzeichenlosen Ganzzahlen mit je vier Byte im Big-Endian-Format. Die erste Ganzzahl gibt die Länge des Segments inklusive des Segmentkopfs in Byte an. Die zweite Ganzzahl enthält den Typkode für das Segment. Segmente werden nicht "aligned".

[0149] Folgende Tabelle gibt ein Überblick über die Typkodes:

1	METER_ID	Segment enthält die Meter-Id
2	RSA_EXPONENT	Enthält den RSA-Exponent als große Ganzzahl im Big-Endian-Format.
3	RSA_MODULUS	Enthält den RSA-Modul als große Ganzzahl im Big-Endian-Format.
4	RIPOSTE_NODE_ID	Riposte-Node-Id in UTF8-Kodierung.
5	RIPOSTE_GROUP_ID	Riposte-Group-Id in UTF8-Kodierung
6	DATE_TIME	Datum und Uhrzeit an dem die signierte Lizenz erzeugt wurde. Anwendung findet das ISO-Format (ISO 8601:2000) mit Datum, Uhrzeit in Sekunden in UTC. Beispiel: 2003-04-28T13:39:24Z
7	HASH_ALGORITHM	Der Hashalgorithmus als String. Einziger erlaubter Wert: SHA-1
8	SIGNATURE_ALGORITHM	Das Verfahren für die Signatur. Einziger erlaubter Wert: PKCS#1-v1.5
0xffffffff	END	Leeres Endesegment, auf das die Signatur folgt.

Tabelle 8: Überblick Typkodes

[0150] Aus der Bytefolge aller Segmente wird dann der Hash mit dem angegebenen Hashalgorithmus berechnet und dieser Hash wird mit dem angegeben Signaturverfahren signiert.

[0151] Es folgt die Beschreibung der Syntax in Augmented Backus Naur Form:

```
signed-license = body signature

body = *segment end-segment

segment = segment-length segment-type segment-data

segment-length = 4OCTET ; big-endian integer

segment-type = 4OCTET ; big-endian integer

segment-data = *OCTET ; byte sequence

end-segment = %x00.00.00.08 %xff.ff.ff.ff

signature = *OCTET ; signature in the PKCS#1-v1.5 format
```

Die Ladungsdaten

[0152] Die Ladungsdaten werden vom Postage-Point nach Prüfung der Lizenz erzeugt. Das XML-Dokument beinhaltet das Root-Element load-data-message. Dieses Root-Element enthält ein einzelnes Element mit dem Tag load-data. Dieses Element integriert in Folge die Elemente riposte-group-id, riposte-node-id, postage-id, cryptostring und encrypted-m-secret. Die Riposte-Ids werden als Strings angegeben, dabei werden Leerzeichen ignoriert. Das Binärformat für die Postage-Id ist im Dokument "Kryptographische Filialfreimachung mit EPOS" beschrieben. Der Cryptostring ist aus Sicht von EPOS eine Bytefolge ohne eine spezifische Struktur.

[0153] Das M-Secret wird nach PKCS#1 v1.5 verschlüsselt mit dem öffentlichen Schlüssel übertragen. (Die Anwendung von OAEP wird im .Net Framework nicht unter allen Windows-Versionen unterstützt.)

[0154] Alle binären Daten sind base64-kodiert in das XML-Dokument aufzunehmen.

[0155] Ein Beispiel für die Ladungsdaten mit gekürzten Base64-Werten.

```
<?xml version="1.0" encoding="utf-8"?>
<load-data-message>
<load-data>
<riposte-group-id>12345</riposte-group-id>
<riposte-node-id>123</riposte-node-id>
<postage-id>8QF05wIAAAACAQAD6DqbAA==</postage-id>
<crypto-string>Iv0VGHXJ...mw18FN7nK+9bO2Ew=</crypto-string>
<encrypted-m-secret>CL4ub4cYBrFh8...WtyQnE6Y4Pty/oY=</encrypted-m-secret>
</load-data>
</load-data-message>
```

[0156] Als Abkürzung für den Dateinamen ist LD zu verwenden. Ein Beispiel für einen Dateinamen ist LD-12345-123-2003-05-27.xml.

Messdatenspeicherung

[0157] Jedes Workflowelement der Einlieferungsstation kapselt Funktionen der Geschäftsobjekte:

- Ein Messdatum ist ebenso Teil des Geschäftsobjekts wie andere Merkmale
- Nach streng objektorientierter Logik ist die Funktion der Messdatenspeicherung so gestaltet, dass nur die Schnittstelle der Messeinrichtung darauf schreibenden und autorisierten Zugriff darauf hat.
- Alle anderen Workflowelemente haben nur lesenden Zugriff

[0158] Ein Produkt in der Einlieferungsstation setzt sich aus Verkaufs- und Annahme-Workflowkomponenten zusammen:

- Während des Verkaufsvorgangs wird je nach Produktkategorie das mögliche Einzelprodukt soweit eingegrenzt, dass nur noch die Kategorie Format bestimmt werden muss
- Die Eingrenzung kann ähnlich Access Control Lists aus verschiedenen Aspekten heraus erfolgen: Produkt, Vertrag, Aktion, konkreter Maschinentyp
- Die Formatermittlung ist Teil der Sendungsannahme und ergänzt die vorher schon gewonnen Produktinformationen zu einem konkreten Einzelprodukt. Die Formatermittlung ist immer maschinenspezifisch

[0159] In Fig. 11 ist ein mögliches Ausführungsbeispiel der erfindungsgemäßen Einlieferungsstation dargestellt. Bei der Einlieferungsstation 10 handelt es sich um einen Selbstbedienungsautomaten, an dem Kunden Postsendungen wie Brief- oder Warensendungen anliefern können. Vorzugsweise handelt es sich dabei um registrierte Kunden, die sich beispielsweise über eine Kundenkarte identifizieren können, so dass die durch die Einlieferungsstation erbrachten Leistungen auf einfache Weise beim Kunden abgerechnet werden können. Zu den Leistungen des

[0160] Automaten zählt insbesondere die Frankierung von Postsendungen mit dem erforderlichen Portoentgelt. Der Automat ermittelt dabei vollautomatisch das Format einer Sendung, berechnet das korrekte Entgelt und druckt dieses als Frankiervermerk auf die Sendung auf. Der Automat kann auch nicht-registrierten Kunden zur Verfügung gestellt werden, wenn geeignete Abrechnungsverfahren integriert werden. Neben Brief- und Warensendungen können beispielsweise auch Postzustellungsaufträge, Einschreiben, Nachnahmesendungen oder eine Anschriftenprüfung von der Einlieferungsstation 10 durchgeführt werden.

[0161] Mehrere Einlieferungsstationen sind vorzugsweise mit einem Backendsystem verbunden, welches wenigstens

den Betrieb der Automaten und die Abrechnung von Dienstleistungen bei den Kunden abwickelt. Zum Betrieb der Automaten gehört beispielsweise die Wartung, die Einstellung von Sammelbehältern für die Aufnahme von Postsendungen und die bedarfsgerechte Abholung eingelieferter Sendungen. Die Backendsysteme können ferner die Identifikation und Legimitation von Kunden, die Bestimmung von Einlieferungslimits und eine Nachverfolgung eingelieferter Sendungen übernehmen. Bei der Gesamtanwendung kann es sich um eine Client-Server-Anwendung handeln, wobei eine Einlieferungsstation jedoch vorzugsweise als Rich-Client ausgebildet ist, auf dem sich die Anwendungslogik befindet.

[0162] Um im Außenbereich eingesetzt werden zu können, ist eine Einlieferungsstation 10 zweckmäßigerweise einbruchsicher und wetterbeständig ausgeführt. Eine Einlieferungsstation umfasst üblicherweise ein für einen Kunden unzugängliches Gehäuse. Sobald der Kunde die Postsendungen in die Vorrichtung eingebracht hat, besteht für ihn keine Möglichkeit mehr, auf die Postsendungen zuzugreifen. Die Vorrichtung ist jedoch für Servicepersonal zugänglich, welches Zugriff auf die verschiedenen technischen Komponenten hat. Zu diesem Zweck können eine oder mehrere verschließbare Klappen vorgesehen sein, welche den Zugriff auf die Technik der Vorrichtung freigeben. Die Vorrichtung ist ferner für Angestellte des Betreibers der Vorrichtung zugänglich, welche eingelieferte Postsendungen entnehmen und diese dem Transport und Zustellprozess zuführen.

[0163] Für die Abholung und den anschließenden Transport werden die eingelieferten Postsendungen 20 vorzugsweise in einem oder mehreren Behältern 12 gesammelt, welche ebenfalls durch eine verschließbare Klappe zugänglich sind. Es kann vorgesehen sein, dass die Vorrichtung eine Füllstandskontrolle der betreffenden Sammelbehälter durchführt. Sind die Sammelbehälter bis zu einem vorgebbaren Maß befüllt, wird der Betreiber der Vorrichtung benachrichtigt, dass eine Entleerung erfolgen muss. Ferner kann die Annahme weiterer Sendungen an der Vorrichtung verweigert werden.

[0164] Die Vorrichtung gemäß Fig. 11 weist ein Annahmemittel 11 zur Annahme von Postsendungen 20 auf. Dabei handelt es sich vorzugsweise um einen Vereinzeler, welcher einen Stapel von Postsendungen einzeln in die Vorrichtung einzieht. Bei dem Vereinzeler kann es sich um eine aus dem Stand der Technik bekannte Vorrichtung handeln, welche einen Einzeleinzug ermöglicht. Der Kunde legt einen Stapel mit Sendungen beispielsweise in eine Annahmeöffnung 11 ein und schließt eine Abdeckungsklappe, hinter welcher daraufhin der Einzug der Sendungen erfolgt. Einzelsendungen können ebenfalls über den Einzug in die Vorrichtung aufgenommen werden. Die Vorrichtung kann ferner wie herkömmliche Briefkästen einen Schlitz zum Einwerfen von Einzelsendungen aufweisen.

[0165] Nach der Vereinzelung der Sendungen durchläuft eine Postsendung 20 die Vorrichtung 10 mittels eines oder mehrerer Transportmittel. Bei den Transportmitteln handelt es sich beispielsweise um Transportbänder und Rollen, welche eine Sendung durch verschiedene Messvorrichtungen und anschließend durch eine Druckanordnung leiten. Die Sendungen werden dabei vorzugsweise hochkant stehend transportiert. Die verschiedenen Messvorrichtungen ermitteln wenigstens das Gewicht und die Abmessungen der Sendung. Die Ermittlung der einzelnen Messwerte kann dabei nacheinander oder durch verschiedene Messeinrichtungen gleichzeitig erfolgen.

[0166] Das Gewicht G einer Sendung 20 kann durch verschiedene Verfahren zur Gewichtsermittlung gemessen werden. In einem besonders bevorzugten Ausführungsbeispiel der Erfindung wird das Gewicht durch eine dynamische Waage 30 ermittelt. Die Waage kann kalibriert werden, wobei ferner die Minimal- und Maximaltoleranzwerte ermittelt werden. Die Toleranzwerte der Waage werden in einem Rechenmittel 50 der Vorrichtung hinterlegt.

[0167] Die Länge L einer Sendung kann ebenfalls mit verschiedenen bekannten Mitteln bestimmt werden. Die Messung der Höhe H einer Sendung kann gleichfalls über bekannte Verfahren erfolgen.

[0168] Die Messung der Breite B eine Sendung erfolgt beispielsweise über eine Bilderkennung oder über fest installierte Breitenmesssensoren. Dabei ist die Breite B als der kleinste Abstand zweier gegenüberliegender Kanten einer Sendung zueinander definiert. Die Toleranzwerte der Messeinrichtung können über Messreihen ermittelt werden.

[0169] Die Messeinrichtungen zur Bestimmung von Länge, Breite und Höhe einer Postsendung 20 werden im Folgenden in ihrer Gesamtheit als Dimensionsmessgerät 40 bezeichnet. Ein solches Dimensionsmessgerät kann somit aus einem oder mehreren Messgeräten bestehen. Die verschiedenen Messeinrichtungen sind mit einer Recheneinheit 50 verbunden, die sich vorzugsweise ebenfalls innerhalb der Vorrichtung 10 befindet. Bei der Recheneinheit 50 kann es sich beispielsweise um einen PC mit einem Prozessor, einem Speicher, mehreren Festplatten und Wechselmedien handeln. Der PC verfügt ferner über einen Netzwerkanschluss beispielsweise in Form von Fast Ethernet.

[0170] Durchläuft eine Postsendung 20 die verschiedenen Messeinrichtungen, werden die ermittelten Messwerte zur Auswertung an die Recheneinheit 50 übergeben. Dabei erzeugt die Recheneinheit 50 aus den Messwerten korrigierte Messwerte, indem die Negativ- und Positivtoleranzen der einzelnen Messeinrichtungen verarbeitet werden. In einem ersten Schritt werden diese Toleranzwerte mit den ermittelten Messwerten H für die Höhe, L für die Länge, G für das Gewicht und B für die Breite der Postsendung verrechnet. Dabei wird jeweils der Betrag der Negativtoleranz zum gemessenen Messwert addiert, um angepasste Messwerte H', L', G' und B' zu erhalten. Ferner wird der Betrag der Positivtoleranz vom gemessenen Messwert subtrahiert, um angepasste Messwerte H", L", G" und B" zu erhalten.

[0171] Wird ein Produkt bzw. eine Produktklasse ermittelt, in deren Wertebereich alle angepassten Messwerte liegen, wird der zugeordnete Portobetrag in eine Ergebnisliste aufgenommen. Enthält diese Ergebnisliste mehrere Portobeträge,

wird der kleinste Betrag ermittelt und als auf die Postsendung aufzubringender Portobetrag bestimmt. Enthält die Ergebnisliste nur einen Eintrag, wird der betreffende Portobetrag als aufzubringender Portobetrag ermittelt. Mit dem so ermittelten Portobetrag wird in einer Frankiereinheit 60 ein Freimachungsvermerk erzeugt und auf die Postsendung 20 aufgedruckt. Als Frankiereinheit können jegliche aus dem Stand der Technik bekannte Frankiereinheiten zum Einsatz kommen, die beispielsweise einen Frankiervermerk in Form eines Matrixcodes auf eine Postsendung aufdrucken.

[0172] Ist die Ergebnisliste leer, konnte anhand der Messungen keine Produktklasse bestimmt werden und die Sendung kann durch die Vorrichtung nicht angenommen werden. In diesem Fall wird dem Nutzer über ein Anzeigemittel der Vorrichtung eine entsprechende Meldung angezeigt und die Sendung aus der Vorrichtung ausgeworfen.

[0173] In einem weiteren Ausführungsbeispiel der Erfindung wird die Ermittlung des Portobetrages durch Angaben eines Nutzers zu der Art der Postsendung ergänzt, so dass es sich um eine halbautomatische Portoermittlung handelt. Die Art der Sendung kann beispielsweise Informationen zu Inhalt, Sendungsziel oder Zusatzleistungen umfassen. Diese Informationen werden in einem Ausführungsbeispiel der Erfindung nicht physikalisch ermittelt, sondern vom Nutzer durch eine Bedieneinheit 13 der Einlieferungsstation 10 eingegeben. Die Bedieneinheit kann beispielsweise eine Tastatur, einen Bildschirm oder einen Touchscreen und ein Kartenlesegerät umfassen.

[0174] Beispielsweise wird von einem Nutzer angegeben, ob das Sendungsziel der Postsendung national oder international ist. Dies kann auch automatisch durch eine Auswertung der Sendungsadresse erfolgen. Da jedoch bei unleserlichen Anschriften eine manuelle Auswertung erforderlich ist, kann vorgesehen sein, dass das Sendungsziel grundsätzlich vom Nutzer eingegeben wird. Dabei ist es vorteilhaft, dass der Nutzer die Unterscheidung zwischen nationalen und internationalen Zustellungen nicht für jede Sendung einzeln, sondern für eine größere Menge zugleich eingelieferter Sendungen angibt.

[0175] Die Einlieferungsstation 10 kann ferner einen Barcodeleser zum Erfassen von auf Postsendungen befindlichen Barcodes umfassen. Darüber hinaus weist die Vorrichtung vorzugsweise ein oder mehrere Kameras auf, um Bilder der Postsendungen aufzunehmen. Dabei werden vorzugsweise Bilder der Adressseite von Postsendungen aufgenommen. Das Bild einer Postsendung kann beispielsweise dazu verwendet werden, um es einem Kunden auf dem Bildschirm der Bedieneinheit 13 anzuzeigen. Der Kunde kann die Adressdaten einsehen und damit ein Einschreiben beauftragen.

[0176] Die Erfindung ist jedoch nicht auf die beschriebene Ausführungsform einer Einlieferungsstation beschränkt, sondern eignet sich für jegliche Vorrichtungen zur Annahme und Frankierung von Postsendungen, welche zugelassen und geeicht werden müssen.

[0177] Bei der Einlieferungsstation kann es sich in Weiterbildungen der Erfindung auch um eine Annahmstelle für Postsendungen handeln, die sich beispielsweise in einer Filiale eines Postdienstleistungsunternehmens befindet.

Patentansprüche

1. Einlieferungsstation (10) zum Einliefern und Frankieren von Postsendungen (20), die wenigstens eine Waage (30) zur Bestimmung des Gewichts einer Postsendung (20), wenigstens ein Dimensionsmessgerät (40) zur Bestimmung der Abmessungen einer Postsendung (20), eine Recheneinheit (50) zur Bestimmung des Portoentgelts für eine Postsendung (20) und eine Frankiereinheit (60) zur Aufbringung eines Frankiervermerks auf die Postsendung (20) umfasst, wobei die Recheneinheit (50) Zugriff auf Messtoleranzen der Waage (30) und des Dimensionsmessgerätes (40) hat,
   dadurch gekennzeichnet,
   dass die Einlieferungsstation (10) ein Messmodul (52) mit einem Mittel zum Empfangen von Messwerten von der Waage (30) und/oder dem Dimensionsmessgerät (40) aufweist und dass das Messmodul (52) und/oder eine Komponente des Messmoduls (52) mit einer TPM-Einheit verbindbar ist.

2. Einlieferungsstation nach Anspruch 1,
   dadurch gekennzeichnet,
   dass das Messmodul (52) und seine Komponenten eine Signatur aufweisen, die auf einer asymmetrischen Verschlüsselung beruht.

3. Einlieferungsstation nach Anspruch 2,
   dadurch gekennzeichnet,
   dass die Signatur mit einem privaten Schlüssel erzeugt wurde, der von der TPM-Einheit erzeugbar ist und/oder in der TPM-Einheit gespeichert ist.

4. Einlieferungsstation nach einem der vorangegangenen Ansprüche,
   dadurch gekennzeichnet,
   dass die TPM-Einheit fest in die Recheneinheit (50) eingebaut ist.

5. Einlieferungsstation nach einem der Ansprüche 3 oder 4,
dadurch gekennzeichnet,
dass ein Zugriff auf den privaten Schlüssel in TPM-Einheit durch ein Passwort geschützt ist.

6. Einlieferungsstation nach einem der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass die Waage (30), das Dimensionsmessgerät (40) und/oder eine zugehörige Schnittstelle Mittel zur Bildung eines Hash-Wertes über einen Messwert aufweisen.

7. Einlieferungsstation nach einem der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass das Messmodul (52) Mittel zur Bildung eines Hash-Wertes über einen Datensatz bestehend aus wenigstens den Messwerten der Waage (30) und des Dimensionsmessegerätes (40), den zugehörigen korrigierten Messwerten und der ermittelten Produktkategorie einer Postsendung (20) aufweist.

8. Einlieferungsstation nach einem der vorangegangenen Ansprüche,
dadurch gekennzeichnet,
dass es sich bei dem Messmodul (52) und seinen Komponenten um Softwarekomponenten in Form von Java Archiv-Files handelt.

9. Einlieferungsstation nach anspruch 8,
dadurch gekennzeichnet,
dass das Messmodul (52) und seine Softwarekomponenten auf einem schreibgeschützten Speichermedium gespeichert sind, dessen mechanischer Schreibschutzschalter physikalisch versiegelt ist, wobei die Verbindung des Speichermediums mit der Recheneinheit (50) ebenfalls physikalisch versiegelt ist.

10. Verfahren zum Einliefern und Frankieren von Postsendungen in einer Einlieferungsstation (10), bei dem das Gewicht einer Postsendung von wenigstens einer Waage (30) und die Dimensionen einer Postsendung (20) von wenigstens einem Dimensionsmessgerät (40) bestimmt und einer Recheneinheit (50) zugeführt werden, und bei dem die Recheneinheit (50) das Portoentgelt für eine Postsendung (20) bestimmt und einer Frankiereinheit (60) zuführt, welche einen Frankiervermerk auf die Postsendung (20) aufbringt, wobei die Recheneinheit (50) zur Erzeugung von korrigierten Messwerten auf Messtoleranzen der Waage (30) und des Dimensionsmessgerätes (40) zugreift, **gekennzeichnet durch** wenigstens folgende Schritte:

- Übermitteln von Messwerten von der Waage (30) und/oder dem Dimensionsmessgerät (40) an ein Messmodul (52);
- Empfangen der Messwerte **durch** das Messmodul (52);
- Signieren der Messwerte für das Gewicht und die Abmessungen der Postsendung (20) **durch** die Waage (30) und das Dimensionsmessgerät (40) oder eine jeweils zugehörige Schnittstelle mit Hilfe eines TPM-Moduls;
- Übermittlung der signierten Messwerte an die Recheneinheit (50) über eine gesicherte Schnittstelle (51);
- Abrufen von Toleranzwerten der Waage (30) und des Dimensionsmessgerätes (40) aus einem signierten Einwegspeicher (55) **durch** ein Messmodul (52) der Recheneinheit (50);
- Ermittlung eines Portoentgelts aus einer Datei (93), die eine Zuordnung zwischen Produktkategorien von Postsendungen und Portoentgelten enthält, anhand der ermittelten Produktkategorie **durch** das Messmodul (52);
- Zuführung des ermittelten Portoentgelts von dem Messmodul (52) zu der Frankiereinheit (60) und Aufbringen eines Frankiervermerks auf die Postsendung (20) **durch** die Frankiereinheit (60); und
- Signieren eines Datensatzes bestehend wenigstens aus Messwerten der Waage (30) und des Dimensionsmessegerätes (40), den zugehörigen korrigierten Messwerten und der ermittelten Produktkategorie einer Postsendung (20) und Speichern dieses signierten Datensatzes im signierten Einwegspeicher (55) **durch** ein Speichermodul (92) des Messmoduls (52);
- Und dass die Signierung mit einem privaten Schlüssel erfolgt, der von einem TPM-Chip (Trusted Platform Module) der Recheneinheit (50) erzeugt wurde und/oder in diesem gespeichert wurde, wobei der TPM-Chip fest in die Recheneinheit (50) eingebaut ist.

11. Verfahren nach Anspruch 10,
dadurch gekennzeichnet,
dass wenigstens Messwerte und/oder korrigierte Messwerte der Waage (30) und des Dimensionsmessgerätes (40)

auf einer Anzeige (80) in Verbindung mit der Recheneinheit (50) angezeigt werden, wobei eine auf der Anzeige (80) angezeigte Maske von dem Messmodul (52) signiert wird.

12. Verfahren nach einem der Ansprüche 10 oder 11,
dadurch gekennzeichnet,
dass das Messmodul (52) und seine Komponenten vor Durchführung der Verfahrensschritte des Anspruchs 13 signiert werden, wobei die Signierung durch eine asymmetrische Verschlüsselung erfolgt.

13. Verfahren nach einem der Ansprüche 10 bis 12,
dadurch gekennzeichnet,
dass das Messmodul (52) und seine Softwarekomponenten vor Durchführung der Verfahrensschritte nach Anspruch 11 auf einem schrelbgeschützten Speichermedium gespeichert werden, dessen mechanischer Schreibschutzschalter nach der Speicherung physikalisch versiegelt wird, wobei die Verbindung des Speichermediums mit der Recheneinheit (50) ebenfalls physikalisch versiegelt wird.

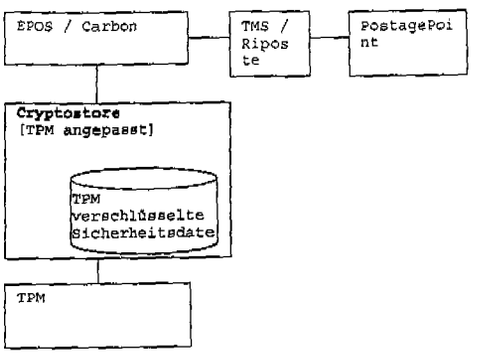
EPOS / Carbon
TMS / Ripos te
PostagePoi nt
Cryptostore
[TPM angepasst]
TPM verschlüsselte Sicherheitsdate
TPM

Fig. 1

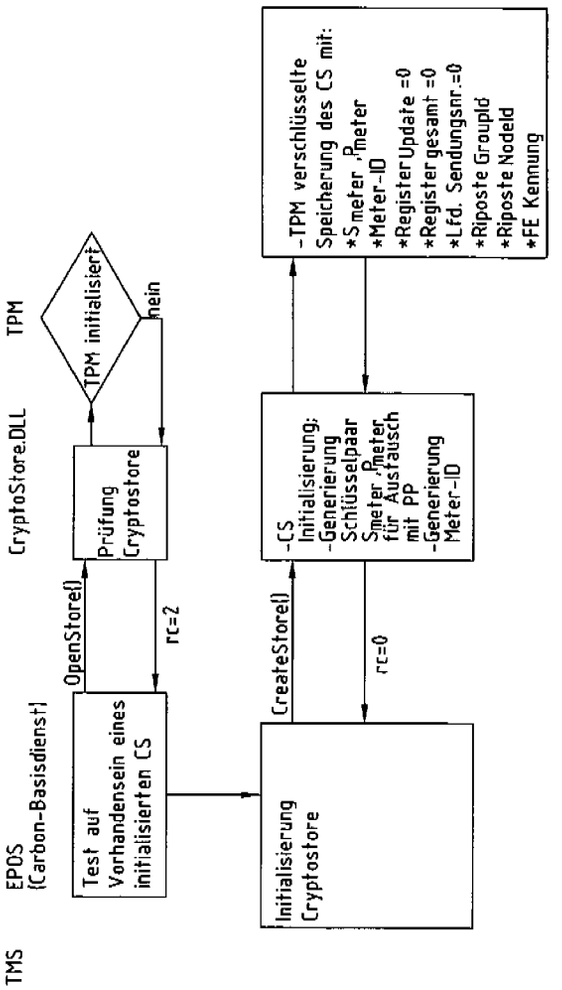
TMS
EPOS
(Carbon-Basisdienst)
CryptoStore.DLL
TPM
Test auf
Vorhandensein eines
initialisierten CS
OpenStore()
rc=2
Prüfung
Cryptostore
TPM initialisiert
nein
CreateStore()
rc=0
Initialisierung
Cryptostore
-CS
Initialisierung:
-Generierung
Schlüsselpaar
Smeter ,Pmeter
für Austausch
mit PP
-Generierung
Meter-ID
-TPM verschlüsselte
Speicherung des CS mit:
*Smeter ,Pmeter
*Meter-ID
*Register Update =0
*Register gesamt =0
*Lfd. Sendungsnr.=0
*Riposte GroupId
*Riposte NodeId
*FE Kennung

Fig.2

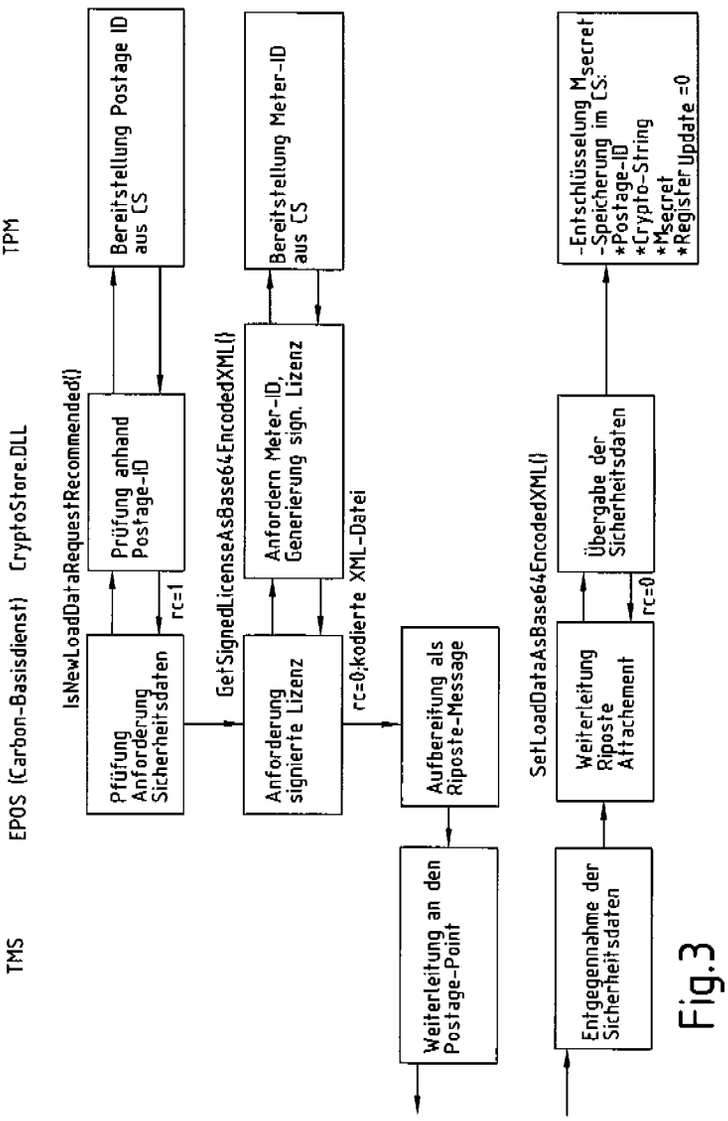
TMS
EPOS (Carbon-Basisdienst)
CryptoStore.DLL
TPM
IsNewLoadDataRequestRecommended()
Prüfung Anforderung Sicherheitsdaten
Prüfung anhand Postage-ID
Bereitstellung Postage ID aus CS
rc=1
GetSignedLicenseAsBase64EncodedXML()
Anforderung signierte Lizenz
Anfordern Meter-ID, Generierung sign. Lizenz
Bereitstellung Meter-ID aus CS
rc=0;kodierte XML-Datei
Aufbereitung als Riposte-Message
Weiterleitung an den Postage-Point
SetLoadDataAsBase64EncodedXML()
Entgegennahme der Sicherheitsdaten
Weiterleitung Riposte Attachement
Übergabe der Sicherheitsdaten
rc=0
-Entschlüsselung Msecret
-Speicherung im CS:
*Postage-ID
*Crypto-String
*Msecret
*Register Update =0

Fig.3

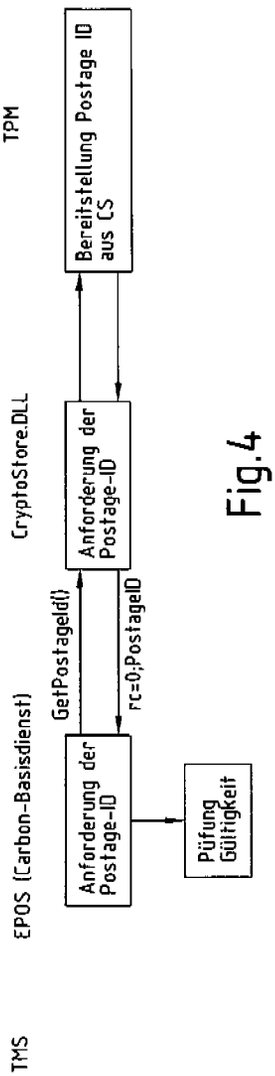
TMS
EPOS (Carbon-Basisdienst)
CryptoStore.DLL
TPM
Anforderung der Postage-ID
GetPostageId()
Anforderung der Postage-ID
Bereitstellung Postage ID aus CS
rc=0;PostageID
Püfung Gültigkeit

Fig.4

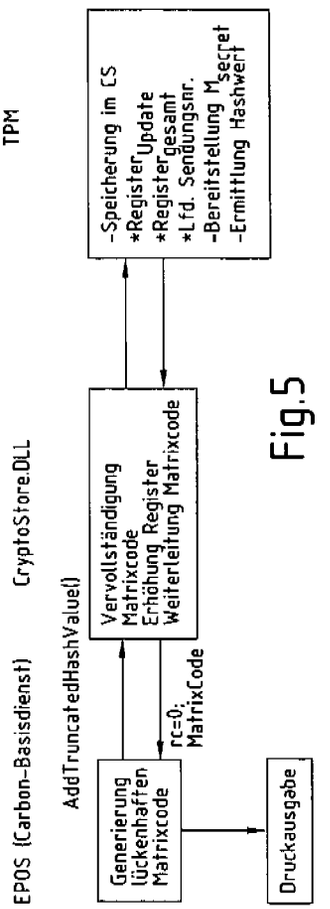
TMS
EPOS (Carbon-Basisdienst)
CryptoStore.DLL
TPM
AddTruncatedHashValue()
Generierung lückenhaften Matrixcode
rc=0; MatrixCode
Vervollständigung Matrixcode Erhöhung Register Weiterleitung Matrixcode
-Speicherung im CS
*Register_Update
*Register_gesamt
*Lfd. Sendungsnr.
-Bereitstellung M_secret
-Ermittlung Hashwert
Druckausgabe

Fig.5

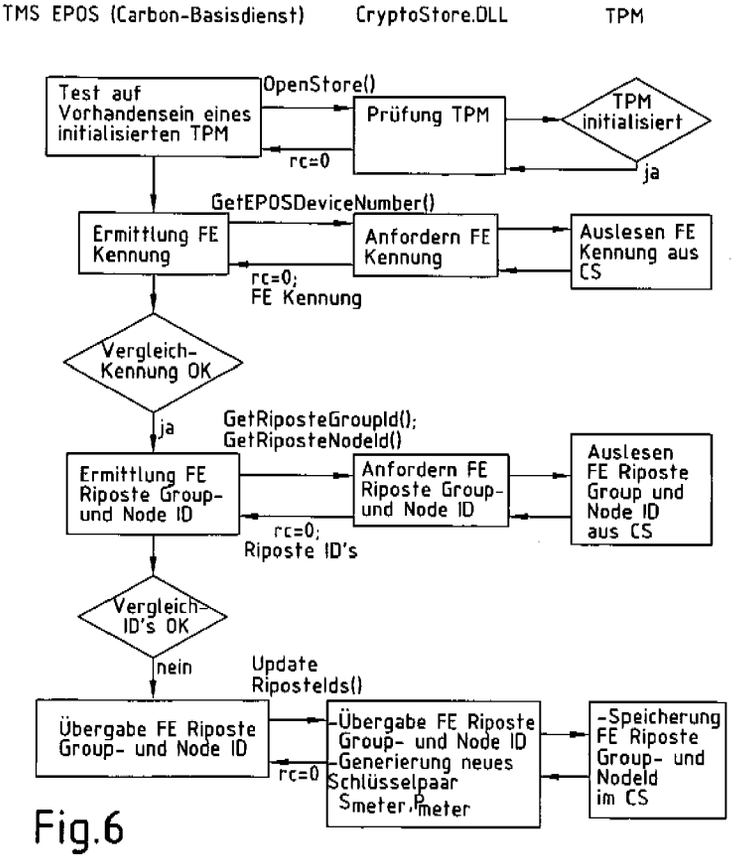
TMS EPOS (Carbon-Basisdienst)
CryptoStore.DLL
TPM
Test auf Vorhandensein eines initialisierten TPM
OpenStore()
Prüfung TPM
TPM initialisiert
rc=0
ja
GetEPOSDeviceNumber()
Ermittlung FE Kennung
Anfordern FE Kennung
Auslesen FE Kennung aus CS
rc=0; FE Kennung
Vergleich-Kennung OK
ja
GetRiposteGroupId(); GetRiposteNodeId()
Ermittlung FE Riposte Group- und Node ID
Anfordern FE Riposte Group- und Node ID
Auslesen FE Riposte Group und Node ID aus CS
rc=0; Riposte ID's
Vergleich-ID's OK
nein
Update RipsteIds()
Übergabe FE Riposte Group- und Node ID
Übergabe FE Riposte Group- und Node ID
Generierung neues Schlüsselpaar
Smeter, Pmeter
-Speicherung FE Riposte Group- und Nodeld im CS
rc=0

Fig.6

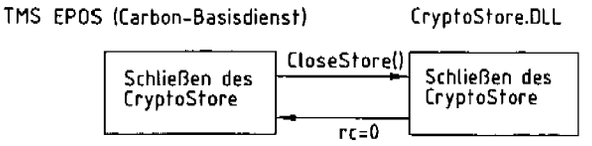
TMS EPOS (Carbon-Basisdienst)
CryptoStore.DLL
TPM
Schließen des CryptoStore
CloseStore()
Schließen des CryptoStore
rc=0

Fig.7

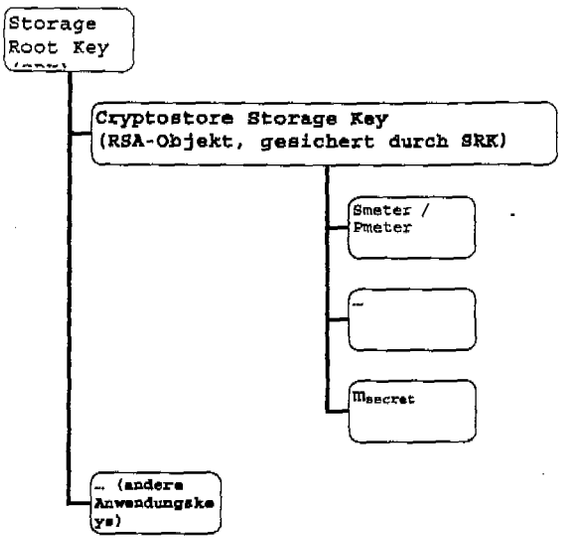
Storage
Root Key
Cryptostore Storage Key
(RSA-Objekt, gesichert durch SRK)
Smeter /
Pmeter
...
Msecret
... (andere
Anwendungske
ys)

Fig. 8

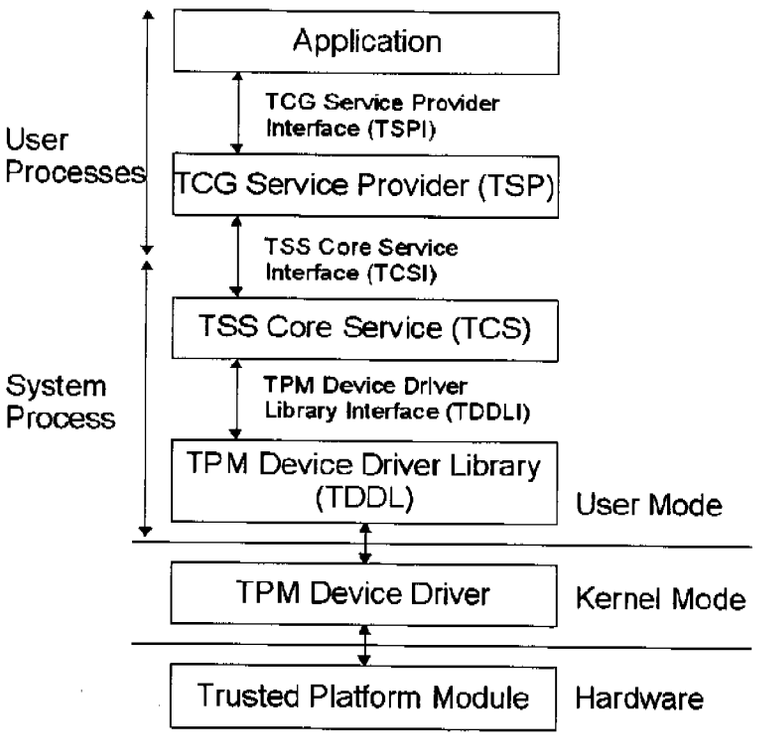
Application
TCG Service Provider Interface (TSPI)
User Processes
TCG Service Provider (TSP)
TSS Core Service Interface (TCSI)
TSS Core Service (TCS)
System Process
TPM Device Driver Library Interface (TDDLI)
TPM Device Driver Library (TDDL)
User Mode
TPM Device Driver
Kernel Mode
Trusted Platform Module
Hardware

Fig. 9

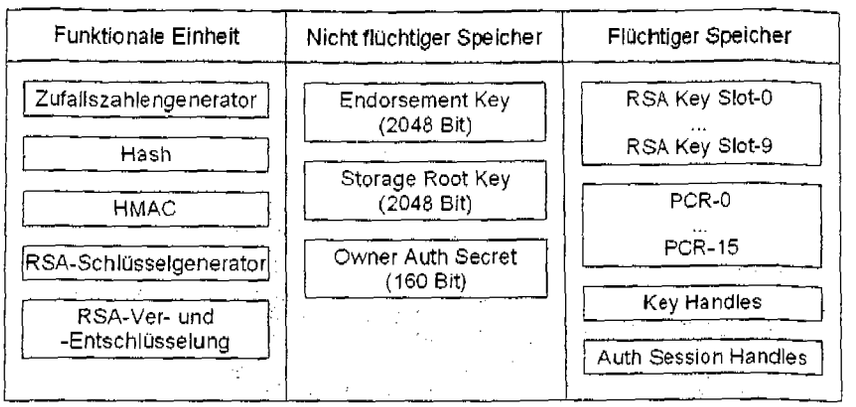
Funktionale Einheit
Nicht flüchtiger Speicher
Flüchtiger Speicher
Zufallszahlengenerator
Hash
HMAC
RSA-Schlüsselgenerator
RSA-Ver- und -Entschlüsselung
Endorsement Key (2048 Bit)
Storage Root Key (2048 Bit)
Owner Auth Secret (160 Bit)
RSA Key Slot-0
...
RSA Key Slot-9
PCR-0
...
PCR-15
Key Handles
Auth Session Handles

Fig. 10

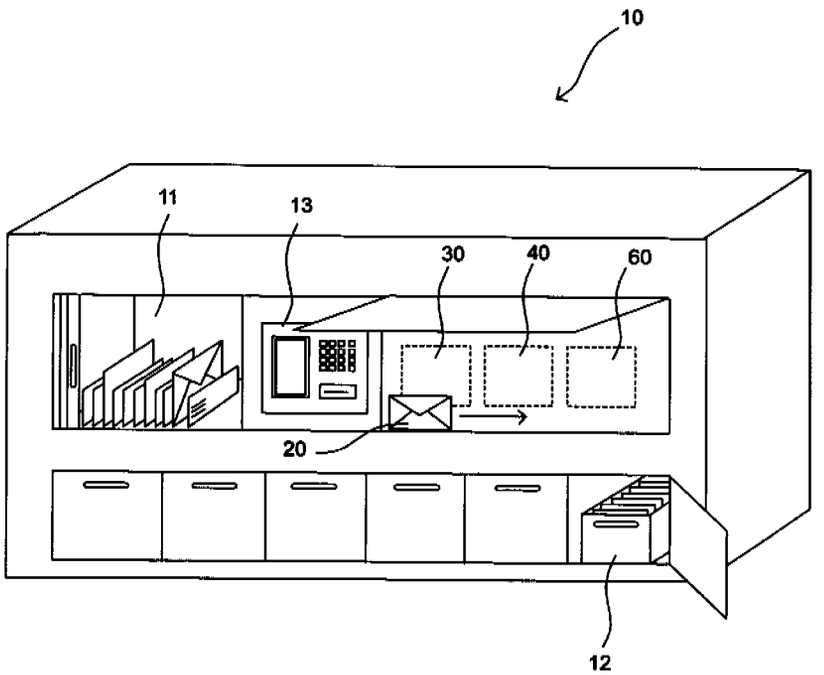

Fig. 11

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 09 00 5922

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
E	EP 2 077 528 A (DEUTSCHE POST AG [DE]) 8. Juli 2009 (2009-07-08) * das ganze Dokument *	1-13	INV. G07B17/00
D,X	DE 10 2005 006005 A1 (DEUTSCHE POST AG [DE]) 10. August 2006 (2006-08-10) * Zusammenfassung * * Absatz [0009] - Absatz [0034] *	1-13	
A	DE 44 45 526 A1 (SARTORIUS GMBH [DE]) 10. August 1995 (1995-08-10) * Zusammenfassung * * Spalte 2, Zeile 23 - Zeile 40 *	1-13	
A	US 2003/226016 A1 (CHALLENER DAVID CARROLL [US] ET AL) 4. Dezember 2003 (2003-12-04) * Zusammenfassung * * Absatz [0015] - Absatz [0016] *	1-13	
A	US 2004/221175 A1 (ATHENS G THOMAS [US] ET AL ATHENS G THOMAS [US] ET AL) 4. November 2004 (2004-11-04) * Zusammenfassung * * Absatz [0003] * * Absatz [0008] *	1-13	RECHERCHIERTE SACHGEBIETE (IPC) G07B
A	EP 1 450 144 A (SCHENCK PROCESS GMBH [DE]) 25. August 2004 (2004-08-25) * Zusammenfassung *	1-13	

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	1. September 2009	Stenger, Michael

KATEGORIE DER GENANNTEN DOKUMENTE

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

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

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

3

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 09 00 5922

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

01-09-2009

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 2077528 A	08-07-2009	WO 2009083103 A1	09-07-2009
DE 102005006005 A1	10-08-2006	CA 2596721 A1	17-08-2006
		EP 1851729 A1	07-11-2007
		WO 2006084484 A1	17-08-2006
		JP 2008530664 T	07-08-2008
		KR 20070101377 A	16-10-2007
		US 2008154721 A1	26-06-2008
DE 4445526 A1	10-08-1995	DE 9420378 U1	01-06-1995
US 2003226016 A1	04-12-2003	JP 3777170 B2	24-05-2006
		JP 2004046820 A	12-02-2004
US 2004221175 A1	04-11-2004	KEINE	
EP 1450144 A	25-08-2004	DE 10308092 A1	02-09-2004

EPO FORM P0461

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

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

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

In der Beschreibung aufgeführte Patentdokumente

- DE 102005006005 A1 **[0006]**
- DE 29613903 U1 **[0011]**
- DE 19527293 A1 **[0012]**