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

(11) **EP 1 857 981 A2**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
21.11.2007 Patentblatt 2007/47

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

(21) Anmeldenummer: **07108049.3**

(22) Anmeldetag: **11.05.2007**

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

(30) Priorität: **11.05.2006 DE 102006022315**

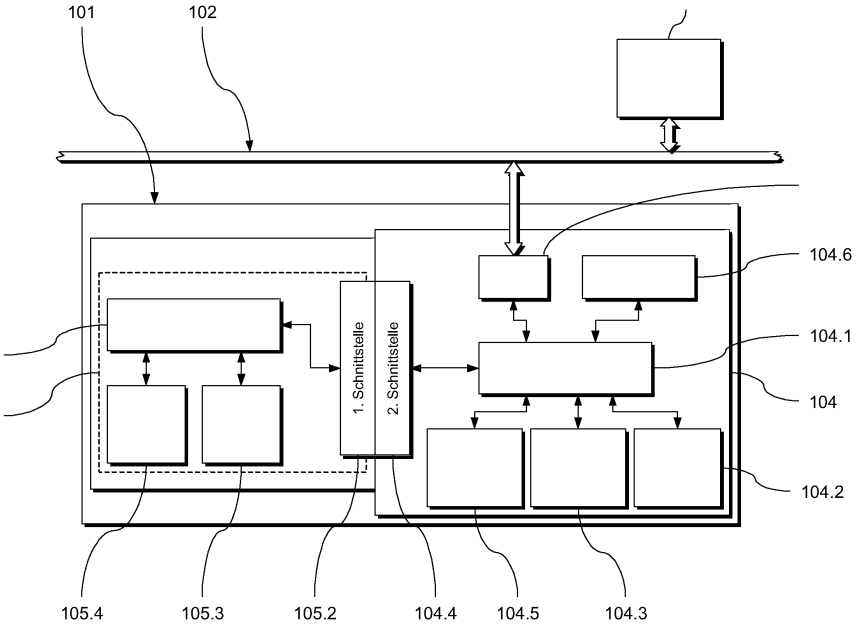
(71) Anmelder: **Francotyp-Postalia GmbH**
16547 Birkenwerder (DE)

(72) Erfinder:
- **Kampert, Werner**
  22081, Hamburg (DE)
- **Rosenau, Dirk**
  13469, Berlin (DE)

(74) Vertreter: **Cohausz & Florack**
Patent- und Rechtsanwälte
Bleichstrasse 14
40211 Düsseldorf (DE)

(54) **Anordnung und Verfahren zum Erstellen eines Frankierabdrucks**

(57) Anordnung zum Erstellen eines Frankierabdrucks, insbesondere Frankiermaschine, mit einer sicheren Verarbeitungseinheit (105.1) zum Erstellen von für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten, und einer mit der sicheren Verarbeitungseinheit (105.1) verbindbaren Speichereinrichtung (104.5) zum abgesicherten Speichern der Abrechnungsdaten, wobei die sichere Verarbeitungseinheit (105.1) in einer logisch und/oder physikalisch vor unerkanntem unautorisierten Zugriff abgesicherten sicheren Umgebung (106) angeordnet ist, und wobei die Speichereinrichtung (104.5) außerhalb der sicheren Umgebung (106) angeordnet ist, die sichere Verarbeitungseinheit (105.1) dazu ausgebildet ist, die Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form zur Verfügung zu stellen, und die sichere Verarbeitungseinheit (105.1) oder eine mit der sicheren Verarbeitungseinheit (105.1) verbindbare weitere Verarbeitungseinheit (104.1) dazu ausgebildet ist, die von der sicheren Verarbeitungseinheit (105.1) zur Verfügung gestellten Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form in die Speichereinrichtung (104.5) zu schreiben.



EP 1 857 981 A2

Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Anordnung zum Erstellen eines Frankierabdrucks, insbesondere eine Frankiermaschine, mit einer sicheren Verarbeitungseinheit zum Erstellen von für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten, und einer mit der sicheren Verarbeitungseinheit verbindbaren Speichereinrichtung zum abgesicherten Speichern der Abrechnungsdaten, wobei die sichere Verarbeitungseinheit in einer logisch und/oder physikalisch vor unerkanntem unautorisierten Zugriff abgesicherten sicheren Umgebung angeordnet ist. Sie betrifft weiterhin ein entsprechendes Verfahren, welches im Zusammenhang mit der erfindungsgemäßen Anordnung verwendet werden kann.

[0002] Heutige Frankiermaschinen werden in der Regel mit einem Sicherheitsmodul ausgestattet, welches die postalischen Register mit den Abrechnungsdaten enthält, mithin also die Abrechnung für die Frankierungen vornimmt bzw. dokumentiert, und einen Teil der mehr oder weniger komplexen Berechnungen zur Erstellung des jeweiligen Frankierabdrucks ausführt. Eine Reihe von Postbeförderern fordert die kryptographische Absicherung eines Teils der abgedruckten Daten, sodass das Sicherheitsmodul häufig als mehr oder weniger aufwändig gestaltetes und zertifiziertes Kryptographiemodul gestaltet ist.

[0003] Der Leistungsumfang der Frankiermaschine spiegelt sich - nicht zuletzt aus Gründen der Herstellungskosten - grundsätzlich im Leistungsumfang des Sicherheitsmoduls wider. So ist in der Regel in einer Frankiermaschine mit geringerem Leistungsumfang auch nur ein Sicherheitsmodul mit geringerem Leistungsumfang erforderlich, während in anspruchsvolleren Frankiermaschinen üblicherweise Sicherheitsmodule mit größerem Leistungsumfang (höhere Rechenleistung, höhere Speicherkapazität etc.) zum Einsatz kommen.

[0004] Bestimmte Postbeförderer, beispielsweise die Postbehörden bestimmter Staaten, verlangen, wenn überhaupt, einen sehr geringen Grad an Absicherung des Frankierabdrucks und/oder der Abrechnungsdaten und damit einen deutlich geringeren Leistungsumfang des Sicherheitsmoduls. Dies hat zur Konsequenz, dass die üblicherweise verwendeten Sicherheitsmodule für eine solche Anwendung in der Regel hinsichtlich ihres Leistungsumfangs überdimensioniert und damit letztlich zu teuer sind, um einen wirtschaftlichen Einsatz einer Frankiermaschine zu ermöglichen.

[0005] Der vorliegenden Erfindung liegt daher die Aufgabe zu Grunde, eine Anordnung bzw. ein Verfahren zum Erstellen eines Frankierabdrucks der eingangs genannten Art zur Verfügung zu stellen, welche bzw. welches die oben genannten Nachteile nicht oder zumindest in geringerem Maße aufweist und insbesondere den wirtschaftlichen Einsatz von Frankiermaschinen bei geringen postalischen Sicherheitsanforderungen ermöglicht.

[0006] Die vorliegende Erfindung löst diese Aufgabe mit einer Anordnung gemäß Anspruch 1. Sie löst diese Aufgabe weiterhin mit einem Verfahren gemäß Anspruch 16.

[0007] Der vorliegenden Erfindung liegt die technische Lehre zu Grunde, dass einen wirtschaftlichen Einsatz von Frankiermaschinen bei vergleichsweise geringen postalischen Sicherheitsanforderungen ermöglicht, wenn die Abrechnungsdaten nicht in dem besonders abgesicherten Bereich des Sicherheitsmoduls gespeichert werden, sondern außerhalb des Sicherheitsmoduls in einem herkömmlichen, in der Regel nicht speziell abgesicherten Speicherbereich in einer Form abgelegt werden, in der sie vor unerkannter Manipulation abgesichert sind.

[0008] Hierdurch ist es zum einen möglich, besonders einfach aufgebaute Sicherheitsmodule zu verwenden. So müssen diese Sicherheitsmodule lediglich noch die entsprechende kryptographische Funktionalität zur Verfügung stellen, während ausreichend große und entsprechend abgesicherte, teure Speicher für die Abrechnungsdaten, wie sie bei den herkömmlichen Sicherheitsmodulen vorhanden sind, nicht mehr erforderlich sind. Zudem reduziert sich hierdurch der Bauraum für das Sicherheitsmodul, sodass sich zum einen der Aufwand für eine eventuelle physikalische Absicherung dessen Sicherheitsmoduls reduziert und zum anderen das Sicherheitsmodul insgesamt kompakter und damit weniger verwundbar ausgebildet sein kann.

[0009] Bei den für die Speicherung der Abrechnungsdaten erforderlichen Speichern kann es sich um Standard-Speichermodule oder dergleichen handeln, welche entsprechend kostengünstiger sind als die üblichen möglichst kompakten Speicherbausteine für Sicherheitsmodule. Zudem müssen diese Speicher nicht in aufwändiger Weise physikalisch geschützt werden, wodurch sich der Aufwand für die Implementierung der Speicherung der Abrechnungsdaten deutlich verringert.

[0010] Ein Gegenstand der vorliegenden Erfindung ist daher eine Anordnung zum Erstellen eines Frankierabdrucks, insbesondere eine Frankiermaschine, mit einer sicheren Verarbeitungseinheit zum Erstellen von für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten und einer mit der sicheren Verarbeitungseinheit verbindbaren Speichereinrichtung zum abgesicherten Speichern der Abrechnungsdaten vorgesehen, wobei die sichere Verarbeitungseinheit in einer logisch und/oder physikalisch vor unerkanntem unautorisierten Zugriff abgesicherten sicheren Umgebung angeordnet ist. Erfindungsgemäß ist hierbei vorgesehen, dass die Speichereinrichtung außerhalb der sicheren Umgebung angeordnet ist. Die sichere Verarbeitungseinheit ist dazu ausgebildet, die Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form zur Verfügung zu stellen. Weiterhin ist die sichere Verarbeitungseinheit oder eine mit der sicheren Verarbeitungseinheit verbindbare weitere Verarbeitungseinheit dazu ausgebildet, die von der sicheren Verarbeitungseinheit zur Verfügung gestellten Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form

in die Speichereinrichtung zu schreiben.

[0011] Dadurch, dass die Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form zur Verfügung gestellt werden, kann immer noch ein ausreichendes Maß an Sicherheit erzielt werden. So kann zu jedem Zeitpunkt nachvollzogen werden, ob die in Integrität der gespeicherten Abrechnungsdaten nach wie vor vorliegt. Lässt sich anhand der Abrechnungsdaten feststellen, dass eine Manipulation der Abrechnungsdaten erfolgt ist, so können hieraus entsprechende Konsequenzen gezogen werden. Hierbei ist es nicht zwingend erforderlich, dass festgestellt werden kann, wann, von wem und/oder in welchem Umfang eine Manipulation vorgenommen wurde, um eine ausreichende Absicherung des Postbeförderers gegen Betrugsversuche zu erzielen. Dies ist letztlich nur eine Frage der mit der Erfassung der Manipulation verbundenen Sanktionen, sodass mit der vorliegenden Erfindung auf sehr kostengünstige Weise eine für die Bedürfnisse bestimmter Postbeförderer ausreichende Sicherheit der Abrechnungsdaten erzielt werden kann.

[0012] Die Absicherung der Abrechnungsdaten kann auf beliebige geeignete Weise erfolgen. Bevorzugt ist vorgesehen, dass die sichere Verarbeitungseinheit dazu ausgebildet ist, die Abrechnungsdaten durch kryptographische Mittel vor unerkannter Manipulation abzusichern. So kann beispielsweise ein Geheimnis, beispielsweise ein geheimer Schlüssel, verwendet werden, um entsprechende Sicherungsdaten zu den Abrechnungsdaten zu erzeugen, anhand derer die Integrität der Abrechnungsdaten nachvollzogen werden kann. Bei diesen Sicherungsdaten kann es sich beispielsweise um einen hinlänglich bekannten, so genannten Message Authentication Code (MAC) oder um eine ebenso hinlänglich bekannte digitale Signatur oder dergleichen handeln, welche nach beliebigen bekannten Verfahren erstellt werden.

[0013] Vorzugsweise werden digitale Signaturen verwendet, da diese auf besonders einfache Weise ohne Kenntnis des geheimen Schlüssels (Signaturschlüssel) über den zugehörigen öffentlichen Schlüssel (Verifizierungsschlüssel) verifiziert werden können, der im Rahmen einer Public-Key-Infrastruktur erlangt werden kann. Bevorzugt ist daher die sichere Verarbeitungseinheit dazu ausgebildet, die Abrechnungsdaten mit einer digitalen Signatur zu versehen.

[0014] Die sichere Verarbeitungseinheit kann grundsätzlich in beliebiger geeigneter Weise gestaltet sein. Insbesondere kann sie Bestandteil einer beliebigen übergeordneten Baueinheit sein, welche alleine oder in Kombination mit anderen Baueinheiten ein Sicherheitsmodul ausbildet. Bevorzugt ist die sichere Verarbeitungseinheit eine Komponente einer Smartcard. Hiermit lässt sich eine besonders günstige Konfiguration erzielen, da solche Smartcards bereits als vorgefertigte Einheiten mit den entsprechenden kryptographischen Funktionalitäten erhältlich sind. Es ist dann lediglich noch erforderlich, eine entsprechende einfache Konfiguration der Smartcard für den betreffenden Einsatzfall vorzunehmen, ohne hierbei jedoch Einfluss auf die Hardware der Smartcard nehmen zu müssen. So kann beispielsweise, sofern dies nicht bereits der Fall ist, eine entsprechende logische Absicherung der sicherheitsrelevanten Bereiche der Smartcard erfolgen, indem beispielsweise eine entsprechende Überprüfung der Zugriffsberechtigung auf diese sicherheitsrelevanten Bereiche implementiert wird. Gegebenenfalls kann lediglich noch eine zusätzliche physikalische Absicherung der Smartcard, beispielsweise durch eine auf die sicherheitsrelevanten Bereiche der Smartcard oder die gesamte Smartcard aufgebrachte Vergussmasse, erfolgen.

[0015] Einen wesentlichen Aspekt bei der Absicherung der Abrechnungsdaten stellt die Fähigkeit sicheren Verarbeitungseinheit dar, zuverlässig die Echtzeit zu bestimmen. Bei bevorzugten Varianten der erfindungsgemäßen Anordnung ist daher vorgesehen, dass die sichere Verarbeitungseinheit eine Zeitermittlungseinheit zur Ermittlung der Echtzeit aufweist. Vorzugsweise ist die sichere Verarbeitungseinheit derart ausgebildet, dass das Erstellen der für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten nur erfolgt, wenn die Zeitermittlungseinheit erfolgreich die Echtzeit ermittelt hat. Hierdurch kann Manipulationsversuchen zuverlässig vorgebaut werden.

[0016] Zur Ermittlung der Echtzeit kann die sichere Verarbeitungseinheit selbst eine Echtzeituhr aufweisen. Derartige Echtzeituhren müssen jedoch vergleichsweise aufwändig gestaltet sein, um eine ausreichend geringe Drift aufzuweisen. Bei besonders kostengünstigen Varianten der erfindungsgemäßen Anordnung ist daher vorgesehen, dass die Zeitermittlungseinheit dazu ausgebildet ist, zu vorgebbaren Zeitpunkten mit einer Echtzeitquelle eine Synchronisation vorzunehmen, sodass auch eine größere Ungenauigkeit bei der Ermittlung der Echtzeit in Kauf genommen werden kann, womit dann eine entsprechend einfachere Gestaltung der Zeitermittlungseinheit möglich ist.

[0017] Bevorzugt erfolgt die Synchronisation mit der Echtzeitquelle über einen entsprechend abgesicherten Kommunikationskanal, um hierbei Manipulationen vorzubeugen. Die Absicherung des Kommunikationskanals kann in beliebiger geeigneter Weise, beispielsweise über eine Verschlüsselung mit einem zuvor nach einem festgelegten Schlüsselgenerierungsprotokoll generierten geheimen Sitzungsschlüssel, erfolgen. Es sind jedoch auch beliebige andere, hinlänglich bekannte Varianten zur Absicherung der Kommunikation im Rahmen der Synchronisation der Zeitermittlungseinheit möglich.

[0018] Die Synchronisation mit der Echtzeitquelle kann auf beliebige geeignete Weise, insbesondere auf beliebigen geeigneten Wegen erfolgen. So kann beispielsweise vorgesehen sein, dass die Zeitermittlungseinheit über ein Modem oder eine andere Kommunikationseinrichtung der erfindungsgemäßen Anordnung eine entsprechende Kommunikation mit der Echtzeitquelle aufbaut. Ebenso ist es möglich, dass im Rahmen einer

bestehenden Kommunikationsverbindung zwischen der erfindungsgemäßen Anordnung und beispielsweise einer entfernten Datenzentrale von der Datenzentrale eine entsprechende Synchronisation mit der Echtzeitquelle initiiert wird.

[0019] Die Synchronisation mit der Echtzeitquelle kann weiterhin zu beliebigen geeigneten Zeitpunkten erfolgen. Sie kann beispielsweise in regelmäßigen vorgebbaren Abständen erfolgen. Ebenso kann sie beim Eintreten beliebiger vorgebbarer Ereignisse, z. B. beim Einschalten der Anordnung selbst oder bestimmter Komponenten der Anordnung, beim Stecken der Smartcard, bei jeder n-ten Kommunikation (n = 1, 2, 3...) der Anordnung mit einer entfernten Datenzentrale, bei jedem m-ten Nachladevorgang (m = 1, 2, 3...) von Guthaben etc., erfolgen.

[0020] Bei einer bevorzugten, weil besonders einfach aufgebauten Variante der erfindungsgemäßen Anordnung ist die Zeitermittlungseinheit mit einem Taktgeber zur Erzeugung von Taktimpulsen verbindbar. Die Zeitermittlungseinheit weist dann zur Ermittlung der aktuellen Echtzeit einen Zähler zur Zählung der Taktimpulse des Taktgebers seit der letzten Synchronisation mit der Echtzeitquelle auf. Bei bekannter Taktfrequenz des Taktgebers kann dann in einfacher Weise über die Zählung der Taktimpulse die Echtzeit ausgehend von dem bei der letzten Synchronisation erhaltenen Wert der Echtzeit die aktuelle Echtzeit ermittelt werden.

[0021] Bei dem Taktgeber kann es sich um eine beliebige Einheit der erfindungsgemäßen Anordnung handeln, welche mit entsprechend stabiler Frequenz Taktikimpulse liefert. Bevorzugt handelt es sich um einen Taktgeber der sicheren Verarbeitungseinheit selbst, da hierbei dann das Risiko von Manipulationen in einfacher Weise minimiert gehalten werden kann.

[0022] Um eventuellen Manipulationen der Zeitermittlungseinheit und damit der ermittelten Echtzeit durch zumindest zeitweises Anhalten des Taktgebers vorzubeugen, ist die sichere Verarbeitungseinheit bevorzugt derart ausgebildet, dass das Erstellen der für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten nur erfolgt, wenn die Zeitermittlungseinheit eine ununterbrochene Zählung von Taktimpulsen des Taktgebers seit der letzten Synchronisation mit der Echtzeitquelle erfasst hat.

[0023] Um eventuellen Manipulationen durch zumindest zeitweises Beeinflussen der Taktfrequenz des Taktgebers vorzubeugen, ist weiterhin bevorzugt vorgesehen, dass die Zeitermittlungseinheit zur Überwachung der Taktfrequenz der Taktimpulse des Taktgebers ausgebildet ist. Die sichere Verarbeitungseinheit ist dann derart ausgebildet, dass das Erstellen der für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten und/oder das Erstellen der für die Generierung des Frankierabdrucks erforderlichen Daten nur erfolgt, wenn die Zeitermittlungseinheit seit der letzten Synchronisation mit der Echtzeitquelle eine Variation der Taktfrequenz erfasst hat, die innerhalb eines vorgebbaren Toleranzbereichs liegt. Mit anderen Worten wird gegebenenfalls verhindert, dass ein Frankierabdruck generiert bzw. eine Abrechnung erfolgt, wenn eine Variation der Taktfrequenz erfasst wird, die außerhalb eines vorgegebenen Toleranzbereichs liegt.

[0024] Bei bevorzugten Varianten der erfindungsgemäßen Anordnung mit der eingangs erwähnten weiteren Verarbeitungseinheit ist die weitere Verarbeitungseinheit zur Generierung der Druckdaten des Frankierabdrucks unter Verwendung eines Datums ausgebildet. Das Datum kann dabei entweder von der Anordnung selbst vorgegeben werden und gegebenenfalls von dem Nutzer der Anordnung lediglich bestätigt werden. Ebenso kann vorgesehen sein, dass der Nutzer der Anordnung das Datum selbst eingibt. In jedem Fall erfolgt die Generierung und/oder die Verwendung der Druckdaten nur dann, wenn die Zeitermittlungseinheit das Vorliegen einer vorgebbaren Beziehung zwischen dem Datum und einer erfolgreich ermittelten aktuellen Echtzeit festgestellt hat. Hierdurch wird in einfacher Weise Manipulationen des Frankierabdrucks durch Eingabe oder Bestätigung eines falschen Datums vorgebeugt.

[0025] Bei weiteren vorteilhaften Weiterbildungen der erfindungsgemäßen Anordnung ist vorgesehen, dass die sichere Verarbeitungseinheit über eine Kommunikationsverbindung mit einer entfernten Datenzentrale verbindbar ist. Die sichere Verarbeitungseinheit ist dann auch zur Absicherung der Kommunikation mit der entfernten Datenzentrale ausgebildet. Diese Absicherung kann wie oben bereits geschildert auf beliebige geeignete Weise erfolgen. Bevorzugt erfolgt sie unter Verwendung kryptographischer Mittel, wie beispielsweise einer symmetrischen Verschlüsselung der auszutauschenden Informationen mittels eines zuvor generierten geheimen Sitzungsschlüssels. Hierdurch kann der vorhandene Leistungsumfang der sicheren Verarbeitungseinheit in vorteilhafter Weise optimal genutzt werden.

[0026] Bei weiteren bevorzugten Ausgestaltungen der erfindungsgemäßen Anordnung ist die weitere Verarbeitungseinheit eine Komponente einer Druckstation zur Erstellung des Frankierabdrucks. Die weitere Verarbeitungseinheit ist wiederum mit einer Schnittstelle der Druckstation verbunden, während die sichere Verarbeitungseinheit eine Komponente eines mit der Schnittstelle verbindbaren Sicherheitsmoduls ist. Bevorzugt ist das Sicherheitsmodul lösbar mit der Schnittstelle verbunden, sodass das Sicherheitsmodul jederzeit, bevorzugt ungehindert, mit der Schnittstelle verbunden werden kann bzw. von dieser gelöst werden kann. Hierdurch ergibt sich eine besonders variable Gestaltung, da dieselbe Druckstation gegebenenfalls einfach mit unterschiedlichen Sicherheitsmodulen betrieben werden kann. Vorzugsweise ist das Sicherheitsmodul steckbar ausgebildet, wodurch sich eine besonders einfach und variabel zu handhabende Gestaltung ergibt.

[0027] Wie bereits oben erwähnt, kann die Absicherung der sicheren Verarbeitungseinheit vor unerkannter Manipulation in beliebiger geeigneter Weise erfolgen.

Bevorzugt ist vorgesehen, dass die sichere Verarbeitungseinheit durch eine physikalische Kapselung, insbesondere eine Vergussmasse, physikalisch vor unerkanntem unautorisiertem Zugriff abgesichert ist. Zusätzlich oder alternativ ist vorgesehen, dass die sichere Verarbeitungseinheit durch einen Algorithmus zur Überprüfung der Zugriffsrechte auf die sichere Verarbeitungseinheit in hinlänglich bekannter Weise logisch vor unerkanntem unautorisierten Zugriff abgesichert ist.

[0028] Die vorliegende Erfindung betrifft weiterhin ein Verfahren zum Erstellen eines Frankierabdrucks, insbesondere mittels einer Frankiermaschine, wobei eine sichere Verarbeitungseinheit für die Abrechnung des erstellten Frankierabdrucks relevante Abrechnungsdaten erstellt und eine mit der sicheren Verarbeitungseinheit verbindbare Speichereinrichtung die Abrechnungsdaten abgesichert speichert. Dabei ist die sichere Verarbeitungseinheit in einer logisch und/oder physikalisch vor unerkanntem unautorisierten Zugriff abgesicherten sicheren Umgebung angeordnet. Erfindungsgemäß ist die Speichereinrichtung außerhalb der sicheren Umgebung angeordnet. Die sichere Verarbeitungseinheit stellt dann die Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form zur Verfügung. Die sichere Verarbeitungseinheit oder eine mit der sicheren Verarbeitungseinheit verbindbare weitere Verarbeitungseinheit schreibt dann die von der sicheren Verarbeitungseinheit zur Verfügung gestellten Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form in die Speichereinrichtung. Mit diesem erfindungsgemäßen Verfahren lassen sich die oben beschriebenen Varianten und Vorteile in demselben Maße realisieren, sodass hier lediglich auf die obigen Ausführungen Bezug genommen werden soll.

[0029] Weitere bevorzugte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen bzw. der nachstehenden Beschreibung eines bevorzugten Ausführungsbeispiels, welche auf die beigefügten Zeichnungen Bezug nimmt. Es zeigt

Figur 1 eine schematische Darstellung einer bevorzugten Ausführungsform der erfindungsgemäßen Anordnung zum Erstellen eines Frankierabdrucks, mit welcher eine bevorzugte Variante des erfindungsgemäßen Verfahrens zum Erstellen eines Frankierabdrucks durchgeführt werden kann.

[0030] Im Folgenden wird unter Bezugnahme auf die Figur 1 eine bevorzugte Ausführungsform der erfindungsgemäßen Anordnung in Form einer Frankiermaschine 101 zum Erstellen eines Frankierabdrucks beschrieben, mit welcher eine bevorzugte Variante des erfindungsgemäßen Verfahrens zum Erstellen eines Frankierabdrucks durchgeführt wird. Die Frankiermaschine 101 kann über ein Kommunikationsnetz 102 mit einer entfernten Datenzentrale 103 verbunden werden und umfasst ein Basismodul 104 und ein damit verbundenes Sicherheitsmodul 105.

[0031] Das Sicherheitsmodul 105 der Frankiermaschine 101 umfasst eine sichere Verarbeitungseinheit in Form eines ersten Prozessors 105.1, der in einer sicheren Umgebung 106 angeordnet ist. Die sichere Umgebung 106 stellt dabei eine physikalische und logische Absicherung des ersten Prozessors 105.1 vor unerkanntem unautorisiertem Zugriff zur Verfügung. Die physikalische Absicherung der sicheren Umgebung 106 wird dabei durch eine Vergussmasse zur Verfügung gestellt, in welche der erste Prozessor 105.1 sowie die weiteren Komponenten innerhalb der sicheren Umgebung 106 eingegossen sind.

[0032] Die logische Absicherung der sicheren Umgebung 106 wird durch einen Algorithmus zur Überprüfung der Zugriffsberechtigung auf die Komponenten des Sicherheitsmoduls 101 zur Verfügung gestellt. Der Zugriff auf die Komponenten des Sicherheitsmoduls 101 kann von außen nur über eine mit dem ersten Prozessor verbundene erste Schnittstelle 105.2 erfolgen, die am Übergang von der sicheren Umgebung 106 zu dem Bereich außerhalb der sicheren Umgebung 106 angeordnet ist.

[0033] Sobald versucht wird, über die erste Schnittstelle 105.2 auf den ersten Prozessor 105.1 zuzugreifen, überprüft dieser die Zugriffsberechtigung des Zugreifenden. Hierzu greift der erste Prozessor 105.1 auf ein Kryptographiemodul in Form eines ebenfalls in der sicheren Umgebung 106 angeordneten Speichers 105.3 des Sicherheitsmoduls 101 zu. Das Kryptographiemodul 105.3 beherbergt in hinlänglich bekannter Weise entsprechende Algorithmen und Daten zur Verifizierung der Zugriffsberechtigung auf das Sicherheitsmodul. Hierbei kann es sich beispielsweise im einfachsten Fall um ein gespeichertes Passwort handeln, welches der Zugreifende eingeben muss, um sich zu autorisieren. Ebenso kann es sich aber um einen entsprechenden Algorithmus zur Überprüfung digitaler Signaturen oder Zertifikate handeln, welche der Zugreifende im Rahmen seiner Autorisierung verwendet.

[0034] Das Sicherheitsmodul 104 dient in üblicher Weise dazu, die für die Frankierung erforderlichen sicherheitsrelevanten postalischen Dienste, wie beispielsweise die sichere Abrechnung der Frankierwerte aber auch die kryptographische Absicherung bestimmter postalischer Daten, zur Verfügung zu stellen.

[0035] Das Basismodul 104 dient ebenfalls in üblicher Weise zum einen dazu, den Frankierabdruck zu erzeugen. Hierzu umfasst das Basismodul 104 eine weitere Verarbeitungseinheit in Form eines zweiten Prozessors 104.1, der mit einem Druckmodul 104.2 verbunden ist. Der zweite Prozessor 104.1 steuert das Druckmodul 104.2 in hinlänglich bekannter Weise zur Generierung des Frankierabdrucks auf dem jeweiligen Poststück an. Hierzu greift der zweite Prozessor 104.1 unter anderem auf einen postalischen Speicher 104.3 des Basismoduls 104 zu, in dem ein Teil der zur Generierung des Frankierabdrucks erforderlichen Daten (z. B. Klischeedaten etc.) abgelegt ist.

[0036] Einen weiteren Teil der zur Generierung des Frankierabdrucks erforderlichen Daten erhält der zweite Prozessor 104.1 im vorliegenden Beispiel von dem Sicherheitsmodul 105. Hierbei kann es sich beispielsweise um entsprechende Prüfsummen, MACs, digitale Signaturen oder dergleichen handeln, welche der erste Prozessor 105.1 des Sicherheitsmoduls 105 über bestimmten Daten des Frankierabdrucks erzeugt. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung mit geringeren Sicherheitsanforderungen an den Frankierabdruck auch vorgesehen sein kann, dass sämtliche zur Generierung des Frankierabdrucks erforderlichen Daten ausschließlich in dem am Basismodul erstellt werden. Ebenso versteht es sich, dass bei anderen Varianten der Erfindung mit höheren Sicherheitsanforderungen an den Frankierabdruck gegebenenfalls auch ein Großteil oder sogar sämtliche zur Generierung des Frankierabdrucks erforderlichen Daten in dem Sicherheitsmodul generiert werden können.

[0037] Soll ein Frankierabdruck generiert werden, so übergibt der zweite Prozessor 104.1 zunächst über eine zweite Schnittstelle 104.4 des Basismoduls 104, die mit der erste Schnittstelle 105.2 des Sicherheitsmoduls 105 verbunden ist, entsprechende Eingabedaten an den ersten Prozessor 105.1. Nachdem der erste Prozessor in der oben bereits beschriebenen Weise die Autorisierung des zweiten Prozessors 104.1 zur Übergabe der Eingabedaten überprüft hat, verarbeitet er diese Eingabedaten nach einem vorgegebenen Schema.

[0038] Dabei überprüft der erste Prozessor 105.1 unter anderem, wie im Folgenden noch näher erläutert werden wird, ob die Eingabedaten bestimmte Bedingungen erfüllen. Ist dies der Fall, generiert der erste Prozessor 105.1 entsprechende Ausgabedaten, die er dann wieder an den zweiten Prozessor 104.1 über die Schnittstellen 105.2 und 104.4 übergibt.

[0039] Unmittelbar vor oder nach der Übergabe der Ausgabedaten an den zweiten Prozessor 104.1 generiert der erste Prozessor Abrechnungsdaten, welche zur Abrechnung des zu generieren Frankierabdrucks verwendet werden. Anders als bei herkömmlichen Frankiermaschinen werden jedoch die Abrechnungsdaten nicht in einem Abrechnungsspeicher innerhalb der sicheren Umgebung 106 gespeichert, sondern über die Schnittstellen 105.2 und 104.4 ebenfalls an den zweiten Prozessor 104.1 übergeben und von diesem in einem Abrechnungsspeicher 104.5 des Basismoduls 104, mithin also außerhalb der sicheren Umgebung 106 gespeichert.

[0040] Um unerkannte Manipulationen der Abrechnungsdaten zu verhindern, ist erfindungsgemäß vorgesehen, dass der erste Prozessor 105.1 die Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form zur Verfügung stellt. Im vorliegenden Beispiel versieht der erste Prozessor 105.1 die Abrechnungsdaten dabei mit einer digitalen Signatur, die er in hinlänglich bekannter Weise zumindest über einen Teil der Abrechnungsdaten unter Zugriff auf das Kryptographiemodul 105.3 generiert. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung auch andere hinlänglich bekannte Mechanismen zur Absicherung der Abrechnungsdaten vor unerkannter Manipulation zum Einsatz kommen können.

[0041] Dieses Vorgehen hat den Vorteil, dass das Sicherheitsmodul 105 lediglich die kryptographische Funktionalität zur Verfügung stellen muss, nicht aber einen entsprechend großen und damit teuren abgesicherten Speicherbereich zur Speicherung der Abrechnungsdaten. Hierdurch kann das Sicherheitsmodul 105 deutlich kostengünstiger gestaltet werden. Insbesondere ist es möglich, für das Sicherheitsmodul 105 wie im vorliegenden Beispiel eine einfache Smartcard zu verwenden, welche bereits standardmäßig mit entsprechender kryptographischer Funktionalität ausgestattet ist. Bei einer solchen Smartcard ist es dann gegebenenfalls lediglich erforderlich, eine entsprechende physikalische Absicherung herzustellen, wie sie oben beschrieben wurde.

[0042] Es versteht sich, dass die Abrechnungsdaten bevorzugt selbst schon in einer Form generiert werden können, welche Manipulationen vorgebeugt. So kann beispielsweise einer einfachen Manipulation durch Löschen einzelner Datensätze vorgebaut werden, indem die einzelnen Datensätze der Abrechnungsdaten mit fortlaufenden Nummern versehen werden, die ebenfalls in den abgesicherten Bereich der Abrechnungsdaten einbezogen werden.

[0043] Weiterhin versteht es sich, dass nicht nur im Zuge einer Frankierung in entsprechend abgesicherte Abrechnungsdaten in dem Abrechnungsspeicher 104.5 abgelegt werden. Vielmehr umfassen die Abrechnungsdaten im Abrechnungsspeicher 104.5 natürlich auch Daten, welche das aktuell verfügbare Guthaben repräsentieren. Diese Daten werden in einem Nachladevorgang im Zuge einer Kommunikation zwischen der Frankiermaschine 101 und der entfernten Datenzentrale 103 über das Sicherheitsmodul 105 in den Abrechnungsspeicher 104.5 eingebracht. Dabei können die Guthabendaten schon von der entfernten Datenzentrale 103 in entsprechender Weise abgesichert sein. Bevorzugt ist jedoch vorgesehen, dass die von der Datenzentrale 103 übermittelten Guthabendaten zunächst in dem Sicherheitsmodul 105 entsprechend aufbereitet und abgesichert werden und erst dann in dem Abrechnungsspeicher 104.5 abgelegt werden.

[0044] Im vorliegenden Beispiel ist das korrekte Datum der Frankierung von wesentlicher Bedeutung für die Sicherheit des Abrechnungsvorgangs. Soll ein Frankierabdruck generiert werden, so gibt der zweite Prozessor 104.1 des Basismoduls 104 mit den Eingabedaten ein entsprechendes Datum an den ersten Prozessor 105.1 weiter. Dieses Datum kann entweder standardmäßig von einer - in Figur 1 nicht dargestellten - Uhr des Basismoduls 104 vorgegeben werden. Gegebenenfalls kann vorgesehen sein, dass der Benutzer der Frankiermaschine 101 dieses Datum bestätigen muss. Ebenso kann aber vorgesehen sein, dass der Nutzer der Frankiermaschine 101 selbst ein entsprechendes Datum über eine Benut-

zerschnittstelle 104.6, beispielsweise eine Tastatur, an den zweiten Prozessor 104.1 übergeben kann, welches dann verwendet wird.

[0045] Wie bereits oben angedeutet, überprüft das Sicherheitsmodul 105 im vorliegenden Beispiel, ob das übergebene Datum in der Vergangenheit liegt. Ist dies der Fall, nimmt das Sicherheitsmodul weder die Generierung der für die Erstellung des Frankierabdrucks erforderlichen Daten noch die Generierung der entsprechenden Abrechnungsdaten vor. Mit anderen Worten werden diese Daten nur generiert, wenn das übergebene Datum dem aktuellen Datum im Sicherheitsmodul 105 entspricht oder ein Datum in der Zukunft repräsentiert. Hierbei kann vorgesehen sein, dass die Zeitspanne, die das übergebene Datum maximal in der Zukunft liegen darf, begrenzt ist.

[0046] Um diese Überprüfung des von dem zweiten Prozessor 104.1 übergebenen Datums vornehmen zu können, weist das Sicherheitsmodul 105 eine Zeitermittlungseinheit in Form eines Zeitermittlungsmoduls 105.4 auf, welches unabhängig von dem Basismodul 104 die Echtzeit ermittelt.

[0047] Hierzu wird das Zeitermittlungsmodul 105.4 zunächst bei Eintreten vorgegebener Ereignisse mit einer Echtzeitquelle der entfernten Datenzentrale 103 synchronisiert. Die Ereignisse, welche die Synchronisation mit der Echtzeitquelle auslösen, können beliebig vorgegeben werden. So kann beispielsweise vorgesehen sein, dass die Synchronisation jedes Mal erfolgt, wenn die Frankiermaschine 101 mittels eines mit dem zweiten Prozessor 104.1 verbunden Modems 104.7 erfolgreich eine Kommunikation mit der entfernten Datenzentrale 103 aufgebaut hat. Ebenso kann vorgesehen sein, dass eine solche Kommunikation mit der entfernten Datenzentrale 103 durch das Sicherheitsmodul 105 nach Ablauf einer vorgegebenen Zeitspanne seit der letzten Synchronisation des Zeitermittlungsmoduls 105.4 mit der Echtzeitquelle der entfernten Datenzentrale 103 erzwungen bzw. automatisch ausgelöst wird.

[0048] Um Manipulationen bei der Synchronisation mit der Echtzeitquelle entgegenzuwirken, wird die Kommunikation mit der Datenzentrale 103, innerhalb derer die Synchronisation erfolgt, durch den ersten Prozessor 105.1 unter Zugriff auf das Kryptographiemodul 105.3 entsprechend in hinlänglich bekannter Weise, beispielsweise durch Verwendung einer Verschlüsselung der ausgetauschten Daten mit einem geheimen Sitzungsschlüssel, abgesichert.

[0049] Sobald das Zeitermittlungsmodul 105.4 im Rahmen der Synchronisation mit der Echtzeitquelle der entfernten Datenzentrale 103 die aktuelle Echtzeit erhalten hat, beginnt das Zeitermittlungsmodul 105.4 mit der Zählung der Taktimpulse eines Taktgebers des ersten Prozessors 105.1. Dabei überwacht das Zeitermittlungsmodul 105.4 unter anderem auch die Taktfrequenz des Taktgebers zum einen daraufhin, ob Abweichungen der Taktfrequenz von einer Soll-Taktfrequenz innerhalb eines bestimmten Toleranzbereichs liegen. Weiterhin überwacht das Zeitermittlungsmodul 105.4 die lückenlose Taktung des Taktgebers. Mit anderen Worten überprüft das Zeitermittlungsmodul 105.4 also, ob die Taktung des Taktgebers zeitweise aussetzt.

[0050] Liegt die Taktfrequenz des Taktgebers innerhalb des vorgegebenen Toleranzbereichs und liegt eine lückenlose Taktung seit der letzten Synchronisation mit der Echtzeitquelle vor, so ermittelt das Zeitermittlungsmodul 105.4 aus der mit der letzten Synchronisation übergebenen Echtzeit, der Anzahl der Takte und der Taktfrequenz des Taktgebers die aktuelle Echtzeit. Liegen diese Voraussetzungen nicht vor, wird festgestellt, dass keine korrekte Echtzeit zu ermitteln ist und die Durchführung weiterer Operationen im Zusammenhang mit der Generierung eines Frankierabdrucks verweigert. In diesem Fall kann eine entsprechende Fehlermeldung an den Benutzer der Frankiermaschine 101 ausgegeben werden oder gegebenenfalls eine neue Synchronisation mit der Echtzeitquelle erzwungen werden.

[0051] Mit den beschriebenen Zeitermittlungsmodul 105.4 kann auf besonders einfache Weise eine ausreichend zuverlässige Ermittlung der Echtzeit erfolgen. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung auch vorgesehen sein kann, dass das Sicherheitsmodul eine Echtzeituhr aufweist, welche

[0052] Konnte das Zeitermittlungsmodul 105.4 die Echtzeit erfolgreich ermitteln, vergleicht sie diese mit dem übergebenen Datum. Entspricht das übergebene Datum den oben geschilderten Vorgaben, generiert der erste Prozessor 105.1 in der oben beschriebenen Weise die für die Erstellung des Frankierabdrucks erforderlichen Daten sowie die Abrechnungsdaten und übergibt diese an den zweiten Prozessor 104.1 zur weiteren Verarbeitung. Andernfalls verweigert der erste Prozessor 105.1 die Durchführung weiterer Operationen im Zusammenhang mit der Generierung und Abrechnung des Frankierabdrucks. Insbesondere werden weder die für die Erstellung des Frankierabdrucks erforderlichen Daten noch entsprechende Abrechnungsdaten generiert.

[0053] Es versteht sich, dass die kryptographischen Leistungsmerkmale des Sicherheitsmoduls 105 von der Frankiermaschine 101 noch in weiterem Umfang genutzt werden können. So kann das Sicherheitsmodul 105 natürlich nicht nur die Kommunikation während der Synchronisation mit der Echtzeitquelle der entfernten Datenzentrale 103 absichern. Vielmehr kann eine solche Absicherung auch für jede beliebige andere Kommunikation zwischen der Frankiermaschine und einer externen Einheit, beispielsweise der entfernten Datenzentrale 103 beim Nachladen von Guthaben oder einem Servicerechner eines Servicetechnikers etc., in der beschriebenen Weise erfolgen. Weiterhin kann das Sicherheitsmodul 105 natürlich in hinlänglich bekannter Weise dazu verwendet werden, die Integrität und Authentizität bestimmter übermittelter Daten zu verifizieren oder selbst für eine entsprechende Authentifizierung zu sorgen. So kann das Sicherheitsmodul 105 beispielsweise genutzt werden, um digitale Signaturen oder ähnlich wirkende Daten zu

verifizieren bzw. zu erstellen.

[0054] Das Sicherheitsmodul 105 ist, wie oben bereits erwähnt wurde, im vorliegenden Beispiel als einfache Smartcard ausgeführt, die zusätzlich noch mit einer physikalischen Absicherung in Form einer Vergussmasse versehen ist, in welcher die Komponenten des Sicherheitsmoduls eingebettet sind. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung auch vorgesehen sein kann, dass nur die entsprechenden in einer sicheren Umgebung anzuordnenden sicherheitsrelevanten Teile einer solchen Smartcard mit einer entsprechenden physikalischen Kapselung versehen sind, während andere Bereiche mehr oder weniger frei zugänglich sind. In diesem Fall ist dann lediglich darauf zu achten, dass für sämtliche möglichen Zugänge zu den sicherheitsrelevanten Komponenten eine entsprechende logische Absicherung wirksam ist.

[0055] Im vorliegenden Beispiel ist das Sicherheitsmodul 105 seine einfache Steckkarte, die in die zweite Schnittstelle 104.4 eingesteckt ist. Dabei kann die zweite Schnittstelle 104.4 frei zugänglich sein, sodass ohne weiteres beliebige Sicherheitsmodule 105 eingesteckt werden können. Dies hat den Vorteil, dass das Basismodul 104 gegebenenfalls frei in Verbindung mit mehreren unterschiedlichen Sicherheitsmodulen betrieben werden kann.

[0056] Hierbei ist es insbesondere möglich, die Frankiermaschine 101 mit den Sicherheitsmodulen unterschiedlicher Postbeförderer zu nutzen. Gegebenenfalls kann in diesem Fall dann vorgesehen sein, dass das Sicherheitsmodul 105 in einem entsprechenden Speicher die entsprechenden Vorschriften (z. B. Algorithmen und Daten etc.) umfasst, nach denen der Frankierabdruck für den betreffenden Postbeförderer zu generieren ist.

[0057] Ist dies der Fall, versteht es sich aber, dass bevorzugt für jedes Sicherheitsmodul ein gesonderter Bereich des Abrechnungsspeichers 104.5 vorgesehen ist. Zusätzlich oder alternativ kann aber auch vorgesehen sein, dass die Abrechnungsdaten in diesem Fall in ihrem abgesicherten Bereich zur Vereinfachung der Zuordnung zu dem jeweiligen Sicherheitsmodul eine eindeutige Identifikation des jeweiligen Sicherheitsmoduls, von welchem sie generiert wurden, umfassen. Bei einer Reihe von Sicherungsmechanismen ist diese Zuordnung ohnehin schon möglich, da die zur Absicherung verwendeten geheimen Daten (z. B. Signaturschlüssel etc.) ohnehin eindeutig einem einzigen Sicherheitsmodul zugeordnet sind.

[0058] Ebenso versteht es sich allerdings, dass bei anderen Varianten der Erfindung auch vorgesehen sein kann, dass das Sicherheitsmodul als fest eingebaute Komponente der Frankiermaschine ausgebildet ist.

[0059] Es sei and dieser Stelle erwähnt, dass die vorstehend beschriebenen Speicher des Sicherheitsmoduls 105 bzw. des Basismoduls 104 alle oder zum Teil sowohl als separate Speichermodule als auch lediglich als einzelne Speicherbereiche eines einzigen Speichermoduls ausgebildet sein können.

Patentansprüche

1. Anordnung zum Erstellen eines Frankierabdrucks, insbesondere Frankiermaschine, mit

   - einer sicheren Verarbeitungseinheit (105.1) zum Erstellen von für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten, und
   - einer mit der sicheren Verarbeitungseinheit (105.1) verbindbaren Speichereinrichtung (104.5) zum abgesicherten Speichern der Abrechnungsdaten, wobei
   - die sichere Verarbeitungseinheit (105.1) in einer logisch und/oder physikalisch vor unerkanntem unautorisierten Zugriff abgesicherten sicheren Umgebung (106) angeordnet ist,

   dadurch gekennzeichnet, dass

   - die Speichereinrichtung (104.5) außerhalb der sicheren Umgebung (106) angeordnet ist,
   - die sichere Verarbeitungseinheit (105.1) dazu ausgebildet ist, die Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form zur Verfügung zu stellen, und
   - die sichere Verarbeitungseinheit (105.1) oder eine mit der sicheren Verarbeitungseinheit (105.1) verbindbare weitere Verarbeitungseinheit (104.1) dazu ausgebildet ist, die von der sicheren Verarbeitungseinheit (105.1) zur Verfügung gestellten Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form in die Speichereinrichtung (104.5) zu schreiben.

2. Anordnung nach Anspruch 1, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) dazu ausgebildet ist, die Abrechnungsdaten durch kryptographische Mittel, insbesondere unter Verwendung eines Geheimnisses, vor unerkannter Manipulation abzusichern.

3. Anordnung nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) dazu ausgebildet ist, die Abrechnungsdaten mit einer digitalen Signatur zu versehen.

4. Anordnung nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) eine Komponente einer Smartcard (105) ist.

5. Anordnung nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) eine Zeitermittlungseinheit (105.4) zur Ermittlung der Echtzeit aufweist.

6. Anordnung nach Anspruch 5, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) derart ausgebildet ist, dass das Erstellen der für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten nur erfolgt, wenn die Zeitermittlungseinheit (105.4) erfolgreich die Echtzeit ermittelt hat.

7. Anordnung nach Anspruch 5 oder 6, **dadurch gekennzeichnet, dass** die Zeitermittlungseinheit (105.4) dazu ausgebildet ist, zu vorgebbaren Zeitpunkten mit einer Echtzeitquelle eine, vorzugsweise durch kryptographische Mittel abgesicherte, Synchronisation vorzunehmen.

8. Anordnung nach Anspruch 7, **dadurch gekennzeichnet, dass**

   - die Zeitermittlungseinheit (105.4) mit einem Taktgeber zur Erzeugung von Taktimpulsen, insbesondere mit einem Taktgeber der sicheren Verarbeitungseinheit (105.1), verbindbar ist und
   - die Zeitermittlungseinheit (105.4) zur Ermittlung der aktuellen Echtzeit einen Zähler zur Zählung der Taktimpulse des Taktgebers seit der letzten Synchronisation mit der Echtzeitquelle aufweist.

9. Anordnung nach Anspruch 8, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) derart ausgebildet ist, dass das Erstellen der für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten nur erfolgt, wenn die Zeitermittlungseinheit (105.4) eine ununterbrochene Zählung von Taktimpulsen des Taktgebers seit der letzten Synchronisation mit der Echtzeitquelle erfasst hat.

10. Anordnung nach Anspruch 9, **dadurch gekennzeichnet, dass**

    - die Zeitermittlungseinheit (105.4) zur Überwachung der Taktfrequenz der Taktimpulse des Taktgebers ausgebildet ist und
    - die sichere Verarbeitungseinheit (105.1) derart ausgebildet ist, dass das Erstellen der für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten nur erfolgt, wenn die Zeitermittlungseinheit seit der letzten Synchronisation mit der Echtzeitquelle eine Variation der Taktfrequenz erfasst hat, die innerhalb eines vorgebbaren Toleranzbereichs liegt.

11. Anordnung nach einem der Ansprüche 5 bis 10, **dadurch gekennzeichnet, dass** die weitere Verarbeitungseinheit (104.1) zur Generierung der Druckdaten des Frankierabdrucks unter Verwendung eines, insbesondere von einem Nutzer eingegebenen, Datums derart ausgebildet ist, dass die Generierung und/oder Verwendung der Druckdaten nur erfolgt, wenn die Zeitermittlungseinheit (105.4) das Vorliegen einer vorgebbaren Beziehung zwischen dem Datum und einer erfolgreich ermittelten aktuellen Echtzeit festgestellt hat.

12. Anordnung nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass**

    - die sichere Verarbeitungseinheit (105.1) über eine Kommunikationsverbindung mit einer entfernten Datenzentrale (103) verbindbar ist und
    - die sichere Verarbeitungseinheit (105.1) zur Absicherung der Kommunikation mit der entfernten Datenzentrale (103) unter Verwendung kryptographischer Mittel ausgebildet ist.

13. Anordnung nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass**

    - die weitere Verarbeitungseinheit (104.1) eine Komponente einer Druckstation (104) zur Erstellung des Frankierabdrucks ist,
    - die weitere Verarbeitungseinheit (104.1) mit einer Schnittstelle (104.4) der Druckstation (104) verbunden ist und
    - die sichere Verarbeitungseinheit (105.1) eine Komponente eines, insbesondere ungehindert lösbar, mit der Schnittstelle (104.4) verbindbaren Sicherheitsmoduls (105) ist.

14. Anordnung nach Anspruch 13, **dadurch gekennzeichnet, dass** das Sicherheitsmodul (105) steckbar ausgebildet ist.

15. Anordnung nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1)

    - durch eine physikalische Kapselung, insbesondere eine Vergussmasse, physikalisch vor unerkanntem unautorisiertem Zugriff abgesichert ist

    und/oder

    - durch einen Algorithmus zur Überprüfung der Zugriffsrechte auf die sichere Verarbeitungseinheit logisch vor unerkanntem unautorisierten Zugriff abgesichert ist.

16. Verfahren zum Erstellen eines Frankierabdrucks, insbesondere mittels einer Frankiermaschine, wobei

    - eine sichere Verarbeitungseinheit (105.1) für die Abrechnung des erstellten Frankierabdrucks relevante Abrechnungsdaten erstellt,

und

- eine mit der sicheren Verarbeitungseinheit (105.1) verbindbare Speichereinrichtung (104.5) die Abrechnungsdaten abgesichert speichert, wobei
- die sichere Verarbeitungseinheit (105.1) in einer logisch und/oder physikalisch vor unerkanntem unautorisierten Zugriff abgesicherten sicheren Umgebung (106) angeordnet ist,

dadurch gekennzeichnet, dass

- die Speichereinrichtung (104.5) außerhalb der sicheren Umgebung (106) angeordnet ist,
- die sichere Verarbeitungseinheit (105.1) die Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form zur Verfügung stellt, und
- die sichere Verarbeitungseinheit (105.1) oder eine mit der sicheren Verarbeitungseinheit (105.1) verbindbare weitere Verarbeitungseinheit (104.1) die von der sicheren Verarbeitungseinheit (105.1) zur Verfügung gestellten Abrechnungsdaten in einer vor unerkannter Manipulation abgesicherten Form in die Speichereinrichtung (104.5) schreibt.

17. Verfahren nach Anspruch 16, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) die Abrechnungsdaten durch kryptographische Mittel, insbesondere unter Verwendung eines Geheimnisses, vor unerkannter Manipulation absichert.

18. Verfahren nach Anspruch 16 oder 17, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) die Abrechnungsdaten mit einer digitalen Signatur versieht.

19. Verfahren nach einem der Ansprüche 16 bis 18, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) eine Komponente einer Smartcard ist.

20. Verfahren nach einem der Ansprüche 16 bis 19, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) über eine Zeitermittlungseinheit (105.4) die Echtzeit ermittelt.

21. Verfahren nach Anspruch 20, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) die für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten nur erstellt, wenn die Zeitermittlungseinheit (105.4) erfolgreich die Echtzeit ermittelt hat.

22. Verfahren nach Anspruch 20 oder 21, **dadurch gekennzeichnet, dass** die Zeitermittlungseinheit (105.4) zu vorgebbaren Zeitpunkten mit einer Echtzeitquelle eine, vorzugsweise durch kryptographische Mittel abgesicherte, Synchronisation vornimmt.

23. Verfahren nach Anspruch 22, **dadurch gekennzeichnet, dass**

- die Zeitermittlungseinheit (105.4) mit einem Taktgeber zur Erzeugung von Taktimpulsen, insbesondere mit einem Taktgeber der sicheren Verarbeitungseinheit(105.1), verbindbar ist und
- die Zeitermittlungseinheit (105.4) zur Ermittlung der aktuellen Echtzeit die Taktimpulse des Taktgebers seit der letzten Synchronisation mit der Echtzeitquelle zählt.

24. Verfahren nach Anspruch 23, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1) Die für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten nur erstellt, wenn die Zeitermittlungseinheit (105.4) eine ununterbrochene Zählung von Taktimpulsen des Taktgebers seit der letzten Synchronisation mit der Echtzeitquelle erfasst hat.

25. Verfahren nach Anspruch 24, **dadurch gekennzeichnet, dass**

- die Zeitermittlungseinheit (105.4) die Taktfrequenz der Taktimpulse des Taktgebers überwacht und
- die sichere Verarbeitungseinheit (105.1) die für die Abrechnung des erstellten Frankierabdrucks relevanten Abrechnungsdaten nur erstellt, wenn die Zeitermittlungseinheit (105.4) seit der letzten Synchronisation mit der Echtzeitquelle eine Variation der Taktfrequenz erfasst hat, die innerhalb eines vorgebbaren Toleranzbereichs liegt.

26. Verfahren nach einem der Ansprüche 20 bis 25, **dadurch gekennzeichnet, dass** die weitere Verarbeitungseinheit (104.1) die Druckdaten des Frankierabdrucks unter Verwendung eines, insbesondere von einem Nutzer eingegebenen, Datums generiert, wobei die Generierung und/oder Verwendung der Druckdaten nur erfolgt, wenn die Zeitermittlungseinheit (105.4) das Vorliegen einer vorgebbaren Beziehung zwischen dem Datum und einer erfolgreich ermittelten aktuellen Echtzeit festgestellt hat.

27. Verfahren nach einem der Ansprüche 16 bis 26, **dadurch gekennzeichnet, dass**

- die sichere Verarbeitungseinheit (105.1) über eine Kommunikationsverbindung mit einer entfernten Datenzentrale (103) verbunden wird und

- die sichere Verarbeitungseinheit (105.1) die Kommunikation mit der entfernten Datenzentrale (103) unter Verwendung kryptographischer Mittel absichert.

28. Verfahren nach einem der Ansprüche 16 bis 27, **dadurch gekennzeichnet, dass**

- die weitere Verarbeitungseinheit (104.1) eine Komponente einer Druckstation (104) zur Erstellung des Frankierabdrucks ist,
- die weitere Verarbeitungseinheit (104.1) mit einer Schnittstelle (104.4) der Druckstation (104) verbunden wird und
- die sichere Verarbeitungseinheit (105.1) eine Komponente eines Sicherheitsmoduls (105) ist, das, insbesondere ungehindert lösbar, mit der Schnittstelle (104.4) verbunden wird.

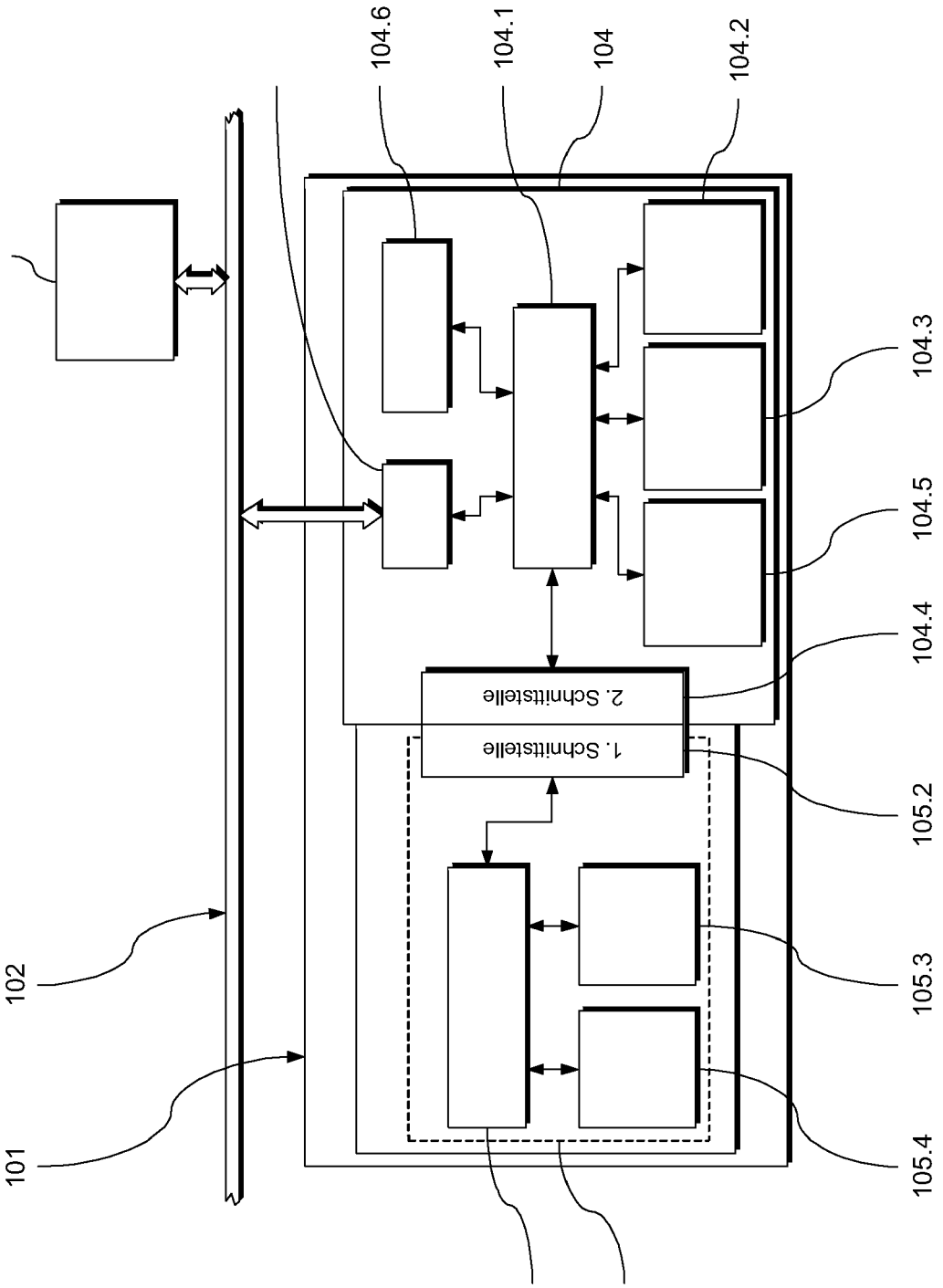
29. Verfahren nach Anspruch 28, **dadurch gekennzeichnet, dass** das Sicherheitsmodul (105) über eine Steckverbindung mit der Druckstation (104) verbunden wird.

30. Verfahren nach einem der Ansprüche 16 bis 29, **dadurch gekennzeichnet, dass** die sichere Verarbeitungseinheit (105.1)

- durch eine physikalische Kapselung, insbesondere eine Vergussmasse, physikalisch vor unerkanntem unautorisiertem Zugriff abgesichert ist

und/oder

- durch einen Algorithmus zur Überprüfung der Zugriffsrechte auf die sichere Verarbeitungseinheit logisch vor unerkanntem unautorisierten Zugriff abgesichert ist.


104.6
104.1
104
104.2
104.3
104.5
104.4
2. Schnittstelle
1. Schnittstelle
105.2
105.3
105.4
102
101