

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 150 256 A1

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:

31.10.2001 Patentblatt 2001/44

(51) Int Cl.7: G07B 17/00

(21) Anmeldenummer: 01104610.9

(22) Anmeldetag: 23.02.2001

(84) Benannte Vertragsstaaten:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR

Benannte Erstreckungsstaaten:

AL LT LV MK RO SI

(30) Priorität: 28.04.2000 DE 10020904

(71) Anmelder: Francotyp-Postalia

Aktiengesellschaft & Co.

16547 Birkenwerder (DE)

(72) Erfinder: Bleumer, Gerrit

16727 Velten (DE)

(74) Vertreter: Eisenführ, Speiser & Partner

Martinistrasse 24

28195 Bremen (DE)

(54) Verfahren zur sicheren Distribution von Sicherheitsmodulen

(57) Die Erfindung betrifft ein Verfahren und ein Distributionssystem zur sicheren Distribution von Sicherheitsmodulen, insbesondere für Frankiermaschinen. Zum Schutz vor Manipulationen von Sicherheitsmodulen wird durch die Erfindung ein Verfahren und ein Distributionssystem geschaffen, bei dem unter allen Umständen, d. h. selbst bei umfassender Unterwanderung der kryptographischen Initialisierung am Produktionsort, gewährleistet wird, dass nur Geräte mit solchen Sicherheitsmodulen vom Kunden in Betrieb genommen werden können, deren Schlüssel nicht kompromittiert sind. Dazu ist erfindungsgemäß die Erzeugung und

Überprüfung von Markierungen ggf. in Kombination mit Zertifikaten vorgesehen. Eine erste Markierung (9) der versandfertigen Verpackung (8) des Sicherheitsmoduls (7) erfolgt am Herstellerort (1) nach einer ersten kryptographischen Initialisierung, wobei die erste Markierung (9) vorzugsweise ein auf ein erstes Label gedruckter öffentlicher Schlüssel ist. Eine zweite Markierung (13) erfolgt in entfernt vom Herstellerort am Einfuhrpunkt (2) beim Registrieren der Verpackung (8) und ermöglicht eine Identifikation beim späteren Registrieren des Gerätes, ausgelöst von dem am Einsatzort befindlichen Benutzer (3) vor dem Laden von angeforderten Daten in die Frankiermaschine.

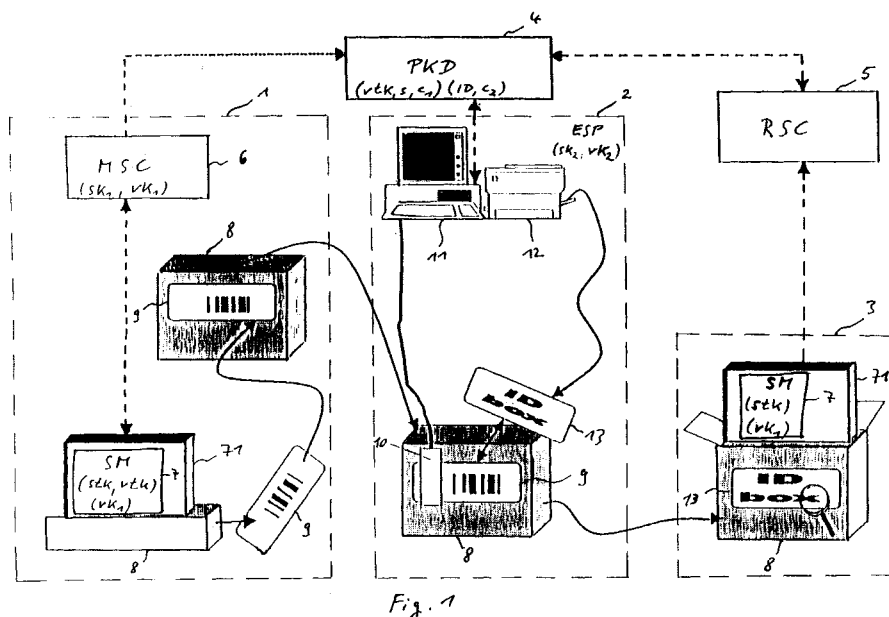


Fig. 1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur sicheren Distribution von Sicherheitsmodulen, insbesondere für Frankiermaschinen, von einem Herstellerort über einen Verteilerort zu einem Benutzerort. Außerdem betrifft die Erfindung ein Distributionssystem zur sicheren Distribution von Sicherheitsmodulen.

[0002] Sicherheitsmodule, insbesondere eingebettete Systeme, können wie Mikroprozessoren und Speicherbausteine in großen Stückzahlen an zentralen Orten gefertigt werden, die für Massenproduktion besonders geeignet sind. Solche Sicherheitsmodule kommen in verschiedenen Geräten zum Einsatz, insbesondere in solchen Geräten, die bestimmte Werte ihrer Benutzer verwahren. Beispiele sind Frankiermaschinen, Registrierkassen, elektronische Geldbörsen, PCs, Notebooks, Palmtops und Mobiltelefone. Wenn diese Geräte ebenfalls Massenware sind, so werden sie vom Kunden, dem späteren Benutzer, am bequemsten zusammen mit dem zugehörigen Sicherheitsmodul direkt durch den Versandhandel oder Einzelhandel bezogen, jedenfalls zumeist ohne weiteren Kontakt mit dem Hersteller der Sicherheitsmodule aufzunehmen.

[0003] Um eine sichere kryptographische Initialisierung und eine effiziente Distribution der Sicherheitsmodule zu gewährleisten, sollte die Initialisierung am Produktionsort erfolgen. Andernfalls müsste es zentrale oder dezentrale Initialisierungs-Center geben, die sehr kostenaufwendig wären. Im allgemeinen werden die Produktionsorte für Massenprodukte und die Sitze ihrer späteren Betreiber, die für Schäden von Schlüsselkompromittierung haften werden, in verschiedenen Ländern liegen und damit in verschiedenen Rechtsgebieten. Gerichtliche Auseinandersetzungen zwischen Produzenten und Betreibern von Sicherheitsmodulen sind damit von vornherein erschwert, wobei es jedoch wünschenswert wäre, sie durch technische vertrauensbildende Maßnahmen möglichst selten zu machen bzw. ganz zu vermeiden. Wenn es eine Domäne gäbe, welcher der Betreiber nicht vertraut, dann bestünde ein Sicherheitsproblem. Den Produktionsprozess vom späteren Betreiber jedoch regelmäßig inspizieren zu lassen, wäre unpraktisch und kostspielig.

[0004] Verschiedene Modelle von derzeit auf dem Markt befindlichen Frankiermaschinen sind mit einer postalischen Sicherheitseinrichtung mit einem Sicherheitsmodul ausgestattet. Diese dient im wesentlichen zur Speicherung und Abrechnung elektronischer Postgebühren und zur Erzeugung elektronischer Signaturen für die Erzeugung gültiger Frankierabdrucke (Indizien). Die Sicherheitsmodule müssen bei der Produktion, beim Transport und bei der Benutzung ersichtlicherweise gegen jegliche Art von Manipulationen geschützt werden, was derzeit zumeist mittels mechanischer Schutzmaßnahmen, wie einem verschlossenen Gehäuse um das Sicherheitsmodul herum erfolgt. Außerdem wird jedes produzierte Sicherheitsmodul kryptogra-

phisch initialisiert und registriert, bevor es in Benutzung genommen werden kann. Da dies jedoch bevorzugt am Ort der Produktion des Sicherheitsmoduls erfolgt, werden die Sicherheitsanforderungen nationaler Postbehörden wie der US-Postbehörde nicht erfüllt. Diese fordern eine Gewähr für die Sicherheit von Sicherheitsmodulen auch beim Transport und vorder Inbetriebnahme, insbesondere eine Registrierung erst beim Endbenutzer der Frankiermaschine oder bei einem nationalen Service-Center. Dies erfordert jedoch die Einrichtung nationaler Service-Center und einen deutlich erhöhten Aufwand an Zeit, Ausrüstung, Verpackung und sonstiger Behandlung.

[0005] Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren und ein Distributionssystem zur Distribution kryptographisch initialisierter Sicherheitsmodule zu schaffen. Zum Schutz vor Manipulationen unter Aufsicht des späteren Betreibers des Sicherheitsmoduls soll unter allen Umständen, d. h. selbst bei umfassender Unterwanderung der kryptographischen Initialisierung am Produktionsort, z. B. bei groß angelegter Bestechung des Personals, gewährleistet werden, dass nur Geräte mit solchen Sicherheitsmodulen vom Kunden in Betrieb genommen werden können, deren kryptographische Schlüssel nicht kompromittiert sind.

[0006] Diese Aufgabe wird erfindungsgemäß durch ein Verfahren gemäß Anspruch 1 und ein Distributionssystem gemäß Anspruch 14 gelöst. Die Erfindung geht dabei von der Erkenntnis aus, dass durch Erzeugung und Überprüfung von speziellen Markierungen gegebenenfalls in Kombination mit entsprechenden Zertifikaten ein erfolgreicher Schutz vor Manipulationen mit Fälschungsabsicht erzielt werden kann. Eine erste Markierung erfolgt dabei am Herstellerort in einem Herstellerzentrum nach einer ersten kryptographischen Initialisierung des Sicherheitsmoduls, wobei die erste Markierung vorzugsweise ein auf ein erstes Label gedruckter öffentlicher Schlüssel ist und das Label bevorzugt an der versandfertigen Verpackung des Sicherheitsmoduls bzw. eines Geräts mit integriertem, Sicherheitsmodul angebracht wird. Die erste Markierung kann dabei den zu versendenden elektronischen Schlüssel in unverschlüsselter oder verschlüsselter Form enthalten je nachdem, ob es sich bei dem zu versendenden Schlüssel um einen öffentlichen Schlüssel oder um einen privaten (geheimen) Schlüssel handelt. Die Verschlüsselung kann beispielsweise mit Hilfe eines Hash-Algorithmus erfolgen.

[0007] Eine zweite Markierung erfolgt entfernt vom Herstellerort bei einem Verteilerzentrum an einem Verteilerort bzw. einem sogenannten Einfuhrpunkt, der jeweils für eine bestimmte Region oder ein bestimmtes Land vorgesehen ist, beim Einführen und Registrieren der Verpackung mit dem Sicherheitsmodul. Dies ermöglicht eine Identifikation der Verpackung beim späteren Registrieren des Sicherheitsmoduls, ausgelöst durch den am Einsatzort befindlichen Benutzer, bevor angeforderte Daten auf das Sicherheitsmodul bzw. die Fran-

kiermaschine geladen werden können und die Frankiermaschine benutzt werden kann. Der am Verteilerort erzeugte Identifizierungscode wird dazu in einer entfernten zentralen Datenbank gespeichert.

[0008] Die Verifizierung erfolgt erfindungsgemäß mittels eines Verifizierungscode, der aus dem Identifizierungscode und dem in dem Sicherheitsmodul gespeicherten elektronischen Schlüssel erzeugt wird. Als ein solcher Verifizierungscode wird bevorzugt eine digitale Signatur oder ein Authentisierungscode, z. B. ein MAC (Message Authentication Code) Verwendung finden.

[0009] Das erfindungsgemäße Verfahren und das erfindungsgemäße Distributionssystem gewährleisten einen sicheren Vertrieb von Sicherheitsmodulen, bei dem die kundenfertig verpackten Geräte, z. B. Frankiermaschinen, inklusive der bereits eingebauten Sicherheitsmodule bzw. die separat vertriebenen und/oder separat verpackten Sicherheitsmodule am Verteilerort bzw. dem Einfuhrpunkt nicht ausgepackt werden brauchen. Dabei ist es besonders wirtschaftlich, einen einzigen zentralen Einfuhrpunkt in einem Land bzw. in einer Region zu haben, durch den alle verpackten Geräte bzw. Sicherheitsmodule importiert werden. Dieser Einfuhrpunkt kann vom Betreiber mit vertretbarem Aufwand regelmäßig inspiziert oder sogar selbst betrieben werden. Alle eintreffenden Geräte bzw. Sicherheitsmodule in diesem Einfuhrpunkt auszupacken und zu inspizieren, was sehr aufwendig wäre, ist erfindungsgemäß nicht mehr erforderlich.

[0010] Vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens bzw. des erfindungsgemäßen Distributionssystems sind in den Unteransprüchen angegeben. Dabei kann selbstverständlich das Distributionssystem in ähnlicher Weise weitergebildet sein, wie es in den Unteransprüche bezüglich des Verfahrens angegeben ist.

[0011] Bevorzugt ist vorgesehen, dass an der Verpackung des Sicherheitsmoduls vom Herstellerzentrum ein Label angebracht wird, auf das ein elektronischer Schlüssel in verschlüsselter oder unverschlüsselter Form, z. B. als Barcode, aufgedruckt ist. Diese maschinenlesbare Markierung wird dann vom Verteilerzentrum bzw. am Einfuhrpunkt gelesen und wird zur Identifizierung verwendet, wonach ein zweites Label mit dem Identifizierungscode an der Verpackung angebracht wird. Dabei wird entweder das erste Label überklebt oder entfernt, so dass es jedenfalls danach, insbesondere beim Benutzer, nicht mehr lesbar ist. Auch der Identifizierungscode kann verschlüsselt oder unverschlüsselt als Barcode auf dem Label aufgebracht sein. Anstelle von Labels mit Barcodes sind auch andere Möglichkeiten zum Versenden bzw. Anbringen des elektronischen Schlüssels und/oder des Identifizierungscode an der Verpackung bzw. dem Sicherheitsmodul selbst denkbar, wie beispielsweise Chipkarten, Magnetstreifenkarten oder ID-Tags. Dabei ist jeweils wieder bevorzugt vorgesehen, dass vom Verteilerzentrum bzw. am Einfuhrpunkt der beim Hersteller gespeicherte elek-

tronische Schlüssel gelöscht und durch den Identifizierungscode ersetzt wird.

[0012] In einer weiteren Ausgestaltung der Erfindung ist die Benutzung eines Authentisierungsalgorithmus und eines einzigen elektronischen Schlüssels beim Hersteller vorgesehen. Ein solcher Authentisierungsalgorithmus kann Teil eines sogenannten MAC (Message Authentication Code) sein. Weiter kann vorgesehen sein, dass dieser elektronische Schlüssel, der in dem Sicherheitsmodul gespeichert ist und gleichzeitig mit dem Sicherheitsmodul in von außen lesbarer Form versendet wird, mittels eines einzigen, nur dem Hersteller bzw. einem Herstellerzentrum und einem Service-Center in der Region des Benutzers bekannt ist. Der elektronische Schlüssel, der dann auf dem Sicherheitsmodul gespeichert ist, ist ebenfalls dem Benutzer bekannt und kann später zur Verschlüsselung weiterer Informationen, beispielsweise zwischen Benutzer und Service-Center, verwendet werden.

[0013] Alternativ ist in einer Weiterbildung die Verwendung eines elektronischen Schlüsselpaars mit einem privaten und einem öffentlichen Schlüssel vorgesehen. Dieses wird mit einem digitalen Signaturalgorithmus erzeugt, wie beispielsweise einem RSA (Rivest, Shamir, Adleman), einem DSA (Digital Signature Algorithm) oder einem ECDSA (Elliptic Curve DSA). Bevorzugt ist der öffentliche Schlüssel dabei in der zentralen Datenbank gespeichert, auf die auch das Verteilerzentrum und das Service-Center zugreifen können, und wird in von außen lesbarer Form mit dem Sicherheitsmodul versendet, während der private Schlüssel ausschließlich im Sicherheitsmodul gespeichert ist und mit diesem versendet wird. Zur Erzeugung von Zertifikaten, mit denen sich das Sicherheitsmodul identifizieren lässt und die den Schutz vor Manipulationen erhöhen, kann ebenfalls ein elektronisches Schlüsselpaar aus einem privaten und einem öffentlichen Schlüssel verwendet werden, wobei sowohl beim Herstellerzentrum als auch beim Verteilerzentrum ein getrenntes elektronisches Schlüsselpaar vorgesehen sein können.

[0014] Alternativ zu einer zentralen Datenbank, in der bestimmte elektronische Schlüssel, der Identifizierungscode und gegebenenfalls erzeugte Zertifikate in verschlüsselter oder unverschlüsselter Form gespeichert werden, kann auch vorgesehen sein, diese Daten über ein separates Netzwerk, in dem Sicherheitsmodul gespeichert oder auf sonstigem Wege, beispielsweise mittels eines per Post verschickten Datenträgers, vom Herstellerzentrum an das Verteilerzentrum und/oder das regionale Service-Center zu übermitteln. Dies hätte den Vorteil, dass die zentrale Datenbank, die bevorzugt die Daten aller global eingesetzten Sicherheitsmodule enthält, geringeren Sicherheitsanforderungen genügen muss, kleiner ausgestaltet sein kann oder gänzlich entfallen kann.

[0015] Die Erfindung ist selbstverständlich auch dann anwendbar, wenn es getrennte Hersteller bzw. Herstellerzentrum für das Sicherheitsmodul und das Anwen-

dungsgerät, beispielsweise die Frankiermaschine, gibt. Die Sicherheitsmodule werden dann in der beschriebenen Weise an den Hersteller der Frankiermaschine gesendet, wo das Sicherheitsmodul identifiziert und registriert werden und anschließend in die Frankiermaschine eingebaut werden kann. Auch beim Versenden der mit dem Sicherheitsmodul ausgestatteten Frankiermaschine kann dann das erfindungsgemäße Verfahren entsprechend angewendet werden.

Die Erfindung wird nachfolgend anhand der Zeichnungen näher erläutert. Es zeigen:

[0016]

- Figur 1 ein Blockschaltbild einer ersten Ausführungsform eines erfindungsgemäßen Distributionssystems,
- Figur 2 ein Ablaufdiagramm zur Erläuterung des erfindungsgemäßen Verfahrens bei einem Distributionssystem gemäß Figur 1,
- Figur 3 eine zweite Ausgestaltung eines erfindungsgemäßen Distributionssystems und
- Figur 4 einen Ablaufplan zur Erläuterung des erfindungsgemäßen Verfahrens bei einem Distributionssystem gemäß Figur 3.

[0017] Das in Figur 1 gezeigte erfindungsgemäße Distributionssystem weist folgende wesentliche Einheiten auf:

- a) Ein Hersteller bzw. Herstellerzentrum 1 von Sicherheitsmodulen 7 und gegebenenfalls Frankiermaschinen an einem Herstellerort umfasst ein Hersteller-Service-Center 6 (MSC = Manufacturing Service Center), worunter ein in oder nahe bei der Fabrik des Herstellers 1 betriebener Server verstanden werden soll. An diesen Server ist ein Drucker oder ein Chipkarten-Schreib-/Lesegerät angeschlossen, so dass frisch produzierte Sicherheitsmodule kryptographisch initialisiert werden können.
- b) Ein Verteiler bzw. Verteilerzentrum 2 an einem Verteilerort, das auch als Einfuhrpunkt (ESP = Entry Service Point) bezeichnet wird, ist in jeder Region vorgesehen, in der Geräte mit Sicherheitsmodulen betrieben werden sollen. Dabei kann es ein oder mehrere solcher Service-Center geben, die alle Geräte mit Sicherheitsmodulen für diese Region registrieren. Z. B. können alle Geräte mit Sicherheitsmodulen, die in einer Region verkauft werden sollen, an ein Verteilerzentrum 2 dieser Region geliefert, dort registriert und anschließend an den betreffenden Kunden ausgeliefert werden.
- c) Ein Benutzer 3 an einem Benutzerort, worunter ein Endkunde verstanden wird, erwirbt ein Gerät mit eingebautem Sicherheitsmodul oder beide Geräte separat und arbeitet damit.

d) Eine zentrale Datenbank 4 (PKD = Public Key Directory) dient als weltweites Verzeichnis aller gefertigten Sicherheitsmodule und bestimmter Attribute dieser Sicherheitsmodule, wobei es ein oder mehrere verteilte Datenbanken geben kann.

e) In jeder Region gibt es ein oder mehrere Service-Center 5 (RSC = Remote Service Center), worunter Regional-Server zu verstehen sind, die für alle in dieser Region registrierten Geräte mit Sicherheitsmodulen Dienste (Remote Services) anbieten. Der oder die regionalen Server 5 können räumlich auch in den Verteilerzentrum 2 der Region angesiedelt sein.

[0018] Weiter kann es in jeder Region einen regionalen Betreiber geben, der alle Geräte mit Sicherheitsmodulen in dieser Region betreibt, wobei dies auch eine postalische Autorität sein kann. Regionaler Betreiber ist derjenige, der für Schäden haftet, die aus der Kompromittierung eines Sicherheitsmoduls resultieren, das in dieser Region registriert ist. Aufgrund dieser Haftung wird vorausgesetzt, dass der regionale Betreiber den Verteilerzentrum seiner Region vertraut, das heißt, dass er sie z. B. regelmäßig inspiziert, inspizieren lässt oder selbst betreibt.

[0019] Das erfindungsgemäße Verfahren wird nachfolgend näher erläutert. Das Herstellerzentrum 1 betreibt neben der Herstellung der Sicherheitsmodule 7 einen lokalen Hersteller-Server (Herstellungs-Service-Center) 6 in unmittelbarer Nähe zum Produktionsendpunkt der Fabrik. Zunächst wird von dem Hersteller-Server 6 ein elektronisches Hersteller-Schlüsselpaar (sk_1 , vk_1) erzeugt (Schritt 20 in Figur 2). Der private Schlüssel sk_1 wird dabei von dem Hersteller-Server 6 benutzt, um Mitteilungen über neu produzierte Sicherheitsmodule 7 zu signieren, während der öffentliche Schlüssel vk_1 von den Service-Centern 5 dazu benutzt wird, diese Signaturen zu verifizieren. Dazu kann der öffentliche Schlüssel vk_1 von dem Hersteller-Server 6 offline an das Verteilerzentrum 2 und/oder das regionale Service-Center 5 übermittelt werden. Um diesen Übertragungskanal zu authentifizieren, können eine oder mehrere zertifizierende Autoritäten vorgesehen sein.

[0020] Auch das Verteilerzentrum 2, das als Einfuhrpunkt für alle in einer bestimmten Region zu betreibenden Sicherheitsmodule dient, erzeugt zunächst ein Verteiler-Schlüsselpaar (sk_2 , vk_2) mit einem privaten Schlüssel sk_2 und einem öffentlichen Schlüssel vk_2 (Schritt 21). Damit können für die Sicherheitsmodule sogenannte Eingangszertifikate als digitale Signaturen erzeugt werden, die in der zentralen Datenbank 4 gespeichert werden können. Die verschiedenen Verteilerzentren der unterschiedlichen Regionen oder Länder kennen dabei die öffentlichen Verteiler-Schlüssel der anderen Verteilerzentren nicht. Jedes Verteilerzentrum muss nur in der Lage sein, seine eigenen Einträge in der zentralen Datenbank 4 prüfen zu können. Grundsätzlich ist es auch möglich, mehrere Verteilerzentrum bzw. Ein-

fuhrpunkte für ein Land oder eine Region vorzusehen.

[0021] Nachdem ein Sicherheitsmodul 7 hergestellt und mit den mechanischen Schutzvorrichtungen versehen ist, wird es mit dem Hersteller-Server 6 verbunden, beispielsweise über einen zwischengeschalteten (nicht gezeigten) Registrierungs-PC. Dieser fordert von dem Sicherheitsmodul 7 einen öffentlichen Schlüssel an, wobei die Anforderung den öffentlichen Hersteller-Schlüssel vk_1 und die Anforderung, ein Transport-Schlüsselpaar zu erzeugen, enthält (Schritt 22). Das Sicherheitsmodul 7 speichert den Schlüssel vk_1 in einem nicht-flüchtigen Speicher und generiert das angeforderte Transport-Schlüsselpaar (stk , vtk), welches einen Signier-Transport-Schlüssel stk (signing transport key) und einen Verifizier-Transport-Schlüssel vtk (verifying transport key) enthält (Schritt 23). Während der private Schlüssel stk von dem Sicherheitsmodul 7 privat gehalten und nur dort gespeichert wird, wird von dem Sicherheitsmodul 7 eine einmalige Seriennummer s , die bei der Herstellung vergeben wurde, und der Verifizier-Transport-Schlüssel vtk über den Registrierungs-PC an den Hersteller-Server 6 weitergegeben (Schritt 24). Dieser erzeugt daraufhin mit Hilfe seines privaten Schlüssels sk_1 und eines Signialgorithmus $cert$ ein öffentliches Schlüssel-Zertifikat c_1 (Schritt 25), das er anschließend zusammen mit der Seriennummer s und dem Verifizier-Transport-Schlüssel vtk in der öffentlichen entfernten zentralen Datenbank 4 speichert (Schritt 26). Nach dieser anfänglichen Registrierung wird das Sicherheitsmodul 7 seinen Verifizier-Transport-Schlüssel vtk niemals mehr herausgeben, auch eine Speicherung desselben ist nicht erforderlich.

[0022] Für die Realisierung des Registrierungs-PCs und des Hersteller-Servers 6 bieten sich verschiedene Möglichkeiten, wie beispielsweise eine Client-Server-Architektur auf der Basis von Windows-NT.

[0023] Anschließend wird das Sicherheitsmodul 7 in einer Transportverpackung 8 verpackt, wobei das Sicherheitsmodul 7 in einer separaten Verpackung oder zusammen mit einem Benutzergeräte 71, z.B. einer Frankiermaschine, in einer gemeinsamen Verpackung 8 enthalten sein kann. Im letzteren Falle kann das Sicherheitsmodul 7, wie in Fig. 1 gezeigt, auch bereits in die Frankiermaschine 71 eingebaut sein. Nachdem die Verpackung 8 verschlossen und versiegelt ist, wird ein Label 9 erzeugt, auf das die Seriennummer s , der Verifizier-Transport-Schlüssel vtk des Sicherheitsmoduls 7 und gegebenenfalls weitere Informationen, bevorzugt in Form eines zweidimensionalen Barcodes, gedruckt sind (Schritt 27). Dieses Label 9 wird von außen sichtbar und lesbar auf die Verpackung 9 aufgebracht, so dass die enthaltene Information mit einer Maschine, z. B. mit einem Barcode-Leser auf einfache Weise gelesen werden kann. Wenn die Labels 9 nicht robust genug sind, um den Transport zu überstehen, können die Barcodes auch direkt auf die Verpackung oder etwaige Begleitpapiere gedruckt werden, die dann in eine entsprechende Hülle auf die Außenseite der Verpackung 8 aufgebracht

werden.

[0024] Die Verpackungen werden anschließend vom Herstellerzentrum 1 direkt zu den Verteilerzentrum 2 in den jeweiligen Regionen gesandt, in denen die Frankiermaschinen 71 bzw. die Sicherheitsmodule 7 dann verkauft und benutzt werden sollen. Dort werden die Barcodes jeder ankommenden Verpackung 9 mit einem Scanner 10 gelesen, der an einen entsprechenden Rechner 11 mit angeschlossenem Drucker 12 angeschlossen ist. Für jede Seriennummer s und jeden Verifizier-Transport-Schlüssel vtk wird anschließend per Zufall ein Identifizierungscode ID gewählt, auch wenn der Endkunde des Produkts weder bereits bekannt noch bestimmt ist. Die Anzahl der Kundennummern muss dabei groß genug sein, so dass Kollisionen von Identifikationscodes äußerst selten sind und es praktisch ausgeschlossen ist, zu erraten, welcher Identifikationscode einem bestimmten Sicherheitsmodul zugewiesen werden wird. Bevorzugt ist deshalb die Benutzung von Identifikationscodes mit einer Länge zwischen 32 und 64 Bit vorgesehen.

[0025] Anschließend verknüpft das Verteilerzentrum 2 den neuen Identifikationscode ID mit der Seriennummer s und dem Verifizier-Transport-Schlüssel vtk auf der Verpackung, indem der Identifizierungscode ID auf ein neues Label 13 gedruckt wird, welches über das erste Label 9 auf der Verpackung 8 geklebt wird, so dass der Barcode des ersten Labels 9 nicht mehr gelesen werden kann. Dazu kann das erste Label 9 auch entfernt werden, bevor das Label 13 aufgeklebt wird. Wenn das Label oder der Barcode auf Begleitpapieren angebracht ist, wird das neue Label 13 an dieser Stelle angebracht. Bevorzugt ist der Identifikationscode ID in normal lesbarer Form auf dem Label 13 aufgebracht, wobei das genaue Format die Eigenschaften der Eingabemittel der mit dem Sicherheitsmodul auszustattenden Frankiermaschine berücksichtigen sollte. Wenn beispielsweise die Eingabemittel ein Ziffernfeld aufweisen, dann kann der Identifikationscode ID auch in Dezimalzahlen gedruckt werden. Wenn jedoch die Eingabemittel nur eine Anzahl von speziellen, beispielsweise farblich unterschiedlichen Tasten aufweisen, dann sollte auch der Identifikationscode in entsprechender Weise codiert sein. Ausserdem wird vom Verteilerzentrum 2 ein Eingangszertifikat c_2 aus der Seriennummer s , dem Verifizier-Transport-Schlüssel vtk und dem Identifikationscode ID mit Hilfe des privaten Verteiler-Schlüssels sk_2 mittels eines Signialgorithmus $cert$ erzeugt (Schritt 28). Dieses wird schließlich zusammen mit dem Identifikationscode ID in der zentralen Datenbank 4 gespeichert und dort den bereits gespeicherten Daten des Sicherheitsmoduls 7 zugeordnet (Schritt 29).

[0026] Konzeptionell ist die zentrale Datenbank ein großes verteiltes Verzeichnis, das öffentliche Verifizier-Schlüssel von Sicherheitsmodulen für Frankiermaschinen in allen Ländern zentral verwaltet. Der Zugriff auf diese globale Datenbank 4 ist streng begrenzt, wobei Lese- und Schreib-Zugriffe auf die Service-Center 5, 6

und die Verteilerzentren 2 beschränkt sind. Die Verteilerzentren 2 und die Service-Center jeder Region haben dabei nur auf die Schlüssel Zugriff, die die in ihrer Region betriebenen Sicherheitsmodule betreffen.

[0027] Alle derartig verarbeiteten Verpackungen 8 mit Sicherheitsmodulen werden anschließend von den Verteilerzentren 2 direkt vermarktet oder über Einzelhändler vertrieben. Im allgemeinen wissen die Verteilerzentren 2 nicht, wer schließlich der Endkunde 3 ist, welches Produkt er erhält und wann er es erhält.

[0028] Nachdem ein Kunde 3 eine Verpackung 18 erhalten und das Sicherheitsmodul 7 entnommen hat, wird er es in die Frankiermaschine 71 einbauen, sofern es nicht wie gezeigt bereits eingebaut ist, diese in Betrieb nehmen und an das Telefonnetz anschließen. Die Frankiermaschine wird dann mit einem regionalen Service-Center 5 seiner Region verbunden, um dort registriert zu werden. Dazu wird zunächst von dem Sicherheitsmodul 7 ein Verifizierungscode sig aus dem in dem Sicherheitsmodul gespeicherten privaten Schlüssel stk und dem auf dem Label 13 enthaltenen Identifikationscode ID erzeugt (Schritt 30). Dieser Verifizierungscode sig wird dann zusammen mit dem Identifikationscode ID an das regionale Service-Center 5 übertragen, welches daraufhin in der zentralen Datenbank 4 nachsieht, ob der übertragene Identifikationscode ID von dem Verteiler 2 dieser Region erzeugt worden ist und ob ein gültiges Eingangszertifikat c_2 vorliegt (Schritte 31, 32). Sofern dies der Fall ist, erhält das regionale Service-Center 5 von der zentralen Datenbank 4 den Verifizier-Schlüssel vtk zurück (Schritt 33), der dann für die Verifizierung des Sicherheitsmoduls mittels des Verifizieralgorithmus ver anhand des erzeugten Verifizierungscode sig und des Identifikationscodes ID benutzt wird (Schritt 34).

[0029] Wenn dieser Test erfolgreich ist, ist das Sicherheitsmodul und die zugehörige Frankiermaschine registriert und für die Benutzung freigegeben, wonach die länderspezifische Software, Initialisierung und Autorisierung heruntergeladen werden können. Danach ist das Sicherheitsmodul als postalische Sicherheitseinrichtung (PSD = Postal Security Device) anerkannt, so dass die Frankiermaschine in Betrieb gehen, Gebühreneinheiten herunterladen und Frankierungen erzeugen kann. Wie unmittelbar aus der oberen Erläuterung ersichtlich ist, ist es bei der Erfindung nicht erforderlich, dass die Verpackung des Sicherheitsmoduls auf dem Weg zum Hersteller bis zum Endbenutzer geöffnet werden muss. Es können demnach Siegel an der Verpackung angebracht werden, so dass beim Benutzer ein unbefugtes Öffnen der Verpackung während des Transports leicht festgestellt werden kann. Durch die Verwendung der beschriebenen Zertifikate und der beschriebenen Labels wird ausserdem ein weitreichender Schutz vor Manipulationen mit Fälschungsabsicht erzielt. Nur wenn die Verifizierung und Registrierung am Ende des beschriebenen Verfahrens erfolgreich verläuft, kann das Sicherheitsmodul auch in Betrieb genommen werden.

[0030] Grundsätzlich muss ein Distributionssystem einer Reihe von Sicherheitsanforderungen genügen und Schutz vor unterschiedlichen Manipulationen bieten. Diese sollen nachfolgend kurz dargestellt werden:

1. Ein Betrüger könnte den privaten Transportschlüssel stk eines Sicherheitsmoduls kompromittieren und sich mittels eines PC an einem regionalen Service-Center in gleicher Weise wie ein Sicherheitsmodul anmelden. Nachdem er sich dann angemeldet, initialisiert und autorisiert hat, könnte er ein geeignetes Schlüsselpaar unter Kontrolle haben, um Frankierungen in beliebiger Zahl und Höhe zu erzeugen. Die Kompromittierung könnte dadurch erfolgen, dass beim Herstellungsprozess der private Transportschlüssel gestohlen wird, dass öffentliche Transportschlüssel bei der Übertragung über ein Netzwerk abgehört werden oder dass die mechanischen Schutzvorrichtungen eines Sicherheitsmoduls aufgebrochen werden. Ausserdem könnte ein solcher Betrüger auch direkt Sicherheitsmodule beim Hersteller stehlen.

2. Ein Betrüger könnte auch seine eigenen Transportschlüssel erzeugen und in das System durch Ankopplung an einen Hersteller-Service 6 oder ein regionales Service-Center 5 einschleusen. Auch der Transport von Verifizier-Schlüsseln neuer Sicherheitsmodule könnte von einem Betrüger unterbrochen werden. In diesem Falle würde das System keinen Unterschied zwischen der Anzahl der hergestellten Sicherheitsmodule und der Anzahl der Transportschlüssel registrieren. Da der Betrüger dann einen privaten Transportschlüssel kennt, der mit einem öffentlichen Transportschlüssel zusammenpasst, ist der Betrüger ebenso mächtig wie jemand, der einen privaten Transportschlüssel kompromittiert.

3. Ein Betrüger könnte auch ein fertiggestelltes Sicherheitsmodul, das mit einem Transportschlüssel ausgestattet ist, entwenden, bevor es zum Kunden geliefert wird. Dieses könnte er dann dazu benutzen, um in einem bestimmten Land Frankierungen zu erzeugen.

4. Schließlich könnte ein Betrüger auch seine eigenen Sicherheitsmodule herstellen und in die Vertriebskette einschleusen. Dabei müsste der Betrüger allerdings öffentliche Transportschlüssel erfolgreich in das System einschleusen, da ansonsten seine Sicherheitsmodule nicht akzeptiert werden.

[0031] Das erfindungsgemäße Verfahren und das erfindungsgemäße Distributionssystem kann allen beschriebenen Missbräuchen standhalten, ausser das Sicherheitsmodul wird beim Kunden gestohlen und die mechanischen Sicherheitsvorrichtungen werden aufge-

brochen oder der öffentliche Transportschlüssel fällt dem Betrüger dabei in die Hände. Bei der erfindungsgemäßen Lösung muss einem Betrüger nicht nur ein registriertes Schlüsselpaar von Transportschlüsseln, sondern auch ein zugehöriger Identifikationscode in die Hände fallen. Wenn ein Betrüger nur das registrierte Transportschlüsselpaar und möglicherweise ein Sicherheitsmodul findet, ist es immer noch erforderlich, dass er dafür einen Identifikationscode beim Verteiler erzeugen lassen muss. Andernfalls wird sonst kein Identifikationscode in die zentrale Datenbank eingetragen und eine Registrierung oder Benutzung wird fehlschlagen. Nachdem das Verteilerzentrum einen Identifikationscode erzeugt und in der zentralen Datenbank gespeichert hat, könnte ein Betrüger auch versuchen, diesen aus der zentralen Datenbank auszulesen oder das Sicherheitsmodul auf dem Transportweg zum Benutzer abzufangen, um den Identifikationscode zu erhalten. Dabei ist anzumerken, dass nicht jedermann eine Verpackung mit einem Sicherheitsmodul und einem Label mit Identifikationscode bestellen kann.

[0032] Das beschriebene erfindungsgemäße Distributionssystem umfasst eine verteilte Datenbank mit höchster Sicherheitsstufe, die in ausreichendem Maße gegen nichtautorisierten Zugriff geschützt werden muss. Dies ist dadurch gesichert, dass die Infrastruktur ein geschlossenes System ist ohne Zugriffsmöglichkeit über das Internet.

[0033] Eine Verpackung mit einem Label auf dem Vertriebswege abzufangen wird allgemein als ausreichend schwierig angesehen. Die Anzahl der Versendungen von Sicherheitsmodulen ist relativ gering und es ist auch nicht möglich, ohne Barcodescanner einen öffentlichen Transportschlüssel von einem Label zu lesen. Noch schwieriger ist es dann, wenn das Label mit dem Identifikationscode über das erste Label geklebt ist.

[0034] Der schwerwiegendste Betrugsversuch liegt vermutlich darin, eine große Anzahl von privaten Transportschlüsseln beim Hersteller zu kompromittieren und deren öffentliche Transportschlüssel mit derselben Anzahl von Verpackungen zu vergleichen, die in Ladenregalen liegen, um wenigstens eine einzige Übereinstimmung zu finden. Diese Betrugsmethode funktioniert nur dann, wenn der Betrüger irgendwie erkennen kann, welche Verpackungen in den Ladenregalen mit welchen von dem Hersteller kommenden Verpackungen übereinstimmen. Dies könnte dadurch erfolgen, dass ein Betrüger beim Verteilerzentrum den öffentlichen auf dem ersten Label gespeicherten Transportschlüssel in irgendeiner Weise ausliest, bevor das zweite Label darüber geklebt wird. Eine andere Möglichkeit wäre die heimliche Markierung von Verpackungen beim Hersteller, um dieselben Verpackungen später wiedererkennen zu können.

[0035] All die beschriebenen Missbrauchsmöglichkeiten werden jedoch bei dem erfindungsgemäßen Distributionssystem und Verfahren unterbunden bzw. weitgehend vermieden, so dass die vorgesehenen Sicher-

heitsmaßnahmen nur unter sehr großem Aufwand umgangen werden können.

[0036] Eine zweite Ausführungsform des erfindungsgemäßen Distributionssystems und des erfindungsgemäßen Verfahrens soll anhand der Figuren 3 und 4 erläutert werden. Anders als bei dem Distributionssystem gemäß Fig. 1 werden hier nicht Schlüsselpaare mit einem privaten und einem öffentlichen Schlüssel, sondern es wird nur jeweils ein symmetrischer Schlüssel eingesetzt. Zunächst erzeugt der Hersteller-Server 6 einen privaten Schlüssel k_1 , der mit dem regionalen Service-Center 5 vereinbart wird (Schritt 40). Ebenso generiert das Verteilerzentrum 2 einen eigenen privaten Schlüssel k_2 und das Sicherheitsmodul 7 einen Transportschlüssel tk (Schritte 41, 42). Nachdem das Sicherheitsmodul 7 den Transportschlüssel tk an den Hersteller-Server 6 übertragen hat (Schritt 43), verschlüsselt dieser den Transportschlüssel tk mit Hilfe seines privaten Schlüssels k_1 mittels eines Verschlüsselungsalgorithmus enc und sendet das Zertifikat c_1 an das Sicherheitsmodul 7 zurück (Schritte 44, 45). Das Sicherheitsmodul 7 speichert das Zertifikat c_1 , erstellt aus dem Transportschlüssel tk einen Hash-Wert h und druckt diesen auf das Label 9, welches dann an der Verpackung 8 des Sicherheitsmoduls 7 angebracht wird (Schritt 46). Dieser Hash-Wert h wird schließlich über den Hersteller-Server 6 auch in die zentrale Datenbank 4 eingetragen (Schritt 47).

[0037] Bei dem Verteilerzentrum 2 wird der Hash-Wert h von dem Label 9 mittels des Scanners 10 gelesen, ein Identifikationscode ID erzeugt und auf das zweite Label 13 gedruckt, welches dann über dem Label 9 auf der Verpackung 8 angebracht wird (Schritt 48). Der Identifikationscode ID wird ebenfalls in der zentralen Datenbank 4 gespeichert und dort den Hash-Wert h zugeordnet (Schritt 49).

[0038] Am Benutzerort 3 wird vom Sicherheitsmodul 7 nach dessen Eintreffen mittels eines Authentisierungsalgorithmus aus dem Transportschlüssel tk , der in dem Sicherheitsmodul gespeichert ist, und dem Identifikationscode ID des Labels 13 ein Verifizierungscode m , oft auch als MAC (Message Authentication Code) bezeichnet, erzeugt (Schritt 50). Dieser wird zusammen mit dem Identifizierungscode ID und dem Zertifikat c_1 an das regionale Service-Center 5 übertragen (Schritt 51). Dort wird das Zertifikat c_1 mit Hilfe des privaten Schlüssels k_1 mittels eines Entschlüsselungsalgorithmus dec entschlüsselt, woraus sich der Transportschlüssel tk ergibt, aus dem dann anschließend ein Hash-Wert h berechnet wird (Schritt 52). Danach prüft das regionale Service-Center 5, ob der Identifizierungscode ID und der Hash-Wert h in der zentralen Datenbank 4 enthalten sind (Schritt 53). Sofern dies der Fall ist, erfolgt schließlich die Verifizierung mittels des Verifizierungsalgorithmus ver mit Hilfe des Transportschlüssels tk , des Identifizierungscodes ID und des Verifizierungscodes m (Schritt 54). Bei erfolgreicher Verifizierung kann dann die Registrierung erfolgen, wonach das Si-

cherheitsmodul bestimmungsgemäß benutzt werden kann.

Patentansprüche

1. Verfahren zur sicheren Distribution von Sicherheitsmodulen (7), insbesondere für Frankiermaschinen, von einem Herstellerort über einen Verteilerort zu einem Benutzerort mit den Schritten:

- a) Erzeugung und Speicherung mindestens eines elektronischen Schlüssels (stk; vtk; tk) in dem Sicherheitsmodul (7) am Herstellerort,
- b) Speicherung des elektronischen Schlüssels (vtk; tk) in einer zentralen Datenbank (4),
- c) Versendung des elektronischen Schlüssels (vtk; tk) zusammen mit dem Sicherheitsmodul (7) in von außen lesbarer Form zum Verteilerort,
- d) Erzeugung eines dem elektronischen Schlüssel (vtk; tk) zugeordneten Identifizierungscode (ID), Speicherung des am Verteilerort erzeugten Identifizierungscode (ID) in der entfernten zentralen Datenbank (4) und Versendung zusammen mit dem Sicherheitsmodul (7) in von außen lesbarer Form am Verteilerort, wobei der von außen lesbare elektronische Schlüssel (vtk; tk) unlesbar gemacht wird,
- e) Erzeugung eines Verifizierungscode (sig; m) aus dem Identifizierungscode (ID) und dem in dem Sicherheitsmodul gespeicherten elektronischen Schlüssel (stk; tk) durch das Sicherheitsmodul am Benutzerort,
- f) Verifizierung der Zusammengehörigkeit von Verifizierungscode (sig; m), Identifizierungscode (ID) und aus der zentralen Datenbank (4) ausgelesenem, dem Identifizierungscode (ID) zugehörigem elektronischen Schlüssel (vtk; tk) durch ein Service-Center (5) und
- g) Registrierung des Sicherheitsmoduls (7) bei erfolgreicher Verifizierung durch den Service-center (5).

2. Verfahren nach Anspruch 1,

dadurch gekennzeichnet, dass zur Versendung mit dem Sicherheitsmodul der elektronische Schlüssel und/oder der Identifizierungscode an dem Sicherheitsmodul, an ein Gerät mit eingebautem Sicherheitsmodul oder an eine Transportverpackung des Sicherheitsmoduls oder des Geräts angebracht sind.

3. Verfahren nach Anspruch 2,

dadurch gekennzeichnet, dass der elektronische Schlüssel und/oder der Identifizierungscode maschinenlesbar angebracht sind, insbesondere als

Barcode oder als Datenträger, insbesondere Chipkarte, Magnetstreifenkarte oder ID-Tag.

4. Verfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet, dass zur Erzeugung des Verifizierungscode der Identifizierungscode in das Sicherheitsmodul eingegeben wird.

5. Verfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet, dass ein Herstellerzentrum (1) am Herstellerort zur vollständigen oder teilweisen Fertigung der Sicherheitsmodule ausgestaltet ist, dass ein Verteilerzentrum (2) am Verteilerort zur Distribution der verpackten und von außen mit dem Identifizierungscode versehenen Sicherheitsmodule ausgestaltet ist und dass der Servicecenter (5) zur Versorgung der Sicherheitsmodule bei dem Benutzer mit Gebühreneinheiten ausgestaltet ist.

6. Verfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet, dass zur Speicherung in dem Sicherheitsmodul und zum Versenden mit dem Sicherheitsmodul in von außen lesbarer Form ein einziger mittels eines Authentisierungsalgorithmus erzeugter elektronischer Schlüssel verwendet wird.

7. Verfahren nach Anspruch 6,

dadurch gekennzeichnet, dass zur Verschlüsselung ein einziger, nur dem Herstellerzentrum (1) und einem Servicecenter (5) bekannter elektronischer Schlüssel verwendet wird.

8. Verfahren nach einem der Ansprüche 1 bis 5,

dadurch gekennzeichnet, dass zur Speicherung in dem Sicherheitsmodul und zum Versenden mit dem Sicherheitsmodul in von außen lesbarer Form ein mittels eines digitalen Signaturalgorithmus erzeugtes elektronisches Schlüsselpaar mit einem privaten und einem öffentlichen Schlüssel verwendet wird.

9. Verfahren nach Anspruch 8,

dadurch gekennzeichnet, dass nur der öffentliche Schlüssel in der zentralen Datenbank (4) gespeichert und mit dem Sicherheitsmodul von außen lesbar versendet wird und dass der private Schlüssel ausschließlich im Sicherheitsmodul gespeichert ist und nur zur Erzeugung des Verifizierungscode verwendet wird.

10. Verfahren nach Anspruch 8 oder 9,

dadurch gekennzeichnet, dass zur Erzeugung von Zertifikaten ein elektronisches Schlüsselpaar

aus einem privaten und einem öffentlichen Schlüssel verwendet wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, 5
dadurch gekennzeichnet, dass der elektronische Schlüssel und der Identifizierungscode statt in der zentralen Datenbank (4) gespeichert zu werden, über ein Netzwerk, in dem Sicherheitsmodul gespeichert oder auf sonstigem Weg für die Verifizierung des Sicherheitsmoduls übermittelt wird. 10

12. Verfahren nach einem der vorhergehenden Ansprüche, 15
dadurch gekennzeichnet, dass die Daten der zentralen Datenbank (4) verschlüsselt sind und dass das Herstellerzentrum (1) und ein zur Registrierung des Sicherheitsmoduls vorgesehenes Servicecenter (5) einen Schlüssel zum Zugriff auf die Datenbank (4) besitzen. 20

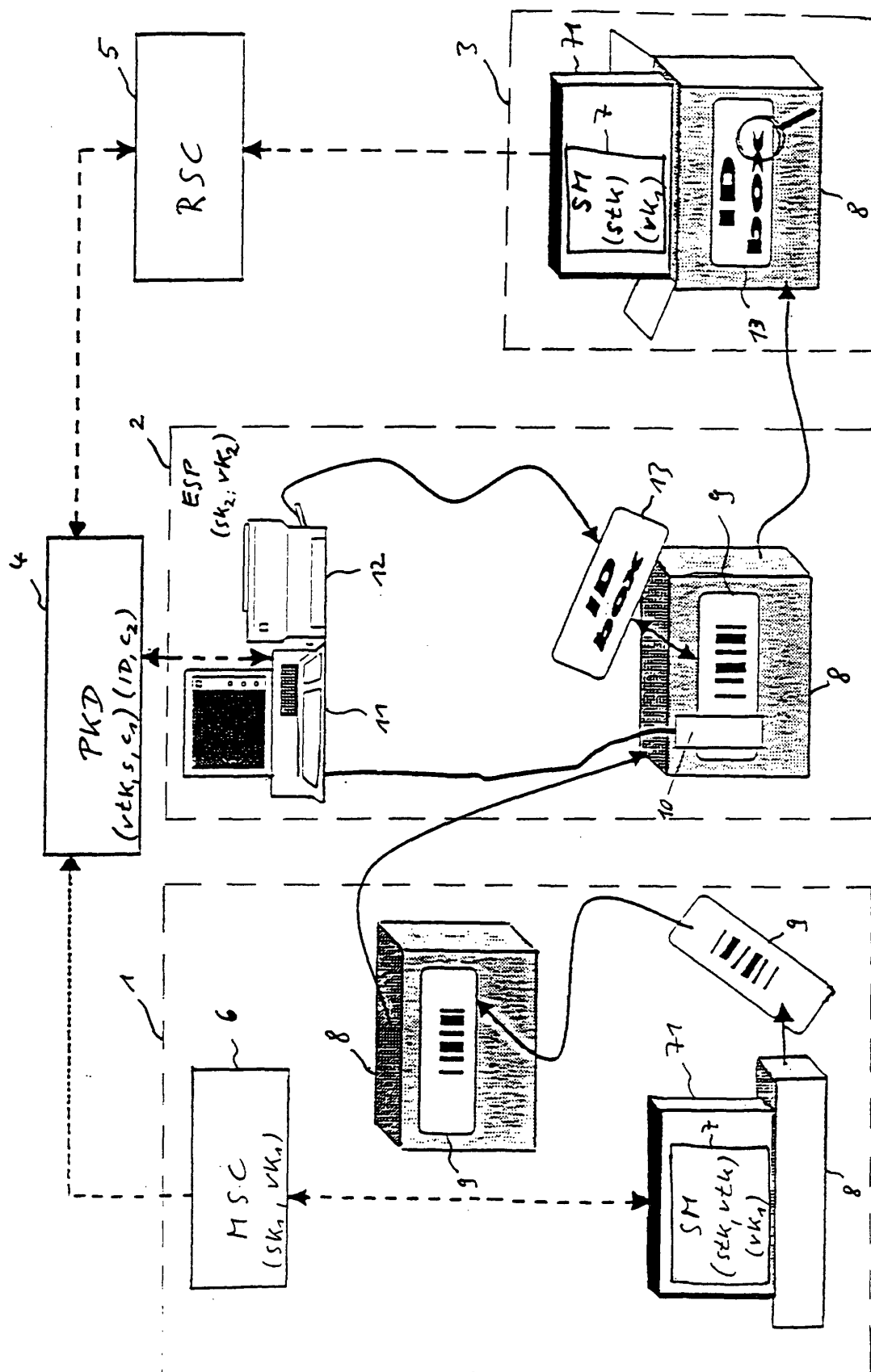
13. Verfahren nach einem der vorhergehenden Ansprüche, 25
dadurch gekennzeichnet, dass die Versendung des Sicherheitsmoduls von dem Herstellerort zum Verteilerort und vom Verteilerort zum Benutzerort in einer verschlossen bleibenden Versandverpackung erfolgt.

14. Distributionssystem zur sicheren Distribution von Sicherheitsmodulen, insbesondere für Frankiermaschinen, mit: 30
 - a) einem Herstellerzentrum (1) zur Erzeugung und Speicherung mindestens eines elektronischen Schlüssels (stk; tk) in dem Sicherheitsmodul (7), zur Speicherung des genannten oder eines weiteren elektronischen Schlüssels (vtk; tk) in einer zentralen Datenbank (4) und zur Versendung des elektronischen Schlüssels (vtk; tk) zusammen mit dem Sicherheitsmodul (7) in von außen lesbarer Form, 35
 - b) einem Verteilerzentrum (2) zum Empfang des Sicherheitsmodul (7) vom Hersteller (1), zur Erzeugung eines dem elektronischen Schlüssel (vtk; tk) zugeordneten Identifizierungscodes (ID), zur Speicherung des am Verteilerort erzeugten Identifizierungscodes (ID) in der entfernten zentralen Datenbank (4) und zur Versendung des Identifizierungscodes (ID) zusammen mit dem Sicherheitsmodul (7) in von außen lesbarer Form, wobei der von außen lesbare elektronische Schlüssel (vtk; tk) unlesbar gemacht wird, 40
 - c) einem Benutzergerät (3), das nach dem Empfang des Sicherheitsmoduls (7) von dem Verteilerzentrum in Betrieb genommen wird, mit dem Sicherheitsmodul (7) zur Erzeugung 45

eines Verifizierungscodes (sig; m) aus dem Identifizierungscode (ID) und dem elektronischen Schlüssel (vtk; tk), und
 d) einem Servicecenter (5) zur Verifizierung der Zusammengehörigkeit von Verifizierungscode (sig; m), Identifizierungscode (ID) und aus der zentralen Datenbank (4) ausgelesenem, dem Identifizierungscode (ID) zugehörigem elektronischen Schlüssel (vtk; tk) und zur Registrierung des Sicherheitsmoduls (7) bei erfolgreicher Verifizierung.

15. Distributionssystem nach Anspruch 14, 15
dadurch gekennzeichnet, dass Verteilerzentrum (2) den Servicecenter (5) umfasst und dass das Verteilerzentrum (2) und/oder der Servicecenter (5) von einem regionalen Betreiber betrieben werden.

16. Distributionssystem nach Anspruch 14 oder 15, 20
dadurch gekennzeichnet, dass das Verteilerzentrum (2) derart ausgestaltet ist, dass alle in einem territorialen Gebiet zu betreibenden Sicherheitsmodule den Verteilerort vor der Registrierung durchlaufen müssen.



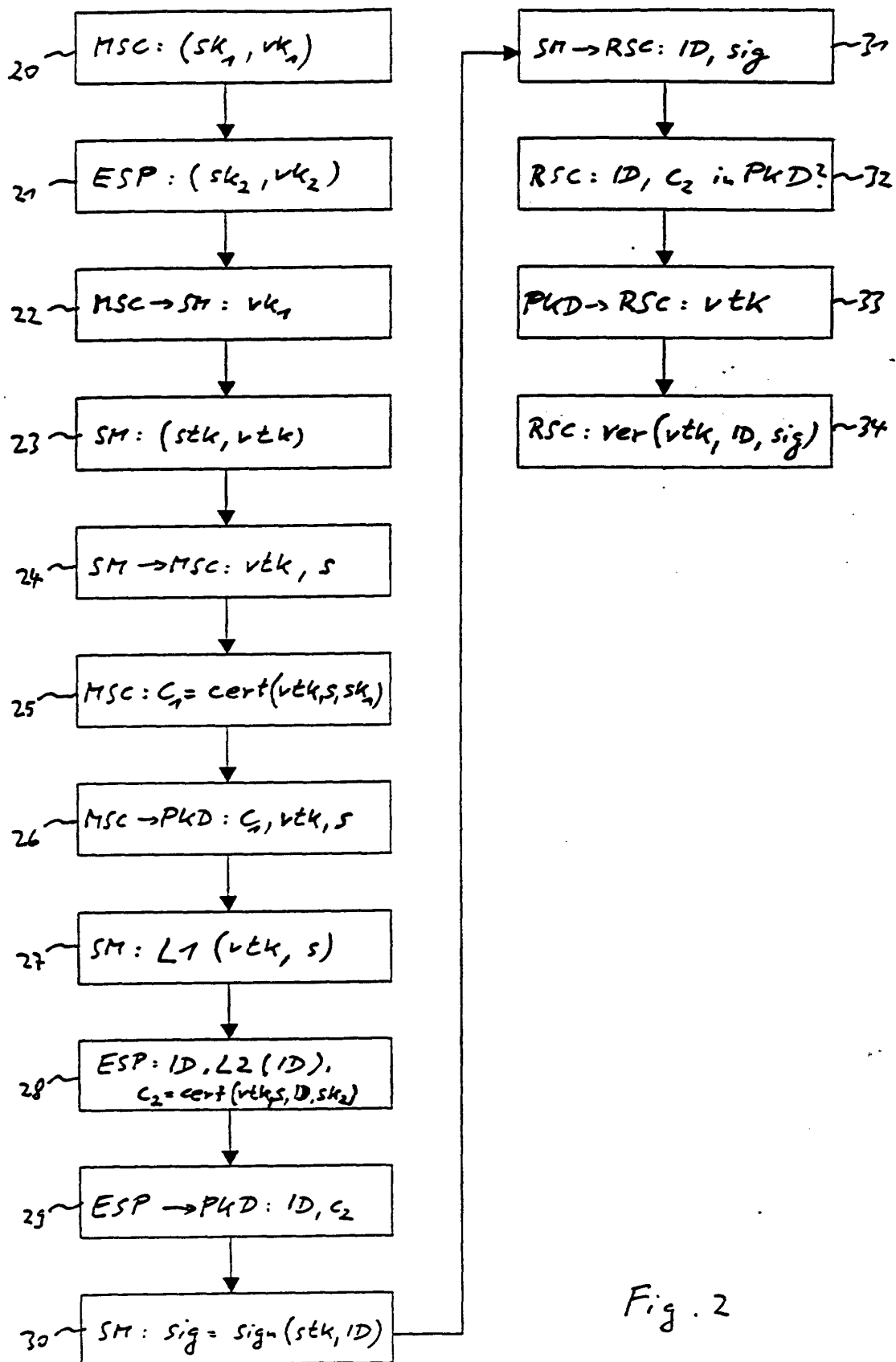


Fig. 2

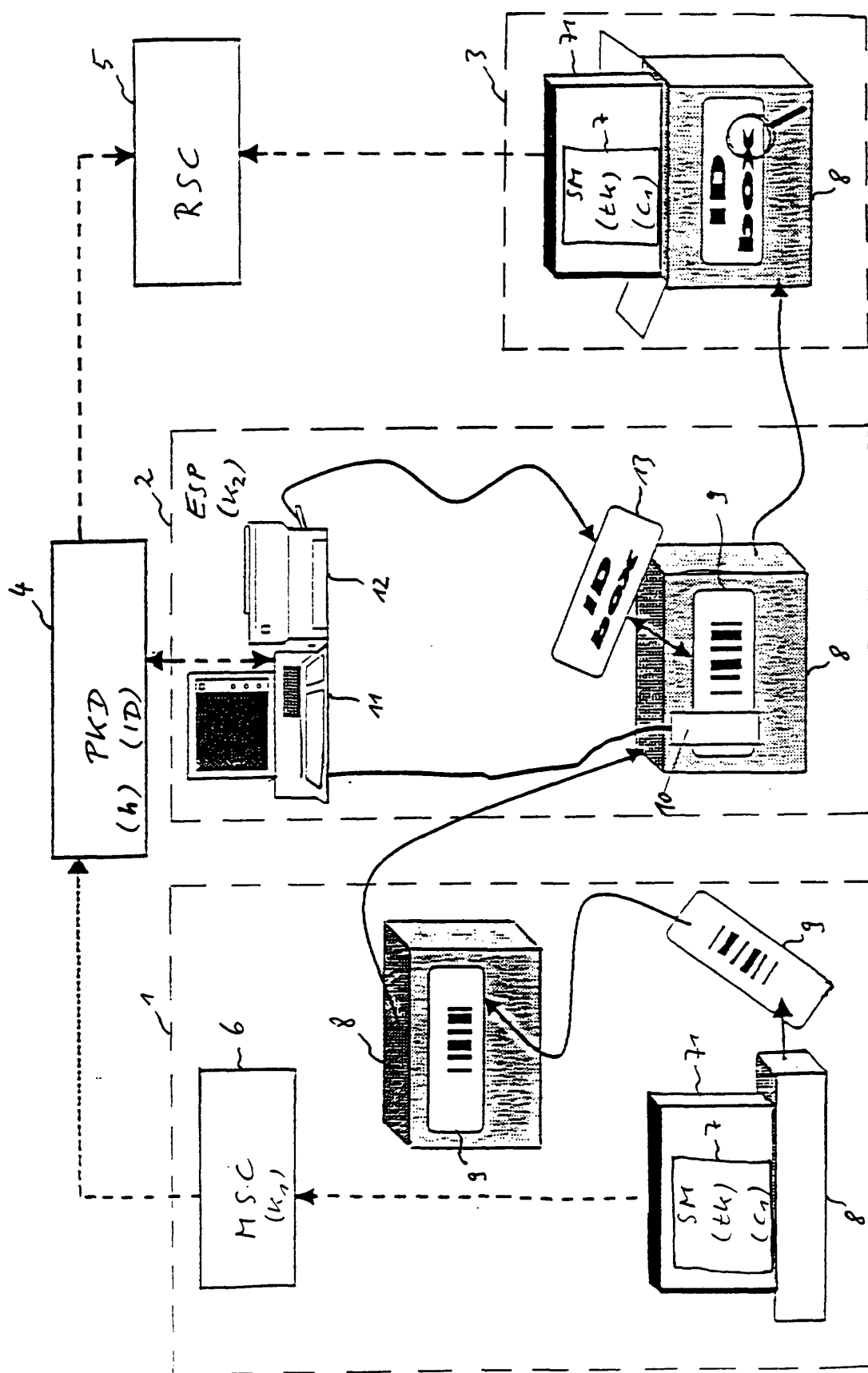


Fig. 3

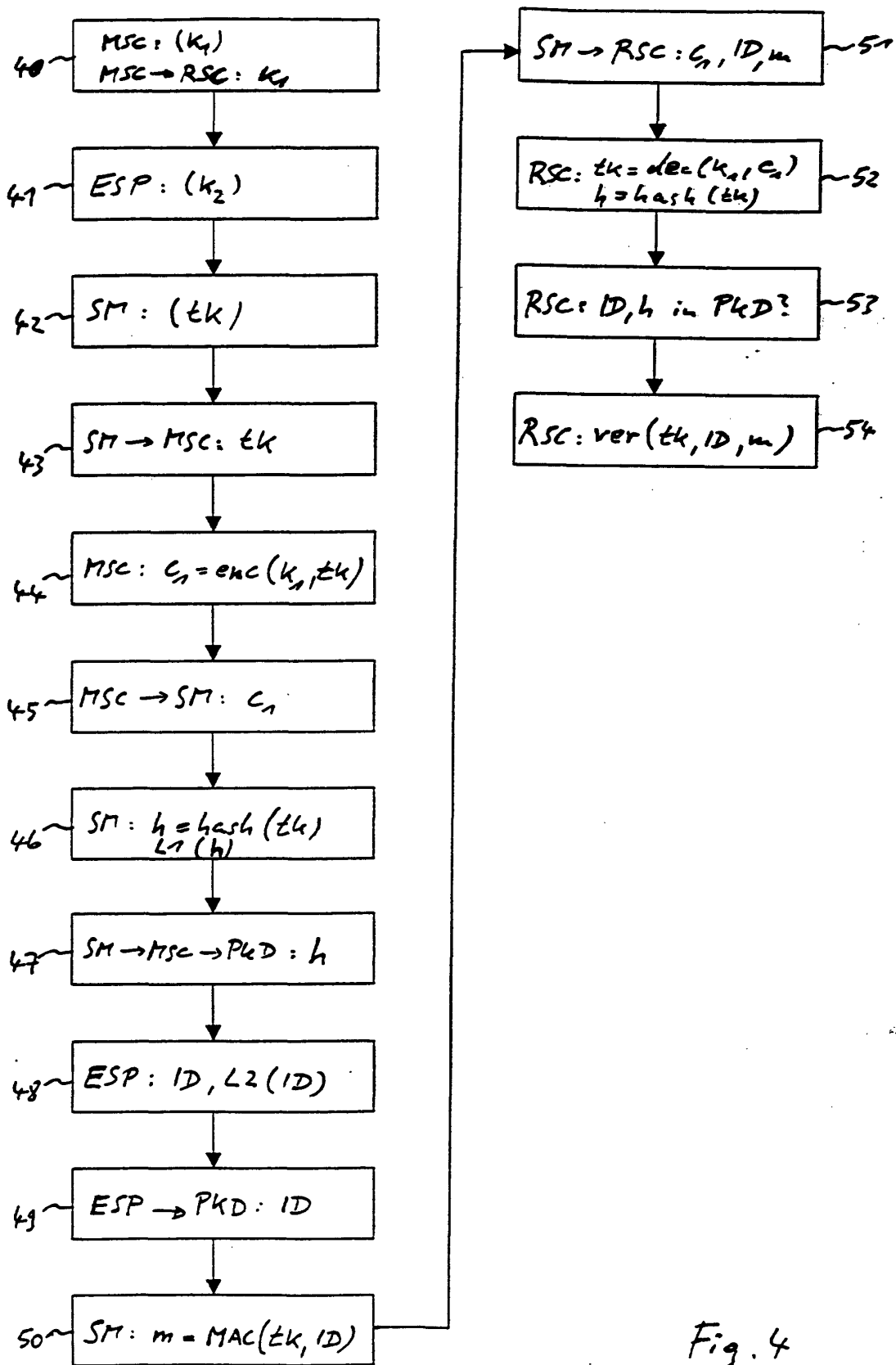


Fig. 4



Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 01 10 4610

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.CI.7)
A	EP 0 948 158 A (FRANCOTYP POSTALIA GMBH) 6. Oktober 1999 (1999-10-06) * Anspruch 1; Abbildung 1 * ---	1-16	G07B17/00
A	EP 0 735 722 A (PITNEY BOWES) 2. Oktober 1996 (1996-10-02) * Anspruch 1; Abbildung 4 * ---	1-16	
A	WO 98 57302 A (RAHRIG JOHN G ; RILEY DAVID W (US); GRAVELL LINDA V (US); PINTSOV L) 17. Dezember 1998 (1998-12-17) * Anspruch 1; Abbildung 2 * ---	1-16	
A	"INFORMATION-BASED INDICIA PROGRAM (IBIP) PERFORMANCE CRITERIA FOR INFORMATION-BASED INDICIA AND SECURITY ARCHITECTURE FOR CLOSED IBI POSTAGE METERING SYSTEMS" INFORMATION BASED INDICIA PROGRAM HOST SYSTEM SPECIFICATION, XX, XX, 12. Januar 1999 (1999-01-12), Seite COMPLETE XP002138350 * das ganze Dokument * -----	1-16	
			RECHERCHIERTE SACHGEBIETE (Int.CI.7)
			G07B
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort DEN HAAG		Abschlußdatum der Recherche 25. Juni 2001	Prüfer Kirsten, K
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 : mündliche 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	

EPO FORM 1503 03.02 (P04003)

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT
ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 01 10 4610

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.

25-06-2001

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0948158 A	06-10-1999	DE 19816344 A	07-10-1999
EP 0735722 A	02-10-1996	US 5812666 A	22-09-1998
		BR 9601231 A	06-01-1998
		CA 2173008 A	01-10-1996
		CN 1147656 A	16-04-1997
		JP 9149021 A	06-06-1997
WO 9857302 A	17-12-1998	AU 7961998 A	30-12-1998
		AU 7963898 A	30-12-1998
		AU 8255898 A	30-12-1998
		AU 8256698 A	30-12-1998
		AU 8567098 A	30-12-1998
		AU 8567298 A	30-12-1998
		BR 9805995 A	31-08-1999
		BR 9806225 A	21-03-2000
		CN 1234890 T	10-11-1999
		CN 1234891 T	10-11-1999
		EP 0925558 A	30-06-1999
		EP 0931299 A	28-07-1999
		EP 0925663 A	30-06-1999
		EP 0920679 A	09-06-1999
		EP 0966728 A	29-12-1999
		EP 0960394 A	01-12-1999
		WO 9857303 A	17-12-1998
		WO 9857460 A	17-12-1998
		WO 9857304 A	17-12-1998
		WO 9857305 A	17-12-1998
		WO 9857306 A	17-12-1998

EPO FORM P461

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