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

(11) EP 1 455 311 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
08.09.2004 Patentblatt 2004/37

(51) Int Cl.[7]: **G07B 17/04**

(21) Anmeldenummer: **04090094.6**

(22) Anmeldetag: **05.03.2004**

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

(30) Priorität: **05.03.2003 DE 10309817**

(71) Anmelder: **Francotyp-Postalia AG & Co. KG**
16547 Birkenwerder (DE)

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

(74) Vertreter: **Karlhuber, Mathias**
COHAUSZ & FLORACK
Patent- und Rechtsanwälte
Bleichstrasse 14
40211 Düsseldorf (DE)

(54) Verfahren zum sicheren Datenaustausch

(57) Verfahren zum sicheren Datenaustausch zwischen einer ersten Datenverarbeitungseinheit (1) und einer zweiten Datenverarbeitungseinheit (2), bei dem in einem Kommunikationsaufbauschritt (20) ein sicherer Kommunikationskanal zwischen der ersten Datenverarbeitungseinheit (1) und der zweiten Datenverarbeitungseinheit (2) hergestellt wird und in einem Datenübermittlungsschritt (22) über den sicheren Kommunikationskanal eine erste Nachricht von der zweiten Datenverarbeitungseinheit (2) an die erste Datenverarbeitungseinheit (1) übersandt wird, wobei in dem Datenübermittlungsschritt (22) in der zweiten Datenverarbeitungseinheit (2) eine zweite Nachricht generiert wird, indem ein vorgegebener Anhang an die erste Nachricht angehängt wird, eine dritte Nachricht generiert wird, indem die zweite Nachricht unter Verwendung eines geheimen Schlüssels verschlüsselt wird, der nur in der ersten Datenverarbeitungseinheit (1) und der zweiten Datenverarbeitungseinheit (2) vorhanden ist, und die dritte Nachricht an die erste Datenverarbeitungseinheit (1) übersandt wird. Anordnung zur Durchführung des Verfahrens.

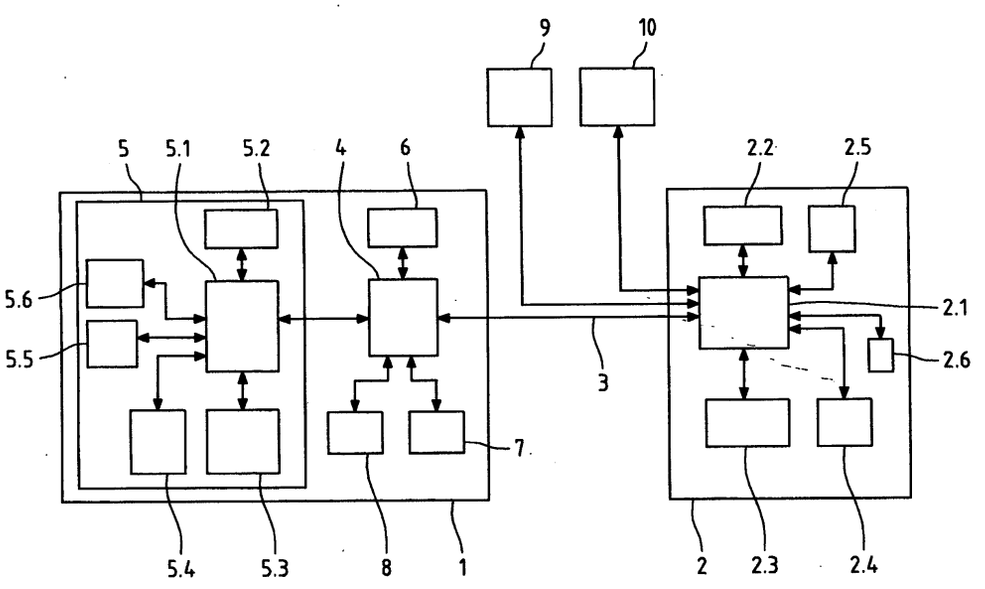

Fig.1

EP 1 455 311 A2

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum sicheren Datenaustausch zwischen einer ersten Datenverarbeitungseinheit und einer zweiten Datenverarbeitungseinheit, bei dem in einem Kommunikationsaufbauschritt ein sicherer Kommunikationskanal zwischen der ersten Datenverarbeitungseinheit und der zweiten Datenverarbeitungseinheit hergestellt wird und in einem Datenübermittlungsschritt über den sicheren Kommunikationskanal eine erste Nachricht von der zweiten Datenverarbeitungseinheit an die erste Datenverarbeitungseinheit übersandt wird. Sie betrifft weiterhin eine Anordnung, die zur Durchführung des erfindungsgemäßen Verfahrens geeignet ist.

[0002] Für eine Vielzahl von Diensten, die mit Hilfe von Datenverarbeitungseinheiten durchgeführt werden, ist es erforderlich, in der Datenverarbeitungseinheit stets die aktuellste Version der zur Durchführung des Dienstes notwendigen Dienstdaten verfügbar zu haben. So ist es beispielsweise bei Frankiermaschinen zur Berechnung des Portowertes für den jeweiligen zu frankierenden Brief erforderlich, stets die aktuellsten Gebührentabellen zu verwenden. Nur so kann der von dem jeweiligen Brief beförderе vorgegebene korrekte Portowert bestimmt und somit eine reibungslose Beförderung des Briefes sichergestellt werden. Vergleichbares gilt für andere Dienste, bei denen das zu bezahlende Entgelt oder andere für die Durchführung des Dienstes erforderliche Daten anhand von solchen Dienstdaten bestimmt wird.

[0003] Solche Dienstdaten werden in ihrer aktuellsten Version in der Regel von dem Anbieter des Dienstes selbst oder einem Dritten zur Verfügung gestellt. Hierbei ist es häufig der Fall, dass die Dienstdaten in einer zweiten Datenverarbeitungseinheit, meist in Form einer Datenzentrale oder dergleichen, zum Herunterladen bereitgestellt werden. Beim Herunterladen werden die Dienstdaten über eine Kommunikationsverbindung in einem Datennetz oder dergleichen übertragen, mit dem beide Datenverarbeitungseinheiten verbunden sind. Hierbei ist es insbesondere im Zusammenhang mit abrechnungsrelevanten oder sicherheitsrelevanten Dienstdaten wichtig, sicherzustellen, dass die Dienstdaten bei der Übertragung nicht manipuliert werden. Diese Manipulationssicherheit soll meist durch den Einsatz kryptographischer Mittel gewährleistet sein.

[0004] So ist aus der US 5,448,641 ist in diesem Zusammenhang bekannt, die Gebührentabellen für Frankiermaschinen zusammen mit einer digitalen Signatur zu versenden, die unter Verwendung der zu versendenden Gebührentabelle erstellt wurde. Zur Erstellung der digitalen Signatur wird die Gebührentabelle oder ein vorgegebener Teil der Gebührentabelle in der Datenzentrale zunächst einen so genannten Hash-Algorithmus, beispielsweise dem Secure Hash Algorithm (SHA), unterworfen, mit dem ein so genannter Nachrichtenkern erzeugt wird. Dieser Nachrichtenkern wird dann mit einem geheimen Schlüssel verschlüsselt. Der so verschlüsselte Nachrichtenkern bildet dann die digitale Signatur.

[0005] Um in der Frankiermaschine zu überprüfen, ob die Gebührentabelle während der Übertragung manipuliert wurde, wird zum einen die digitale Signatur entschlüsselt, um den Nachrichtenkern zu erhalten. Zum anderen wird aus der übersandten Gebührentabelle bzw. dem vorgegebenen Teil der Gebührentabelle mit demselben Hash-Algorithmus ein neuer Nachrichtenkern berechnet und überprüft, ob der neue Nachrichtenkern dem aus der digitalen Signatur gewonnenen Nachrichtenkern entspricht. Da solche Hash-Algorithmen die Eigenschaft haben, dass schon eine äußerst geringe Veränderung der Eingangsinformation eine starke Abweichung im Ergebnis der Berechnung hervorruft, ist bei eine Übereinstimmung der beiden Nachrichtenkerne davon auszugehen, dass keine Manipulation stattgefunden hat und die Gebührentabelle demgemäß verwendet werden kann.

[0006] Mit diesem Verfahren kann zwar eine vergleichsweise hohe Sicherheit erreicht werden, dass Manipulationen an den Dienstdaten, also den Gebührentabellen, während der Übertragung nicht unerkannt bleiben. Es weist jedoch den Nachteil auf, dass es relativ aufwändig ist. So muss zum einen in der Frankiermaschine der entsprechende Hash-Algorithmus vorhanden sein. Zum anderen ist bei der Integritätsprüfung vergleichsweise viel Rechenaufwand erforderlich, da für den Vergleich nicht nur die Entschlüsselung der Signatur sondern auch die Erzeugung des neuen Nachrichtenkerns erfolgen muss.

[0007] Aus der EP 0 969 420 A2 ist im Zusammenhang mit der Aktualisierung von Gebührentabellen bei Frankiermaschinen weiterhin bekannt, zur Überprüfung der Integrität der von einer Datenzentrale übersandten Gebührentabelle einen so genannten MAC (Message Authentication Code) zu verwenden. Dabei wird in der Frankiermaschine aus der Gebührentabelle durch einen vorgegebenen Prüfsummenalgorithmus zunächst eine Prüfsumme generiert, die dann zur Bildung des MAC mit einem geheimen Schlüssel verschlüsselt wird. Dieser MAC wird an die Datenzentrale zurückgesandt. Die Datenzentrale generiert aus der zuvor versandten Gebührentabelle mit demselben Prüfsummenalgorithmus zunächst eine neue Prüfsumme, die dann mit dem geheimen Schlüssel verschlüsselt wird, um einen neuen MAC' zu bilden. Stimmt diese neue MAC' mit dem von der Frankiermaschine übersandten MAC überein, wird angenommen, dass die Übertragung ohne Manipulationen erfolgte und es wird eine entsprechende Nachricht eine Frankiermaschine gesandt, welche die Gebührentabelle dann akzeptiert.

[0008] Bei dieser Variante besteht ebenfalls das Problem, dass sie vergleichsweise aufwändig ist, da zum einen wiederum ein entsprechender Prüfsummenalgorithmus in beiden Daten Verarbeitungseinheit vorhanden sein muss. Zum anderen ist eine Reihe von Kom-

munikationsschritten erforderlich ist, um die Aktualisierung der Dienstdaten abzuschließen. Hier bieten sich wieder eine Reihe von Manipulationsmöglichkeiten, denen der entsprechende Maßnahmen entgegengewirkt werden muss.

[0009] Der vorliegenden Erfindung liegt daher die Aufgabe zu Grunde, ein Verfahren bzw. eine Anordnung der eingangs genannten Art zur Verfügung zu stellen, welches bzw. welche die oben genannten Nachteile nicht oder zumindest in geringerem Maße aufweist und insbesondere einen einfachen und zuverlässig sicheren Datenaustausch gewährleistet.

[0010] Die vorliegende Erfindung löst diese Aufgabe ausgehend von einem Verfahren gemäß dem Oberbegriff des Anspruchs 1 durch die im kennzeichnenden Teil des Anspruchs 1 angegebenen Merkmale. Sie löst diese Aufgabe weiterhin ausgehend von einer Anordnung gemäß dem Oberbegriff des Anspruchs 15 durch die im kennzeichnenden Teil des Anspruchs 15 angegebenen Merkmale.

[0011] Der vorliegenden Erfindung liegt die technische Lehre zu Grunde, dass man einen einfachen und zuverlässig sicheren Datenaustausch gewährleisten kann, wenn in dem Datenübermittlungsschritt in der zweiten Datenverarbeitungseinheit zunächst eine zweite Nachricht generiert wird, indem ein vorgegebener Anhang an die erste Nachricht angehängt wird. Anschließend wird eine dritte Nachricht generiert, indem die zweite Nachricht unter Verwendung eines geheimen Schlüssels verschlüsselt wird, der nur in der ersten Datenverarbeitungseinheit und der zweiten Datenverarbeitungseinheit vorhanden ist. Schließlich wird die dritte Nachricht an die erste Datenverarbeitungseinheit übersandt.

[0012] Die Verschlüsselung der zweiten Nachricht mit dem geheimen Schlüssel stellt dabei sicher, dass die Daten bei der Übertragung nicht manipuliert werden können. Der Anhang an der ersten Nachricht bietet eine einfache, zusätzliche Möglichkeit, eventuelle Manipulationen zu erkennen, ohne dass hierfür aufwändige Prüfalgorithmen erforderlich wären.

[0013] Hierbei kann zum einen vorgesehen sein, dass neben der dritten Nachricht auch die erste Nachricht an die erste Datenverarbeitungseinheit übersandt wird. Bevorzugt wird nur die dritte Nachricht an die erste Datenverarbeitungseinheit übersandt, da diese ohnehin die erste Nachricht enthält. Diese erste Nachricht kann dann durch eine einfache Entschlüsselung und eine einfache weitere Trennung aus der dritten Nachricht isoliert werden.

[0014] Mit dem erfindungsgemäßen Verfahren ist in der ersten Datenverarbeitungseinhelt bei einer späteren Integritätsprüfung lediglich eine einfache Verschlüsselung bzw. Entschlüsselung und ein einfacher Vergleich der so gewonnenen Daten erforderlich.

[0015] So kann für den Fall, dass die erste Nachricht zusammen mit der dritten Nachricht übersandt wird, zum einen vorgesehen sein, dass in der ersten Datenverarbeitungseinheit zur Integritätsprüfung zunächst an die erste Nachricht der vorgegebene Anhang angehängt wird, um so eine neue zweite Nachricht zu bilden. Diese neue zweite Nachricht wird dann mit dem geheimen Schlüssel verschlüsselt, um so eine neue dritte Nachricht zu generieren. Stimmt diese neue dritte Nachricht mit der übersandten dritten Nachricht überein, wird angenommen, dass keine Manipulationen bei der Übertragung erfolgt sind.

[0016] Vorzugsweise wird in einem Entschlüsselungsschritt die dritte Nachricht in der ersten Datenverarbeitungseinheit unter Verwendung des geheimen Schlüssels entschlüsselt und die zweite Nachricht in einem nachfolgenden Integritätsprüfungsschritt auf ihre Integrität überprüft. Hierbei kann für den Fall, dass die erste Nachricht zusammen mit der dritten Nachricht übersandt wird, zum einen vorgesehen sein, dass zunächst an die erste Nachricht der vorgegebene Anhang angehängt wird, um so eine neue zweite Nachricht zu bilden. Stimmt diese neue zweite Nachricht dann mit der durch die Entschlüsselung der übersandten dritten Nachricht gewonnenen zweiten Nachricht überein, wird angenommen, dass keine Manipulationen bei der Übertragung erfolgt sind.

[0017] Bei bevorzugten Varianten des erfindungsgemäßen Verfahrens mit einem geringen zu übertragenden und bei der Integritätsprüfung zu bewältigenden Datenvolumen ist vorgesehen, dass zur Integritätsprüfung in dem Integritätsprüfungsschritt der Anhang aus der zweiten Nachricht isoliert wird und überprüft wird, ob der Anhang einem vorgegebenen Anhang entspricht. Hierbei ist es insbesondere nicht erforderlich, dass die erste Nachricht zusammen mit der dritten Nachricht übermittelt wird.

[0018] Bei dem Anhang kann es sich grundsätzlich um einen beliebig gestalteten Anhang handeln, der in beiden Datenverarbeitungseinheiten vorhanden ist. Um die Sicherheit zu erhöhen, wird dieser Anhang vorzugsweise von Zeit zu Zeit ausgewechselt, beispielsweise in fest vorgegebenen Intervallen oder aber auch in zufällig bestimmten Intervallen. Um die jeweils in den Datenverarbeitungseinheiten zu speichernden Datenmengen gering zu halten, ist der Anhang vorzugsweise zumindest ein Teil des geheimen Schlüssels. Um welchen Teil des geheimen Schlüssels es sich dabei handelt, kann fest vorgegeben sein, wobei auch hier der vorgegebene Teil von Zeit zu Zeit variieren kann. Ebenso kann vorgesehen sein, dass der vorgegebene Teil mit einer festen oder zufällig ermittelten Anzahl von Datenaustauschvorgängen variiert. Insbesondere kann vorgesehen sein, dass er sich mit jedem Datenaustauschvorgang ändert.

[0019] Bei dem geheimen Schlüssel kann es sich grundsätzlich um einen beliebigen für derartige kryptographische Anwendungen geeigneten Schlüssel handeln. Es muss lediglich sichergestellt sein, dass er auf entsprechend sichere Weise in die beiden Datenverarbeitungseinheiten eingebracht wurde, um ein ausrei-

chendes Maß an Sicherheit zu gewährleisten. Das sichere Einbringen von kryptographischen Schlüsseln in Datenverarbeitungseinheiten ist hinlänglich bekannt, sodass hierauf nicht näher eingegangen werden soll.

[0020] Bei bevorzugten Varianten des erfindungsgemäßen Verfahrens wird die Sicherheit dadurch erhöht, dass der geheime Schlüssel ein geheimer Sitzungsschlüssel ist, der in dem Kommunikationsaufbauschritt generiert wird. Die Möglichkeit von Manipulationen wird hierdurch deutlich eingeschränkt, da der geheime Schlüssel vor Aufbau der Kommunikation nicht bekannt ist und daher nicht vorab kompromittiert werden kann.

[0021] Der geheime Schlüssel kann dabei grundsätzlich in beliebiger geeigneter Weise nach beliebigen, hinlänglich bekannten Verfahren zum Generieren solcher kryptographischer Schlüssel erzeugt werden. Vorzugsweise wird der geheime Schlüssel generiert, indem zum einen ein erster Teilschlüssel in der ersten Datenverarbeitungseinheit generiert und an die zweite Datenverarbeitungseinheit gesandt wird. Zum anderen wird ein zweiter Teilschlüssel in der zweiten Datenverarbeitungseinheit generiert und an die erste Datenverarbeitungseinheit gesandt. Schließlich wird der geheime Schlüssel in der ersten Datenverarbeitungseinheit und in der zweiten Datenverarbeitungseinheit aus dem ersten Teilschlüssel und dem zweiten Teilschlüssel nach einem vorgebbaren Schlüsselerzeugungsschema generiert. Dieses Verfahren hat den Vorteil, dass der geheime Schlüssel nie als Ganzes zwischen den beiden Datenverarbeitungseinheiten ausgetauscht werden muss, wodurch sich ein Zugriff auf den geheimen Schlüssel weiter erschwert.

[0022] Bei dem Schlüsselerzeugungsschema kann es sich um einen beliebigen vorgebbaren Algorithmus handeln. Bei besonders einfachen Varianten wird der geheime Schlüssel einfach aus dem ersten Teilschlüssel und dem zweiten Teilschlüssel zusammengesetzt.

[0023] Der geheime Schlüssel kann sobald er einmal generiert wurde dauerhaft verwendet werden. Um die Sicherheit zu erhöhen, ist jedoch bevorzugt vorgesehen, dass der geheime Schlüssel ein temporärer Schlüssel ist, der nur vorübergehend verwendet und wie oben beschrieben nach einer bestimmten Zeit ausgetauscht wird.

[0024] Bei weiteren vorteilhaften Ausgestaltungen des erfindungsgemäßen Verfahrens wird das Ergebnis der Integritätsprüfung an die zweite Datenverarbeitungseinheit zurückgemeldet. Hierzu ist ein entsprechender Bestätigungsschritt vorgesehen. Im Fall der Feststellung der Integrität der zweiten Nachricht im Integritätsprüfungsschritt wird dabei eine positive Bestätigungsnachricht von der ersten Datenverarbeitungseinheit an die zweite Datenverarbeitungseinheit gesandt. Diese Bestätigungsnachricht kann wiederum die erste Nachricht enthalten, um auch in der zweiten Datenverarbeitungseinheit eine erneute Integritätsprüfung zu ermöglichen.

[0025] Alternativ oder zusätzlich kann vorgesehen sein, dass im Fall der Feststellung fehlender Integrität der zweiten Nachricht im Integritätsprüfungsschritt anschließend eine negative Bestätigungsnachricht von der ersten Datenverarbeitungseinheit an die zweite Datenverarbeitungseinheit gesandt wird. Für diesen Fall kann im Übrigen ein Fehlermodus vorgesehen sein, der beispielsweise die zweite Datenverarbeitungseinheit für eine vorgegebene Anzahl von Versuchen dazu veranlasst, die vorherigen Schritte zu wiederholen, insbesondere die zuvor gesandten Daten erneut zu senden, um eine fehlerfreie Übertragung der ersten Nachricht zu versuchen. Erhält die zweite Datenverarbeitungseinheit auch nach der vorgegebenen Anzahl von Versuchen keine positive Bestätigungsnachricht, bricht sie die Kommunikation mit der ersten Datenverarbeitungseinheit ab. Vorzugsweise werden zumindest im Fall solcher Fehler, welche den Ablauf vorgegebener Fehlerroutinen erzwingen, sämtliche Schritte der jeweiligen Datenverarbeitungseinheit für die spätere Weiterverwendung protokolliert und gespeichert.

[0026] Bei bevorzugten Varianten des erfindungsgemäßen Verfahrens ist vorgesehen, dass der sichere Kommunikationskanal zumindest nach Erhalt der positiven Bestätigungsnachricht durch die zweite Datenverarbeitungseinheit in einem Kommunikationsabbruchschritt geschlossen wird und der geheime Schlüssel sowohl in der ersten Datenverarbeitungseinheit als auch in der zweiten Datenverarbeitungseinheit vernichtet wird. Dasselbe geschieht bevorzugt, wenn in dem oben beschriebenen Fehlermodus die vorgegebene Anzahl von Fehlversuchen erreicht wurde.

[0027] Weitere vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens zeichnen sich dadurch aus, dass die erste Datenverarbeitungseinheit ein erstes Verarbeitungsmodul und ein damit verbundenes Sicherheitsmodul umfasst, wobei der Entschlüsselungsschritt durch das Sicherheitsmodul durchgeführt wird. Hierdurch ist es möglich, die sicherheitsrelevanten Vorgänge in einem entsprechend begrenzten, abgesicherten und einfacher zu kontrollierenden Bereich ablaufen zu lassen. Bevorzugt wird daher auch der Integritätsprüfungsschritt und zusätzlich oder Alternativ der Bestätigungsschritt durch das Sicherheitsmodul durchgeführt.

[0028] Vorzugsweise ist hierbei vorgesehen, dass das Verarbeitungsmodul bei Feststellung der Integrität der zweiten Nachricht zumindest einen Teil der ersten Nachricht zur weiteren Verwendung in einem mit dem Verarbeitungsmodul verbundenen Speicher ablegt. Bei Feststellung fehlender Integrität der zweiten Nachricht schaltet das Verarbeitungsmodul und zusätzlich oder alternativ das Sicherheitsmodul jedoch in einen Fehlermodus. In einem solchen Fehlermodus kann die entsprechende Einrichtung jeweils für einen weiteren Betrieb gesperrt sein. Weiterhin kann eine entsprechende Fehlernachricht bzw. ein entsprechendes Fehlersignal an dem Benutzer der ersten Datenverarbeitungseinheit ausgegeben werden, um ihn über den Fehlerzustand zu

informieren. Ebenso kann vorgesehen sein, dass automatisch eine entsprechende Fehlernachricht an die zweite Datenverarbeitungseinheit oder an andere Einrichtungen Dritter übermittelt wird. Im Fall einer Frankiermaschine kann dies beispielsweise das Datenzentrum des Herstellers aber auch das Datenzentrum eines betroffenen Postbeförderers sein.

[0029] Bei weiteren vorteilhaften Varianten des erfindungsgemäßen Verfahrens ist vorgesehen, dass die erste Nachricht eine Information und eine digitale Signatur der zweiten Datenverarbeitungseinheit über der ersten Information umfasst. Mit einer solchen digitalen Signatur wird zum einen eine weitere Absicherung der zu übermittelnden Daten erzielt. Zum anderen bietet eine solche digitale Signatur die Möglichkeit, die Integrität der durch die erste Datenverarbeitungseinheit verwendeten Daten nicht nur in dem Integritätsprüfungsschritt unmittelbar nach der Datenübertragung sondern auch zu einem späteren Zeitpunkt zu überprüfen, sofern die digitale Signatur in der ersten Datenverarbeitungseinheit gespeichert wird.

[0030] Hierzu ist bevorzugt vorgesehen, dass der Integritätsprüfungsschritt zumindest teilweise zu vorgebbaren Zeitpunkten wiederholt wird. Dies kann beispielsweise nach Ablauf einer bestimmten Nutzungszeit der ersten Datenverarbeitungseinheit, nach einer bestimmten Anzahl von Nutzungen der ersten Datenverarbeitungseinheit oder nach einer bestimmten Anzahl von Einschaltvorgängen der ersten Datenverarbeitungseinheit, insbesondere mit jedem Einschalten der ersten Datenverarbeitungseinheit, der Fall sein.

[0031] Die digitale Signatur kann in beliebiger geeigneter Weise mittels hinlänglich bekannter Signaturalgorithmen generiert und im Integritätsprüfungsschritt verifiziert werden. Hierbei können Signaturalgorithmen mit Nachrichtenwiederherstellung verwendet werden, die bei der Verifizierung der Signatur die der Signatur zugrundeliegende Nachricht wiederherstellen und diese mit der übersandten Nachricht vergleichen. Ein Beispiel für einen solchen Signaturalgorithmus mit Nachrichtenwiederherstellung ist der RSA-Signaturalgorithmus. Im Hinblick auf den erforderlichen Berechnungsaufwand finden jedoch bevorzugt Signaturalgorithmen ohne Nachrichtenwiederherstellung Anwendung, bei denen es im Rahmen der Verifikation der Signatur zu keiner Rekonstruktion der Nachricht kommt, die der Signatur zugrunde liegt. Beispiele für derartige Signaturalgorithmen ohne Nachrichtenwiederherstellung sind ElGamal und dessen Abwandlungen (zum Beispiel Schnorr-Signaturen), DSA, Gost, ECDSA, ESIGN und GMR. Derartige Signaturalgorithmen ohne Nachrichtenwiederherstellung bieten im Übrigen auch schon bei der Anwendung im Rahmen der eingangs beschriebenen bekannten Verfahren bei einer Reduktion des Berechnungsaufwandes den Vorteil einer zusätzlichen Erhöhung der Sicherheit, da es mit ihnen nicht möglich ist, die der Signatur zugrundeliegende Nachricht zu rekonstruieren.

[0032] Die vorliegende Erfindung betrifft weiterhin eine Anordnung zum sicheren Datenaustausch mit einer ersten Datenverarbeitungseinheit und einer zweiten Datenverarbeitungseinheit, die zum Aufbau eines sicheren Kommunikationskanals und zur Übermittlung einer ersten Nachricht von der zweiten Datenverarbeitungseinheit an die erste Datenverarbeitungseinheit über den sicheren Kommunikationskanal ausgebildet sind. Erfindungsgemäß ist ein geheimer Schlüssel vorgesehen, der ausschließlich in der ersten Datenverarbeitungseinheit und in der zweiten Datenverarbeitungseinheit gespeichert ist. Weiterhin ist vorgesehen, dass die zweite Datenverarbeitungseinheit zum Generieren einer zweiten Nachricht durch Anhängen eines vorgegebenen Anhangs an die erste Nachricht ausgebildet ist. Weiterhin ist sie zum Generieren einer dritten Nachricht durch Verschlüsselung der zweiten Nachricht unter Verwendung des geheimen Schlüssels ausgebildet. Schließlich ist sie zum Übersenden der dritten Nachricht an die erste Datenverarbeitungseinheit über den sicheren Kommunikationskanal ausgebildet.

[0033] Die erfindungsgemäße Anordnung eignet sich zur Durchführung des erfindungsgemäßen Verfahrens. Mit ihr lassen sich die oben beschriebenen Vorteile und Funktionen des erfindungsgemäßen Verfahrens in derselben Weise realisieren, sodass an dieser Stelle auf die obigen Ausführungen Bezug genommen wird.

[0034] Die oben im Zusammenhang mit dem erfindungsgemäßen Verfahren beschriebenen Funktionen lassen sich dabei auf beliebige Weise realisieren. So können je nach Komplexität der Funktion beispielsweise anwendungsspezifisch konfigurierte integrierte Schaltkreise (ASIC) ebenso Verwendung finden wie Softwarelösungen, bei denen die Funktion durch eine Verarbeitungseinheit zur Verfügung gestellt wird, die hierbei auf entsprechende Programme und Daten zugreift, die in einem mit der Verarbeitungseinheit verbundenen Speicher abgelegt sind.

[0035] Vorzugsweise ist die erste Datenverarbeitungseinheit zum Entschlüsseln der dritten Nachricht unter Verwendung des geheimen Schlüssels und zur Durchführung einer Integritätsprüfung an der zweiten Nachricht ausgebildet. Um die oben beschriebene Integritätsprüfung durchführen zu können, ist die erste Datenverarbeitungseinheit bevorzugt zum Isolieren des Anhangs aus der zweiten Nachricht und zum Vergleich des Anhangs mit einem vorgegebenen Anhang ausgebildet.

[0036] Vorzugsweise ist der geheime Schlüssel wie erwähnt ein geheimer Sitzungsschlüssel, der bevorzugt nur für die jeweils aktuelle Sitzung generiert, verwendet und nach Beendigung der Sitzung vernichtet wird. Das Generieren des Sitzungsschlüssels kann sowohl in der ersten Datenverarbeitungseinheit als auch in der zweiten Datenverarbeitungseinheit erfolgen, die dementsprechend dann jeweils zum Generieren des geheimen Schlüssels und zum Übersenden des generierten Sitzungsschlüssels an die andere Datenverarbeitungsein-

heit ausgebildet ist. In der jeweiligen Datenverarbeitungseinheit ist hierzu beispielsweise ein entsprechender Schlüsselgenerierungsalgorithmus gespeichert, auf den die jeweilige Datenverarbeitungseinheit dann zurückgreift.

[0037] Vorzugsweise wird der geheime Sitzungsschlüssel unter Verwendung beider Datenverarbeitungseinheiten generiert, ohne dass er als Ganzes zwischen den beiden Datenverarbeitungseinheiten ausgetauscht wird. Dabei ist die erste Datenverarbeitungseinheit zum Generieren eines ersten Teilschlüssels und zum Übersenden des ersten Teilschlüssels an die zweite Datenverarbeitungseinheit ausgebildet. Die zweite Datenverarbeitungseinheit ist zum Generieren eines zweiten Teilschlüssels und zum Übersenden des zweiten Teilschlüssels an die erste Datenverarbeitungseinheit ausgebildet. Schließlich ist in beiden Datenverarbeitungseinheiten ein entsprechendes Schlüsselerzeugungsschema vorhanden, nach dem die jeweilige Datenverarbeitungseinheit den geheimen Schlüssel aus dem ersten Teilschlüssel und dem zweiten Teilschlüssel generiert.

[0038] Die erste Datenverarbeitungseinheit ist wie erwähnt zur Durchführung der Integritätsprüfung ausgebildet. Hierbei ist sie weiterhin bevorzugt zum Übersenden einer positiven Bestätigungsnachricht an die zweite Datenverarbeitungseinheit im Fall der Feststellung der Integrität der zweiten Nachricht ausgebildet. Zusätzlich oder alternativ ist sie zum Übersenden einer negativen Bestätigungsnachricht an die zweite Datenverarbeitungseinheit im Fall der Feststellung fehlender Integrität der zweiten Nachricht ausgebildet. Die zweite Datenverarbeitungseinheit ist weiterhin bevorzugt so ausgebildet, dass sie den sicheren Kommunikationskanal zumindest nach Erhalt der positiven Bestätigungsnachricht schließt. Wird der Kommunikationskanal geschlossen, vernichtet dann sowohl die erste Datenverarbeitungseinheit als auch die zweite Datenverarbeitungseinheit den geheimen Sitzungsschlüssel.

[0039] Die erfindungsgemäße Anordnung kann grundsätzlich in beliebiger geeigneter Weise aufgebaut sein. Die oben beschriebenen Funktionen des erfindungsgemäßen Verfahrens können dabei auf beliebige geeignete Weise durch entsprechend anwendungsspezifisch konfigurierte Hardware oder durch Standardbauteile und anwendungsspezifische Software realisiert werden. Bevorzugt umfasst die erste Datenverarbeitungseinheit ein erstes Verarbeitungsmodul und ein damit verbundenes Sicherheitsmodul, das zumindest zum Entschlüsseln der dritten Nachricht ausgebildet ist. Vorzugsweise ist das Sicherheitsmodul auch zur Durchführung der Integritätsprüfung und zusätzlich oder alternativ auch zum Übersenden einer Bestätigungsnachricht in Abhängigkeit vom Ergebnis der Integritätsprüfung ausgebildet.

[0040] Bei bevorzugten Varianten der erfindungsgemäßen Anordnung ist das Verarbeitungsmodul zum Speichern zumindest eines Teils der ersten Nachricht bei Feststellung der Integrität der zweiten Nachricht ausgebildet. Die erste Nachricht wird dabei zur weiteren Verwendung in einem mit dem Verarbeitungsmodul verbundenen Speicher abgelegt. Für den Fall, dass fehlende Integrität der zweiten Nachricht festgestellt wird, ist das Verarbeitungsmodul und zusätzlich oder alternativ das Sicherheitsmodul zum Umschalten in einen oben bereits eingehend beschriebenen Fehlermodus ausgebildet.

[0041] Bei günstigen Weiterbildungen der erfindungsgemäßen Anordnung ist die zweite Datenverarbeitungseinheit zum Erstellen einer ersten digitalen Signatur über einer ersten Information und zum Erstellen der ersten Nachricht aus der ersten Information und der ersten digitalen Signatur ausgebildet. Hierdurch ist es wie erwähnt möglich, auch zu späteren Zeitpunkten die Integrität der verwendeten Daten zu überprüfen. Hierzu ist erste Datenverarbeitungseinheit zur zumindest teilweisen Wiederholung der Integritätsprüfung zu vorgebbaren Zeiten ausgebildet.

[0042] Die Erfindung lässt sich im Zusammenhang mit beliebigen Anwendungen einsetzen, bei denen Daten auf entsprechend abgesicherte Weise von einer ersten Datenverarbeitungseinheit zu einer zweiten Datenverarbeitungseinheit übermittelt werden müssen. Hierbei kann sie wie erwähnt im Zusammenhang mit beliebigen Diensten verwendet werden, die mit Hilfe von Datenverarbeitungseinheiten durchgeführt werden und bei denen es erforderlich ist, in der ersten Datenverarbeitungseinheit stets die aktuellste Version der zur Durchführung des Dienstes notwendigen Dienstdaten verfügbar zu haben.

[0043] Dank des geringen zu übertragenden Datenvolumens ist die Anwendung der Erfindung bei Konstellationen von besonderem Vorteil, bei denen eine zentrale zweite Datenverarbeitungseinheit, beispielsweise eine entfernte Datenzentrale, mehrere erste Datenverarbeitungseinheiten mit entsprechenden Dienstdaten versorgen muss. Besonders vorteilhaft lässt sich die Erfindung im Zusammenhang mit Frankiermaschinen einsetzen. Vorzugsweise ist die erste Datenverarbeitungseinheit daher eine Frankiermaschine.

[0044] Die vorliegende Erfindung betrifft weiterhin eine Datenverarbeitungseinheit, welche die Merkmale der oben beschriebenen ersten Datenverarbeitungseinheit oder der oben beschriebenen zweiten Datenverarbeitungseinheit der erfindungsgemäßen Anordnung aufweist.

[0045] 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 zeigen

Figur 1 eine schematische Darstellung einer bevorzugten Ausführungsform der erfindungsgemäßen Anordnung zur Durchführung des erfindungsgemäßen Verfahrens;

Figur 2 ein schematisches Ablaufdiagramm des erfindungsgemäßen Verfahrens bei der Anordnung aus Figur 1;

Figur 2A ein erstes Detail des Ablaufdiagramms aus Figur 2;

Figur 2B ein zweites Detail des Ablaufdiagramms aus Figur 2;

Figur 2C ein drittes Detail des Ablaufdiagramms aus Figur 2.

[0046] Figur 1 zeigt eine schematische Darstellung einer bevorzugten Ausführungsform der erfindungsgemäßen Anordnung zur Durchführung des erfindungsgemäßen Verfahrens. Die Anordnung umfasst eine erste Datenverarbeitungseinheit in Form einer Frankiermaschine 1 und eine zweite Datenverarbeitungseinheit in Form einer entfernten Datenzentrale 2, die mit der Frankiermaschine 1 mittels - aus Gründen der Übersichtlichkeit nicht dargestellter - Kommunikationsmittel über eine Kommunikationsverbindung 3 zum Datenaustausch verbunden werden kann. Die Frankiermaschine 1 umfasst dabei ein Verarbeitungsmodul 4 und ein damit verbundenes Sicherheitsmodul 5, welches sicherheitsrelevante Vorgänge in der Frankiermaschine 1 abwickelt.

[0047] An die Frankiermaschine 1 soll im Rahmen eines Datenaustauschs von der Datenzentrale 2 eine erste Nachricht gesandt werden. Diese erste Nachricht enthält eine erste Information in Form einer Gebührentabelle, welche die Frankiermaschine 1 bei der Berechnung des Portowertes benutzt, der zur Beförderung eines bestimmten Poststückes durch einen Postbeförderer erforderlich ist. Wurde die Gebührentabelle unversehrt übertragen, wird sie in einem mit dem Verarbeitungsmodul 4 verbundenen Gebührentabellenspeicher 6 gespeichert. Der erforderliche Portowert für ein bestimmtes Poststück wird dann vom Verarbeitungsmodul 4 unter Zugriff auf den Gebührentabellenspeicher 6 in Abhängigkeit vom Gewicht des Poststückes und von Eingaben des Benutzers zur Versendungsart etc. berechnet. Das Gewicht des Poststückes wird über eine mit dem Verarbeitungsmodul 4 verbundene Waage 7 ermittelt. Die Eingaben des Benutzers erfolgen über eine Eingabeeinrichtung 8, die ebenfalls mit dem Verarbeitungsmodul 4 verbunden ist.

[0048] Wie der Figur 1 weiterhin zu entnehmen ist, können mit der Datenzentrale 2 noch weitere Frankiermaschinen 9 und 10 verbunden werden, die in derselben Weise ausgebildet sind wie Frankiermaschine 1.

[0049] Um zum einen zu verhindern, dass die Beförderung des Poststückes durch den Postbeförderer infolge eines zu geringen Portowertes verweigert oder mit Nachforderungen an den Empfänger verbunden wird, und zum anderen zu verhindern, dass zum anderen ein zu hoher Portowert verwendet wird, ist es erforderlich, dass in der Frankiermaschine 1 stets die unversehrte, aktuelle Gebührentabelle des Postbeförderers vorhanden ist. Hierbei ist insbesondere im Sinne des Benutzers der Frankiermaschine 1 darauf zu achten, dass die Gebührentabelle bei der Übertragung keinen Manipulationen durch Dritte unterworfen wird.

[0050] Die Übersendung der Gebührentabelle kann entweder durch die Datenzentrale 2 durch Verbindungsaufnahme mit der Frankiermaschine 1 initiiert werden, sobald eine neue Version der Gebührentabelle in der Datenzentrale 2 vorliegt. Ebenso ist jedoch möglich, dass die Übersendung der neuen Gebührentabelle erfolgt, sobald die Frankiermaschine 1 die Datenzentrale 2 kontaktiert.

[0051] Bezug nehmend auf die Figuren 1 und 2 wird im Folgenden der Ablauf des erfindungsgemäßen Verfahrens mit der erfindungsgemäßen Anordnung aus Figur 1 erläutert.

[0052] Um eine manipulationssichere Übertragung der ersten Nachricht mit der Gebührentabelle zu gewährleisten, wird zunächst in einem Kommunikationsaufbauschritt 20 über die Kommunikationsverbindung 3 zwischen der Frankiermaschine 1 und der Datenzentrale 2 ein sicherer Kommunikationskanal aufgebaut. Der Aufbau des sicheren Kommunikationskanals erfolgt in hinlänglich bekannter Weise, indem sich das Sicherheitsmodul 5 und die Datenzentrale 2 unter Zwischenschaltung des Verarbeitungsmoduls 4 unter Verwendung kryptographischer Mittel wechselseitig authentifizieren.

[0053] Bei der wechselseitigen Authentifizierung wird im vorliegenden Beispiel ein System mit öffentlichen und geheimen Schlüsseln verwendet, welches hinlänglich bekannt ist und daher an dieser Stelle nicht erläutert werden soll. Es sei nur so viel erwähnt, dass die erste Verarbeitungseinheit 5.1 des Sicherheitsmoduls 5 bei der wechselseitigen Authentifizierung auf einen ersten Speicher 5.2 zugreift, in dem neben den erforderlichen Verschlüsselungs- und Verifikationsalgorithmen sowie dem öffentlichen Schlüssel und dem geheimen Schlüssel des Sicherheitsmoduls 5 auch der öffentliche Schlüssel der Datenzentrale 2 sowie entsprechende Zertifikate gespeichert sind. Auf Seiten der Datenzentrale 2 greift deren zweite Verarbeitungseinheit 2.1 auf einen zweiten Speicher 2.2 zu, in dem neben den erforderlichen Verschlüsselungs- und Verifikationsalgorithmen sowie dem öffentlichen Schlüssel und dem geheimen Schlüssel der Datenzentrale 2 auch der öffentliche Schlüssel des Sicherheitsmoduls 5 sowie entsprechende Zertifikate gespeichert sind.

[0054] Nach erfolgreichem Aufbau des sicheren Kommunikationskanals erfolgt in einem Schlüsselgenerierungsschritt 21 in der Frankiermaschine 1 und der Datenzentrale 2 die Erzeugung eines geheimen Schlüssels in Form eines geheimen Sitzungsschlüssels, der ausschließlich in der Frankiermaschine 1 und der Datenzentrale 2 vorhanden ist..

[0055] Wie der Figur 2A zu entnehmen ist werden in dem Schlüsselgenerierungsschritt 21 zunächst in ei-

nem Teilschritt 21.1 in der ersten Verarbeitungseinheit 5.1 ein erster Teilschlüssel generiert und in der zweiten Verarbeitungseinheit 2.1 ein zweiter Teilschlüssel generiert. Die erste Verarbeitungseinheit 5.1 greift dabei auf einen dritten Speicher 5.3 zu, der einen entsprechenden Schlüsselgenerierungsalgorithmus enthält. Die zweite Verarbeitungseinheit 2.1 greift hierzu auf einen vierten Speicher 2.3 zu, der ebenfalls einen entsprechenden Schlüsselgenerierungsalgorithmus enthält. Es versteht sich hierbei, dass das Generieren der Teilschlüssel bei anderen Varianten der Erfindung auch schon vor der Herstellung des sicheren Kommunikationskanals erfolgen kann.

[0056] Anschließend werden in einem Teilschritt 21.2 die beiden Teilschlüssel über den sicheren Kommunikationskanal ausgetauscht, indem der erste Teilschlüssel an die zweite Verarbeitungseinheit 2.1 und der zweite Teilschlüssel an die erste Verarbeitungseinheit 5.1 gesandt wird.

[0057] In einem Teilschritt 21.3 wird der geheime Sitzungsschlüssel sowohl in der Frankiermaschine 1 als auch in der Datenzentrale 2 nach einem vorgegebenen Schlüsselerzeugungsschema aus den beiden Teilschlüsseln generiert und in dem dritten Speicher 5.3 des Sicherheitsmoduls 5 bzw. dem vierten Speicher 2.3 der Datenzentrale 2 gespeichert.

[0058] Das Schlüsselerzeugungsschema ist dabei ebenfalls in dem dritten Speicher 5.3 des Sicherheitsmoduls 5 bzw. dem vierten Speicher 2.3 der Datenzentrale 2 gespeichert. Im vorliegenden Fall besteht das Schlüsselerzeugungsschema lediglich darin, dass der zweite Teilschlüssel an den ersten Teilschlüssel angehängt wird. Es versteht sich jedoch, dass der geheime Sitzungsschlüssel bei anderen Varianten der Erfindung auch nach beliebigen anderen Schemata aus dem ersten und zweiten Teilschlüssel generiert werden kann.

[0059] Wie Figur 2 zu entnehmen ist, folgt auf den Schlüsselgenerierungsschritt 21 ein Datenübermittlungsschritt 22, in dem die Gebührentabelle von der Datenzentrale 2 über den sicheren Kommunikationskanal an die Frankiermaschine 1 übersandt wird.

[0060] Wie Figur 2B zu entnehmen ist, wird dabei zunächst in einem Teilschritt 22.1 in der Datenzentrale 2 durch die zweite Verarbeitungseinheit 2.1 eine erste Nachricht generiert, welche eine erste Information in Form der zu übersendenden Gebührentabelle enthält.

[0061] Die erste Nachricht enthält im vorliegenden Beispiel weiterhin eine erste digitale Signatur, die von der zweiten Verarbeitungseinheit 2.1 unter Zugriff auf den zweiten Speicher 2.2 in hinlänglich bekannter Weise über der ersten Information, also der Gebührentabelle, erzeugt wurde. Dabei wird ein digitaler Signaturalgorithmus ohne Nachrichtenwiederherstellung verwendet. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung eine solche digitale Signatur über der ersten Information auch fehlen kann.

[0062] In einem Teilschritt 22.2 wird in der Datenzentrale 2 aus der ersten Nachricht eine zweite Nachricht generiert, indem die zweite Verarbeitungseinheit 2.1 an die erste Nachricht um einen Anhang erweitert. Bei dem Anhang handelt es sich im vorliegenden Fall um den im vierten Speicher 2.3 gespeicherten geheimen Sitzungsschlüssel.

[0063] In einem Teilschritt 22.3 wird in der Datenzentrale 2 aus der zweiten Nachricht eine dritte Nachricht generiert, indem die zweite Verarbeitungseinheit 2.1 die zweite Nachricht unter Verwendung des geheimen Sitzungsschlüssels verschlüsselt. Die zweite Verarbeitungseinheit 2.1 greift hierbei auf einen entsprechenden Verschlüsselungsalgorithmus zu, der in einem fünften Speicher 2.4 der Datenzentrale 2 abgelegt ist.

[0064] In einem Teilschritt 22.4 wird die dritte Nachricht anschließend von der Datenzentrale 2 über den sicheren Kommunikationskanal an die Frankiermaschine 1 übermittelt.

[0065] Bei dem Anhang handelt es sich im vorliegenden Fall wie erwähnt um den geheimen Sitzungsschlüssel. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung auch beliebige andere Anhänge verwendet werden können. Weiterhin kann es sich bei dem Anhang auch um einen vorgegebenen Teil des geheimen Sitzungsschlüssel handeln. Um welchen Teil des geheimen Sitzungsschlüssels es sich dabei handelt, kann beispielsweise vorab im Rahmen einer Kommunikation, insbesondere über den sicheren Kommunikationskanal, zwischen der Frankiermaschine und der Datenzentrale vereinbart bzw. vorgegeben worden sein. Ebenso kann diese Vorgabe gleichzeitig mit oder nach der Übermittlung der dritten Nachricht erfolgen.

[0066] Wie Figur 2 weiterhin zu entnehmen ist, erfolgt in einem Entschlüsselungsschritt 23 im Sicherheitsmodul 5 der Frankiermaschine 1 eine Entschlüsselung der dritten Nachricht, sodass im Sicherheitsmodul 5 dann die zweite Nachricht vorliegt. Hierzu greift die erste Verarbeitungseinheit 5.1 des Sicherheitsmoduls auf dem dritten Speicher 5.3, in dem der geheime Sitzungsschlüssel gespeichert ist, und einen sechsten Speicher 5.4 zu, der einen entsprechenden Entschlüsselungsalgorithmus enthält.

[0067] Anschließend erfolgt gemäß Figur 2 in einem Integritätsprüfungsschritt 24 im Sicherheitsmodul 5 der Frankiermaschine 1 eine Integritätsprüfung, bei der die zweite Nachricht auf ihre Integrität überprüft wird. Hierbei greift die erste Verarbeitungseinheit 5.1 auf einen Integritätsprüfungsalgorithmus zu, der in einem siebten Speicher 5.5 des Sicherheitsmoduls 5 abgelegt ist. Je nach dem Ergebnis der Integritätsprüfung wird in einem Bestätigungsschritt 25 eine entsprechende Bestätigungsnachricht von der Frankiermaschine 1 an die Datenzentrale 2 übersandt.

[0068] Wie Figur 2C zu entnehmen ist, wird in dem Integritätsprüfungsschritt 24 zunächst in einem Teilschritt 24.1 durch die erste Verarbeitungseinheit 5.1 sowohl der Anhang aus der zweiten Nachricht isoliert als auch die erste Nachricht. Hierzu löst die erste Verarbeitungseinheit 5.1 im vorliegenden Beispiel jeweils eine

Bitsequenz mit vorgegebener Position und Länge aus der zweiten Nachricht.

[0069] In einem Teilschritt 24.2 wird dieser aus der zweiten Nachricht herausgelöste Anhang durch die erste Verarbeitungseinheit 5.1 mit einem vorgegebenen Anhang verglichen, hier also mit dem in dem dritten Speicher 5.3 gespeicherten geheimen Sitzungsschlüssel.

[0070] Ist das Ergebnis der Überprüfung in dem Teilschritt 24.2 positiv, d. h. entspricht der herausgelöste Anhang dem vorgegebenen Anhang, wird in einem Teilschritt 24.3 aus der ersten Nachricht die erste Information, also die Gebührentabelle, und die erste digitale Signatur herausgelöst. Hierzu löst die erste Verarbeitungseinheit 5.1 im vorliegenden Beispiel wiederum entsprechende Bitsequenzen mit vorgegebener Position und Länge aus der ersten Nachricht.

[0071] In einem Teilschritt 24.4 wird dann die erste digitale Signatur verifiziert. Die erste Verarbeitungseinheit 5.1 greift hierbei neben der ersten Information und der ersten digitalen Signatur auf einen entsprechenden Verifizierungsalgorithmus ohne Nachrichtenwiederherstellung sowie den öffentlichen Schlüssel der Datenzentrale 2 zu, die beide im ersten Speicher 5.2 gespeichert sind. Es versteht sich jedoch, dass bei Varianten der Erfindung, bei denen die erste digitale Signatur fehlt, auch die Teilschritt 24.3 und 24.4 fehlen können.

[0072] Ist auch das Ergebnis der Verifizierung im Teilschritt 24.4 positiv, d. h. entspricht die erste digitale Signatur der ersten Information, ist die Integritätsprüfung erfolgreich abgeschlossen. Die Gebührentabelle wird dann in einem Teilschritt 24.5 auf Veranlassung des Sicherheitsmoduls 5 durch das Verarbeitungsmodul 4 in dem Gebührentabellenspeicher 6 abgelegt, wobei gegebenenfalls eine dort vorhandene alte Gebührentabelle überschrieben wird.

[0073] Wurde die Integritätsprüfung erfolgreich abgeschlossen, d. h. die Integrität der zweiten Nachricht festgestellt, wird in dem Bestätigungsschritt in einem Teilsschritt 25.1 eine positive Bestätigungsnachricht von dem Sicherheitsmodul 5 der Frankiermaschine 1 an die Datenzentrale 2 übersandt.

[0074] Bei Erhalt der positiven Bestätigungsnachricht beendet die Datenzentrale 2 in einem Kommunikationsabbruchschritt 26 die Kommunikation mit der Frankiermaschine 1, wie dies Figur 2 zu entnehmen ist.

[0075] Gemäß Figur 2C protokolliert die Datenzentrale 2 hierbei zunächst den erfolgreichen Abschluss der Übermittlung der Gebührentabelle in einem Teilschritt 26.1 in einem achten Speicher 2.5, der mit der zweiten Verarbeitungseinheit 2.1 verbunden ist.

[0076] In einem Teilschritt 26.2 wird dann ausgehend von der Datenzentrale 2 der sichere Kommunikationskanal geschlossen und die Verbindung mit der Frankiermaschine 1 getrennt.

[0077] Anschließend wird in einem Teilschritt 26.3 in der Datenzentrale 2 der geheime Sitzungsschlüssel vernichtet, indem der entsprechende Speicherbereich des vierten Speichers 2.3 durch die zweite Verarbeitungseinheit 2.1 überschrieben wird. Auf Seiten der Frankiermaschine 1 wird ebenso vorgegangen, nachdem der Abbruch der Kommunikation mit der Datenzentrale 2 festgestellt wurde. Es wird also im Teilschritt 26.3 auch im Sicherheitsmodul 5 der geheime Sitzungsschlüssel vernichtet, indem der entsprechende Speicherbereich des dritten Speichers 5.3 durch die erste Verarbeitungseinheit 5.1 überschrieben wird. Hiermit ist der Verfahrensablauf dann beendet.

[0078] Ist das Ergebnis der Überprüfung in dem Teilschritt 24.2 aus Figur 2C jedoch negativ, d. h. entspricht der herausgelöste Anhang nicht dem vorgegebenen Anhang, wird im Sicherheitsmodul 5 in einem Teilschritt 24.6 zunächst überprüft, ob bereits eine vorgegebene Anzahl erfolgloser Datenübermittlungsschritte 22 durchgeführt wurde. Ebenso wird verfahren, wenn das Ergebnis der Verifikation im Teilschritt 24.4 des Integritätsprüfungsschrittes 24 negativ ist.

[0079] Ist die vorgegebene Anzahl erfolgloser Datenübermittlungsschritte 22 noch nicht erreicht, wird in einem Teilschritt 25.2 des Bestätigungsschrittes 25 eine erste negative Bestätigungsnachricht von dem Sicherheitsmodul 5 an die Datenzentrale 2 übersandt. Bei Erhalt der ersten negativen Bestätigungsnachricht wird der Teilschritt 22.4 des Datenübermittlungsschrittes 24 wiederholt, d. h. die Datenzentrale 2 sendet erneut die dritte Nachricht. Dies ist in den Figuren 2, 2B und 2C durch den Anknüpfungspunkt 27 angedeutet.

[0080] Ergibt die Überprüfung in dem Teilschritt 24.6 des Integritätsprüfungsschrittes 24 jedoch, dass die vorgegebene Anzahl erfolgloser Datenübermittlungsschritte 22 erreicht ist, wird das Sicherheitsmodul 5 in einem Teilschritt 24.7 in einen Fehlermodus geschaltet, in dem die Frankiermaschine 1 keine Frankierungen vornehmen kann. Hierüber wird der Benutzer der Frankiermaschine durch ein entsprechendes akustisches Signal und/oder ein entsprechendes optisches Signal in Kenntnis gesetzt.

[0081] In diesem Fall wurde die Integritätsprüfung somit erfolglos abgeschlossen, d. h. die fehlende Integrität der zweiten Nachricht festgestellt. In einem Teilschritt 25.3 des Bestätigungsschrittes 25 wird demgemäß eine zweite negative Bestätigungsnachricht von dem Sicherheitsmodul 5 an die Datenzentrale 2 übersandt. Bei Eintreffen der zweiten negativen Bestätigungsnachricht wird dann der Kommunikationsabbruchschritt 26 wie oben beschrieben durchgeführt. Hierbei wird allerdings in dem Teilschritt 26.1 der erfolglose Abschluss der Übermittlung der Gebührentabelle in dem achten Speicher 2.5 protokolliert.

[0082] Bei der Anordnung aus Figur 1 erfolgt zum einen in regelmäßigen Zeitintervallen und zum anderen mit jedem Einschalten der Frankiermaschine 1 eine erneute Überprüfung der ersten digitalen Signatur, die zusammen mit der Gebührentabelle in dem Gebührentabellenspeicher 6 gespeichert wurde. Hierzu wird der oben beschriebene Teilschritt 24.4 des Integritätsprü-

fungsschrittes 24 wiederholt, in dem die erste digitale Signatur verifiziert wird. Ist das Ergebnis der Verifizierung im Teilschritt 24.4 positiv, d. h. entspricht die erste digitale Signatur der ersten Information, kann die Frankiermaschine 1 weiter betrieben werden. Ist das Ergebnis der Verifizierung im Teilschritt 24.4 jedoch negativ, wird die Frankiermaschine 1 in einen Fehlermodus geschaltet, wie er oben im Zusammenhang mit dem Teilschritt 24.7 des Integritätsprüfungsschrittes 24 beschrieben wurde.

[0083] Im Rahmen dieser regelmäßigen Überprüfung wird die Gebührentabelle noch dahingehend überprüft, ob ein mit der Gebührentabelle verbundenes Gültigkeitsdatum überschritten wurde oder nicht. Ist dies der Fall, wird die Frankiermaschine 1 ebenfalls in den beschriebenen Fehlermodus geschaltet.

[0084] Es sei an dieser Stelle angemerkt, dass es sich bei den vorstehend beschriebenen Speichern nicht notwendigerweise um getrennte Speichermodule handeln muss. Vielmehr können in dem Sicherheitsmodul 5 und in der Datenzentrale 2 gegebenenfalls jeweils eines oder mehrere Speichermodule vorgesehen sein, wobei einzelne Speichermodule unterschiedlichen Speicherbereiche aufweisen, welche die unterschiedlichen Speicher ausbilden. Zur Vervollständigung sei hier noch angemerkt, dass das Sicherheitsmodul 5 einen mit der ersten Verarbeitungseinheit 5.1 verbundenen ersten Arbeitsspeicher 5.6 aufweist, in dem sämtliche für den aktuellen Verfahrensschritt erforderlichen Daten abgelegt werden. Gleiches gilt für die Datenzentrale 2, die einen mit der zweiten Verarbeitungseinheit 2.1 verbundenen zweiten Arbeitsspeicher 2.6 aufweist.

[0085] Die vorliegende Erfindung wurde vorstehend anhand eines konkreten Ausführungsbeispiels beschrieben. Es versteht sich jedoch, dass bei anderen Varianten auch ein anderer Verfahrensablauf gewählt werden kann. Insbesondere können die Teilschritte innerhalb eines Verfahrensschrittes gegebenenfalls in abweichender Reihenfolge durchgeführt werden.

[0086] Die vorliegende Erfindung wurde vorstehend weiterhin ausschließlich anhand eines Beispiels aus dem Bereich der Frankiermaschinen beschrieben. Es versteht sich jedoch, dass die vorliegende Erfindung auch in anderen Bereichen Anwendung finden kann, in denen es auf die sichere Übertragung von Dienstdaten zwischen einer ersten Datenverarbeitungseinheit und einer zweiten Datenverarbeitungseinheit ankommt.

Patentansprüche

1. Verfahren zum sicheren Datenaustausch zwischen einer ersten Datenverarbeitungseinheit (1) und einer zweiten Datenverarbeitungseinheit (2), bei dem in einem Kommunikationsaufbauschritt (20) ein sicherer Kommunikationskanal zwischen der ersten Datenverarbeitungseinheit (1) und der zweiten Datenverarbeitungseinheit (2) hergestellt wird und in einem Datenübermittlungsschritt (22) über den sicheren Kommunikationskanal eine erste Nachricht von der zweiten Datenverarbeitungseinheit (2) an die erste Datenverarbeitungseinheit (1) übersandt wird, **dadurch gekennzeichnet, dass** in dem Datenübermittlungsschritt (22)

   - in der zweiten Datenverarbeitungseinheit (2) eine zweite Nachricht generiert wird, indem ein vorgegebener Anhang an die erste Nachricht angehängt wird,
   - eine dritte Nachricht generiert wird, indem die zweite Nachricht unter Verwendung eines geheimen Schlüssels verschlüsselt wird, der nur in der ersten Datenverarbeitungseinheit (1) und der zweiten Datenverarbeitungseinheit (2) vorhanden ist, und
   - die dritte Nachricht an die erste Datenverarbeitungseinheit (1) übersandt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** in einem Entschlüsselungsschritt (23) die dritte Nachricht in der ersten Datenverarbeitungseinheit (1) unter Verwendung des geheimen Schlüssels entschlüsselt wird und die zweite Nachricht in einem Integritätsprüfungsschritt (24) auf ihre Integrität überprüft wird.

3. Verfahren nach Anspruch 2, **dadurch gekennzeichnet, dass** zur Integritätsprüfung in dem Integritätsprüfungsschritt (24) der Anhang aus der zweiten Nachricht isoliert wird und überprüft wird, ob der Anhang einem vorgegebenen Anhang entspricht.

4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Anhang zumindest ein, insbesondere vorgebbarer, Teil des geheimen Schlüssels ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der geheime Schlüssel ein geheimer Sitzungsschlüssel ist, der in dem Kommunikationsaufbauschritt (20) oder nach dem Kommunikationsaufbauschritt (20) generiert wird.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, dass** der geheime Schlüssel generiert wird, indem

   - ein erster Teilschlüssel in der ersten Datenverarbeitungseinheit (1) generiert und an die zweite Datenverarbeitungseinheit (2) gesandt wird,
   - ein zweiter Teilschlüssel in der zweiten Daten-

verarbeitungseinheit (2) generiert und an die erste Datenverarbeitungseinheit (1) gesandt wird und

- der geheime Schlüssel in der ersten Datenverarbeitungseinheit (1) und in der zweiten Datenverarbeitungseinheit (2) aus dem ersten Teilschlüssel und dem zweiten Teilschlüssel nach einem vorgebbaren Schlüsselerzeugungsschema generiert wird, insbesondere aus dem ersten Teilschlüssel und dem zweiten Teilschlüssel zusammengesetzt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der geheime Schlüssel ein temporärer Schlüssel ist, der nur vorübergehend verwendet wird.

8. Verfahren nach einem der Ansprüche 2 bis 7, **dadurch gekennzeichnet, dass** in einem Bestätigungsschritt (25)

- im Fall der Feststellung der Integrität der zweiten Nachricht im Integritätsprüfungsschritt (24) eine positive Bestätigungsnachricht, die insbesondere die erste Nachricht enthält, von der ersten Datenverarbeitungseinheit (1) an die zweite Datenverarbeitungseinheit (2) gesandt wird und/oder

- im Fall der Feststellung fehlender Integrität der zweiten Nachricht im Integritätsprüfungsschritt (24) eine negative Bestätigungsnachricht von der ersten Datenverarbeitungseinheit (1) an die zweite Datenverarbeitungseinheit (2) gesandt wird.

9. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, dass** der sichere Kommunikationskanal zumindest nach Erhalt der positiven Bestätigungsnachricht durch die zweite Datenverarbeitungseinheit (2) in einem Kommunikationsabbruchschritt (26) geschlossen wird und der geheime Schlüssel sowohl in der ersten Datenverarbeitungseinheit (1) als auch in der zweiten Datenverarbeitungseinheit (2) vernichtet wird.

10. Verfahren nach einem der Ansprüche 2 bis 9, **dadurch gekennzeichnet, dass** die erste Datenverarbeitungseinheit (1) ein erstes Verarbeitungsmodul (4) und ein damit verbundenes Sicherheitsmodul (5) umfasst, wobei der Entschlüsselungsschritt (23) durch das Sicherheitsmodul (5) durchgeführt wird.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet, dass** der Integritätsprüfungsschritt (24) und/oder der Bestätigungsschritt (25) durch das Sicherheitsmodul (5) durchgeführt wird.

12. Verfahren nach Anspruch 10 oder 11, **dadurch gekennzeichnet, dass**

- das Verarbeitungsmodul (4) bei Feststellung der Integrität der zweiten Nachricht zumindest einen Teil der ersten Nachricht zur weiteren Verwendung in einem mit dem Verarbeitungsmodul (4) verbundenen Speicher (6) ablegt und

- das Verarbeitungsmodul (4) und/oder das Sicherheitsmodul (5) bei Feststellung fehlender Integrität der zweiten Nachricht in einen Fehlermodus schaltet.

13. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die erste Nachricht eine Information und eine digitale Signatur der zweiten Datenverarbeitungseinheit (2) über der ersten Information umfasst.

14. Verfahren nach Anspruch 12 und 13, **dadurch gekennzeichnet, dass** der Integritätsprüfungsschritt (24) zu vorgebbaren Zeitpunkten zumindest teilweise wiederholt wird.

15. Anordnung zum sicheren Datenaustausch mit einer ersten Datenverarbeitungseinheit (1) und einer zweiten Datenverarbeitungseinheit (2), die zum Aufbau eines sicheren Kommunikationskanals und zur Übermittlung einer ersten Nachricht von der zweiten Datenverarbeitungseinheit (2) an die erste Datenverarbeitungseinheit (1) über den sicheren Kommunikationskanal ausgebildet sind, **dadurch gekennzeichnet, dass** ein geheimer Schlüssel vorgesehen ist, der ausschließlich in der ersten Datenverarbeitungseinheit (1) und in der zweiten Datenverarbeitungseinheit (2) gespeichert ist, und dass die zweite Datenverarbeitungseinheit (2)

- zum Generieren einer zweiten Nachricht durch Anhängen eines vorgegebenen Anhangs an die erste Nachricht ausgebildet ist,

- zum Generieren einer dritten Nachricht durch Verschlüsselung der zweiten Nachricht unter Verwendung des geheimen Schlüssels ausgebildet ist, und

- zum Übersenden der dritten Nachricht an die erste Datenverarbeitungseinheit (1) über den sicheren Kommunikationskanal ausgebildet ist.

16. Anordnung nach Anspruch 15, **dadurch gekennzeichnet, dass** die erste Datenverarbeitungseinheit (1) zum Entschlüsseln der dritten Nachricht un-

ter Verwendung des geheimen Schlüssels und zur Durchführung einer Integritätsprüfung an der zweiten Nachricht ausgebildet ist.

17. Anordnung nach Anspruch 16, **dadurch gekennzeichnet, dass** zur Integritätsprüfung die erste Datenverarbeitungseinheit (1) zum Isolieren des Anhangs aus der zweiten Nachricht und zum Vergleich des Anhangs mit einem vorgegebenen Anhang ausgebildet ist.

18. Anordnung nach einem der Ansprüche 15 bis 17, **dadurch gekennzeichnet, dass** der Anhang zumindest ein, insbesondere vorgebbarer, Teil des geheimen Schlüssels ist.

19. Anordnung nach einem der Ansprüche 15 bis 18, **dadurch gekennzeichnet, dass** der geheime Schlüssel ein geheimer Sitzungsschlüssel ist und dass die erste Datenverarbeitungseinheit (1) und/oder die zweite Datenverarbeitungseinheit (2) zum Generieren des geheimen Schlüssels ausgebildet ist.

20. Anordnung nach Anspruch 19, **dadurch gekennzeichnet, dass** zum Generieren des geheimen Schlüssels

- die erste Datenverarbeitungseinheit (1) zum Generieren eines ersten Teilschlüssels und zum Übersenden des ersten Teilschlüssels an die zweite Datenverarbeitungseinheit (2) ausgebildet ist,

- die zweite Datenverarbeitungseinheit (2) zum Generieren eines zweiten Teilschlüssels und zum Übersenden des zweiten Teilschlüssels an die erste Datenverarbeitungseinheit (1) ausgebildet ist, und

- die erste Datenverarbeitungseinheit (1) und die zweite Datenverarbeitungseinheit (2) zum Generieren des geheimen Schlüssels aus dem ersten Teilschlüssel und dem zweiten Teilschlüssel nach einem vorgebbaren Schlüsselerzeugungsschema, insbesondere zum Zusammensetzen des ersten Schlüssels aus dem ersten Teilschlüssel und dem zweiten Teilschlüssel, ausgebildet sind.

21. Anordnung nach einem der Ansprüche 15 bis 20, **dadurch gekennzeichnet, dass** der geheime Schlüssel ein temporärer Schlüssel mit begrenzter Gültigkeitsdauer ist.

22. Anordnung nach einem der Ansprüche 16 bis 21, **dadurch gekennzeichnet, dass** die erste Datenverarbeitungseinheit (1)

- zum Übersenden einer positiven Bestätigungsnachricht, die insbesondere die erste Nachricht enthält, an die zweite Datenverarbeitungseinheit (2) im Fall der Feststellung der Integrität der zweiten Nachricht ausgebildet ist und/oder

- zum Übersenden einer negativen Bestätigungsnachricht an die zweite Datenverarbeitungseinheit (2) im Fall der Feststellung fehlender Integrität der zweiten Nachricht ausgebildet ist.

23. Anordnung nach Anspruch 22, **dadurch gekennzeichnet, dass** die zweite Datenverarbeitungseinheit (2) zum Schließen des sicheren Kommunikationskanals zumindest nach Erhalt der positiven Bestätigungsnachricht ausgebildet ist und dass die erste Datenverarbeitungseinheit (1) und die zweite Datenverarbeitungseinheit (2) zum Vernichten des geheimen Schlüssels nach Schließen des sicheren Kommunikationskanals ausgebildet sind.

24. Anordnung nach einem der Ansprüche 16 bis 23, **dadurch gekennzeichnet, dass** die erste Datenverarbeitungseinheit (1) ein erstes Verarbeitungsmodul (4) und ein damit verbundenes Sicherheitsmodul (5) umfasst, das zum Entschlüsseln der dritten Nachricht ausgebildet ist.

25. Anordnung nach Anspruch 24, **dadurch gekennzeichnet, dass** das Sicherheitsmodul (5) zur Durchführung der Integritätsprüfung und/oder zum Übersenden einer Bestätigungsnachricht in Abhängigkeit vom Ergebnis der Integritätsprüfung ausgebildet ist.

26. Anordnung nach Anspruch 24 oder 25, **dadurch gekennzeichnet, dass**

- das Verarbeitungsmodul (4) zum Speichern zumindest eines Teils der ersten Nachricht bei Feststellung der Integrität der zweiten Nachricht zur weiteren Verwendung in einem mit dem Verarbeitungsmodul (4) verbundenen Speicher (6) ausgebildet ist und

- das Verarbeitungsmodul (4) und/oder das Sicherheitsmodul (5) zum Umschalten in einen Fehlermodus bei Feststellung fehlender Integrität der zweiten Nachricht ausgebildet ist.

27. Anordnung nach einem der Ansprüche 15 bis 26, **dadurch gekennzeichnet, dass** die zweite Datenverarbeitungseinheit (2) zum Erstellen einer ersten digitalen Signatur über einer ersten Information und zum Erstellen der ersten Nachricht aus der ersten Information und der ersten digitalen Signatur ausgebildet ist.

28. Anordnung nach Anspruch 26 und 27, **dadurch gekennzeichnet, dass** die erste Datenverarbeitungseinheit (1) zur zumindest teilweisen Wiederholung der Integritätsprüfung zu vorgebbaren Zeitpunkten ausgebildet ist.

29. Anordnung nach einem der Ansprüche 15 bis 28, **dadurch gekennzeichnet, dass** die erste Datenverarbeitungseinheit eine Frankiermaschine (1) ist und/oder die zweite Datenverarbeitungseinheit eine entfernte Datenzentrale (2) ist.

30. Datenverarbeitungseinheit, **dadurch gekennzeichnet, dass** sie wie die erste Datenverarbeitungseinheit (1) oder die zweite Datenverarbeitungseinheit (2) nach einem der Ansprüche 16 bis 29 ausgebildet ist.

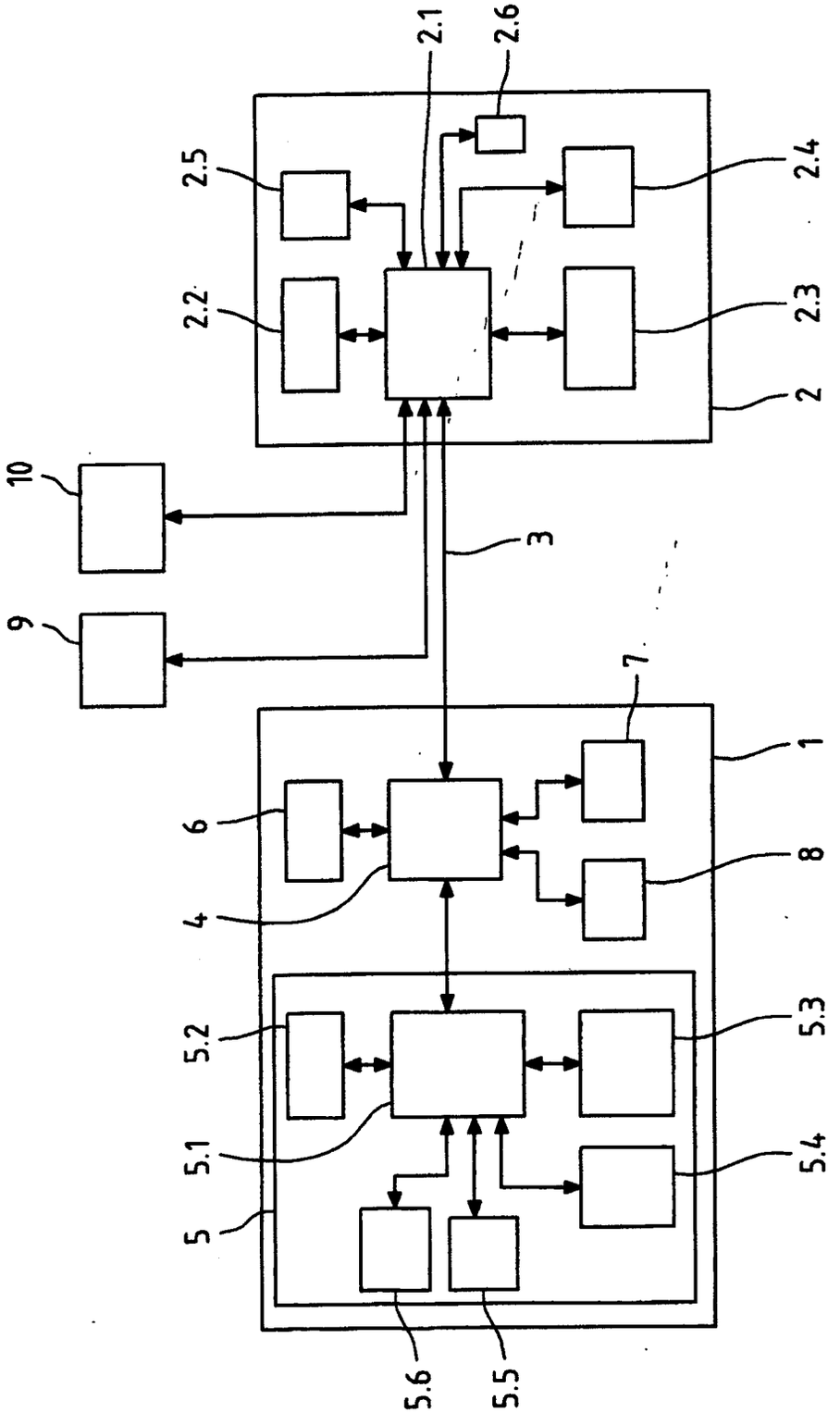

Fig.1

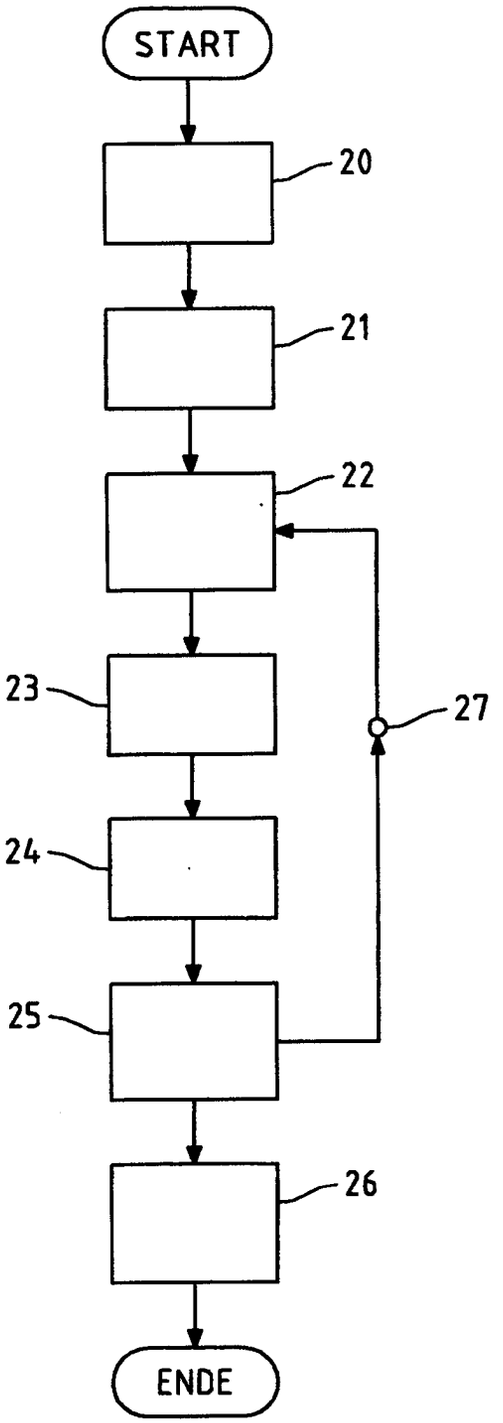

Fig.2

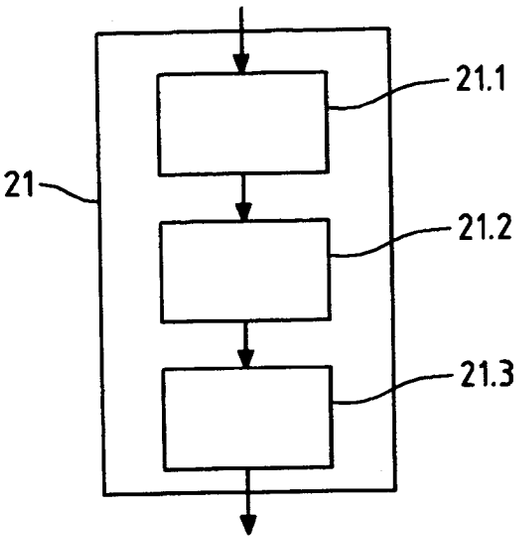

Fig.2A

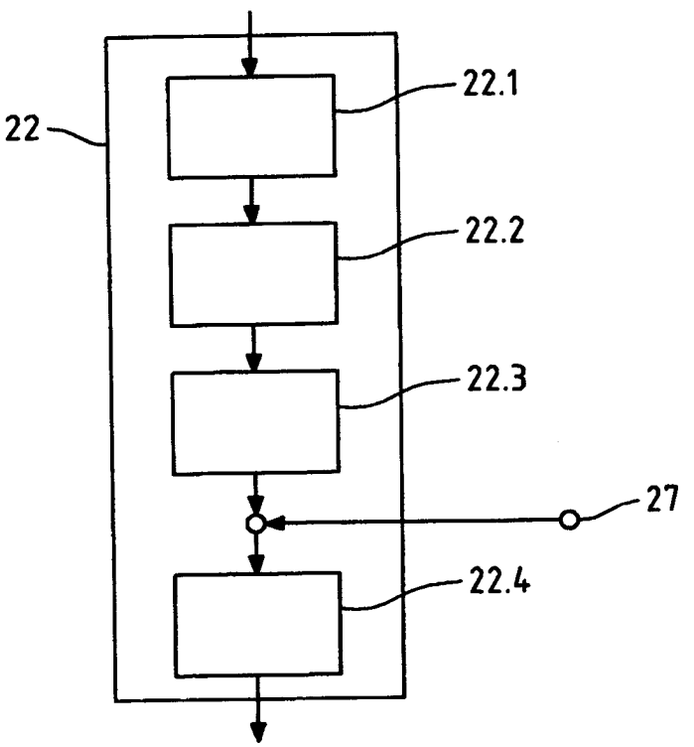

Fig.2B

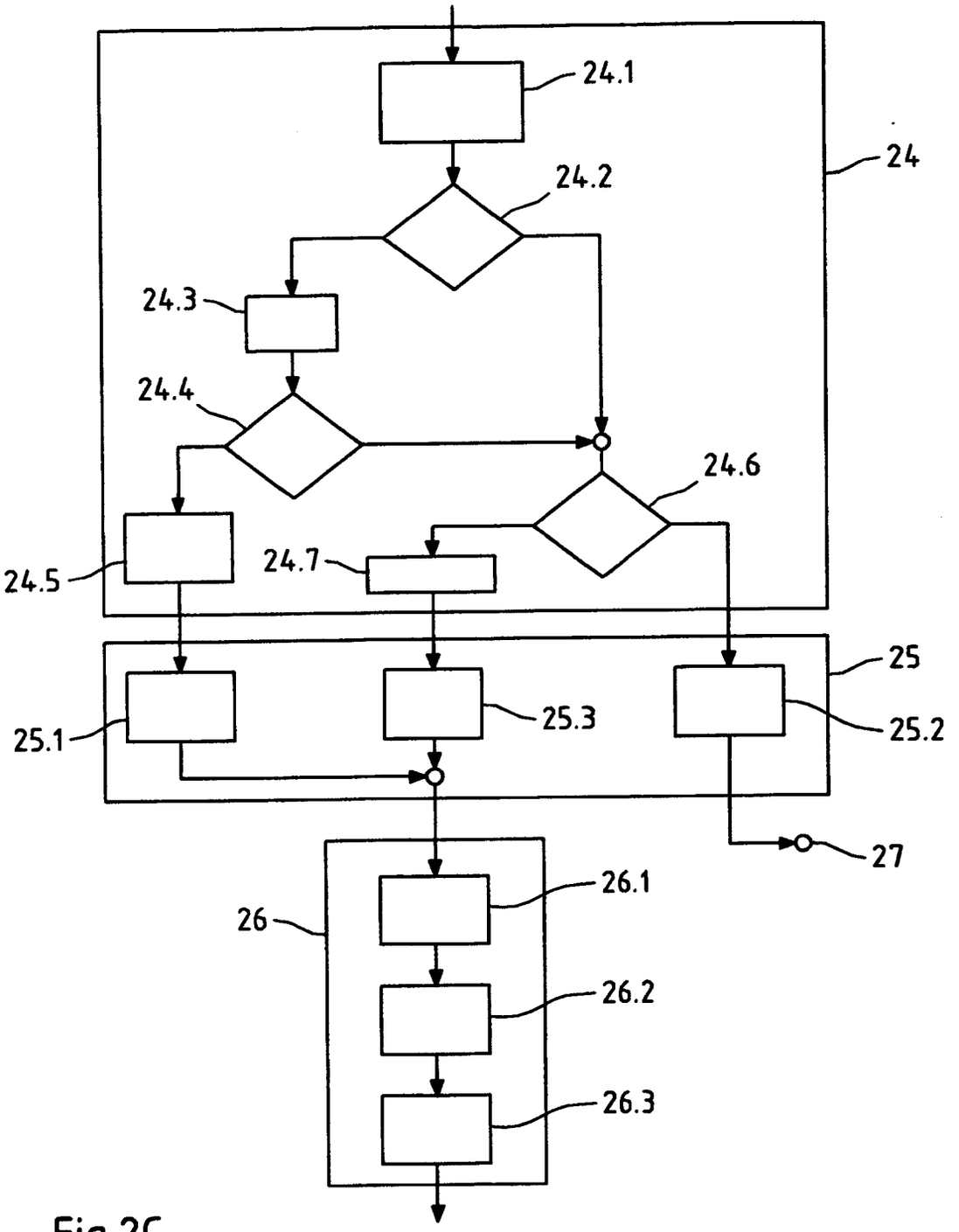

Fig.2C