(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 601 32 254 T2** 2008.12.18

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 378 847 B1**
(21) Deutsches Aktenzeichen: **601 32 254.1**
(96) Europäisches Aktenzeichen: **03 077 585.2**
(96) Europäischer Anmeldetag: **08.11.2001**
(97) Erstveröffentlichung durch das EPA: **07.01.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **02.01.2008**
(47) Veröffentlichungstag im Patentblatt: **18.12.2008**

(51) Int Cl.[8]: ***G06Q 10/00*** (2006.01)

(30) Unionspriorität:

0027280	**08.11.2000**	**GB**
923704	**07.08.2001**	**US**

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

(73) Patentinhaber:
Orchestria Ltd., London, GB

(72) Erfinder:
Malcolm, Peter Bryan, Okehampton, Devon EX20 4QJ, GB

(74) Vertreter:
Kuhnen & Wacker Patent- und Rechtsanwaltsbüro, 85354 Freising

(54) Bezeichnung: **Ein Informationsverwaltungssystem**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

HINTERGRUND DER ERFINDUNG

[0001] Die vorliegende Erfindung betrifft die Bereitstellung von erweiterter Managementfunktionalität für Internetanwendungen, insbesondere in den Bereichen Informationssicherheit, Transaktionsprüfung und -berichte, zentralisierte Richtlinien und Anwendungsverknüpfbarkeit.

[0002] Elektronischer Handel („eCommerce"), insbesondere zwischen Unternehmen („B2B"), aber auch zwischen Unternehmen und Kunden („B2C"), ist ein schnell wachsender Markt, auf dem Käufer und Verkäufer über das Internet, einem weltweiten Netzwerk von verknüpften Computersystemen, anstatt über traditionelle Mittel wie Post, Telefon und persönliches Zusammenkommen kommunizieren. Verkäufer werben für ihre Produkte und Dienste mit digitalen Broschüren und Katalogen, die über eine Internetverbindung, durch Seiten auf dem World Wide Web oder über elektronische Märkte, die in Waren und Diensten eines bestimmten Marktsektors handeln, betrachtet oder heruntergeladen werden können. Käufer können Lieferanten finden, Waren auswählen, Angebote einholen, Bestellungen aufgeben und verfolgen und sogar Zahlungen vollkommen elektronisch und jederzeit vornehmen. eCommerce verspricht erhöhte Flexibilität, Auswahl und Effizienz zu drastisch reduzierten Beschaffungskosten.

[0003] Es gibt zwei universell akzeptierte Mittel, über die Benutzer mit dem Internet Verbindung aufnehmen können. Das erste ist der „Webbrowser", der es Benutzern gestattet, Seiten auf dem World Wide Web durch Zugreifen auf einzelne Websites zu betrachten, deren Adressen gewöhnlich weit verbreitet mit traditionellen Mitteln veröffentlicht werden, oder auf die auf einer andere Website verwiesen wird. Der am weitesten verbreitete Webbrowser ist der „Internet Explorer" von Microsoft.

[0004] Das zweite Mittel zur Verbindungsaufnahme ist die Verwendung eines Electronic-Mail-Programms, mit dem der Benutzer eine Nachricht verfasst, Email genannt, die dann elektronisch über das Internet zur Adresse des beabsichtigten Empfängers geleitet wird. Gut bekannte Electronic-Mail-Programme sind z. B. „Lotus Notes" von IBM und „Gutlook" von Microsoft.

[0005] In einem typischen eCommerce-Szenario könnte ein Käufer ein bestimmtes Produkt zusammen mit Preis- und Lieferinformationen auf der Website des Verkäufers identifizieren. Er könnte dann einen Auftrag erteilen, entweder durch Ausfüllen eines elektronischen Auftragsformulars auf der Website oder durch Senden einer Email direkt zum Verkäufer. Der Auftrag würde dann typischerweise eine Zahlungsverpflichtung beinhalten, möglicherweise in Form von Kreditkartendetails oder mit einem anderen elektronischen Zahlungsmittel. Der Verkäufer würde dann typischerweise eine Email zum Bestätigen der Annahme des Auftrags zurücksenden.

[0006] Webbrowser arbeiten gemäß anerkannten Normen, insbesondere dem Hypertext Transfer Protocol („HTTP"), das im Internet-Standarddokument RFC2616 umfassend beschrieben ist. Electronic-Mail-Programme arbeiten gemäß anerkannten Normen, insbesondere dem Simple Mail Transfer Protocol das im Internet-Standarddokument RFC0821 umfassend beschrieben ist, und dem Multipurpose Internet Mail Extensions („MIME"), das im Internet-Standarddokument RFC2045-2049 umfassend beschrieben ist.

[0007] eCommerce bietet zwar enorme Vorteile, aber seine Praxis wirft auch viele neue Fragen auf, die angegangen werden müssen, um seine dauerhafte Nutzung zu gewährleisten, besonders dann, wenn traditionelle Methoden irgendwann ersetzt werden sollen. Eine der zentralen Fragen ist Sicherheit.

[0008] Das Internet ist ein offenes Kommunikationsnetzwerk, das definitionsgemäß unsicher ist, da es von jedermann benutzt werden kann. Mittel zum Sichern empfindlicher Informationen, die über das Internet ausgetauscht werden sollen (z. B. in einer eCommerce-Transaktion), kamen mit der Ankunft sicherer Übertragungsprotokolle und Messaging. Sichere Punkt-zu-Punkt-Übertragungsprotokolle, wie sie beispielsweise zwischen einem Webserver und einem Webbrowser benutzt werden, beinhalten die ‚Secure Socket Lager' („SSL"), die von Netscape Communications definiert wird, und ihren Nachfolger ‚Transport Lager Security' („TLS"), die im Internet-Standarddokument RFC2246 definiert ist. Sichere Email-Nachrichtenstandards sind z. B., Secure Multipurpose Internet Mail Extensions' („S/MIME"), im Internet-Standarddokument RFC2633 umfassend beschrieben, und „Pretty Good Privacy", ein von Philip Zimmerman entwickeltes sicheres Public-Domain-Messaging-System.

[0009] Um den Zugang zu Informationen auf mit dem Internet verbundenen Servern zu kontrollieren, wurde weithin ein System von Benutzernamen und Passwörtern benutzt. So kann beispielsweise der Zugang zu Rabattpreislisten auf einem bestimmten Webserver auf Handelsbenutzer beschränkt sein, denen zuvor ein Benutzername und ein Passwort zum Zugreifen gegeben wurde. Ebenso benutzen Online-Informationsdienste typischerweise häufig Benutzernamen und Passwörter zum Beschränken des Zugangs auf Personen, die für den Dienst bezahlt haben. Indem jedem Benutzer ein eindeutiger Benutzername und ein änderbares Passwort gegeben werden, kann der Dienst gewährleisten, dass nur zahlen-

de Abonnenten auf das System zugreifen können, und kann den Zugriff auf die von dem Dienst gespeicherten persönlichen Daten durch Andere verhindern.

[0010] In eCommerce-Anwendungen ist ein bedeutendes Problem die Frage von Identität und Vertrauen. Wenn ein Lieferant einen Auftrag über das Internet erhält, dann ist es vollkommen möglich, ja sogar wahrscheinlich, dass er keinerlei Vorkenntnisse über den Kunden hat. Der Lieferant muss feststellen, ob der Kunde a) der ist, für den er sich ausgibt, mit anderen Worten, dass er sich nicht als jemand anderes ausgibt, und dass er b) vertrauenswürdig ist und schließlich für die zu liefernden Waren oder Dienste bezahlen kann. Diese Fragen wurden im B2C-Markt vornehmlich durch die Verwendung von Kreditkarten gelöst. Der Kunde gibt seine Kreditkartennummer und Adresse mit dem Auftrag an, die der Lieferant dann mit dem Kreditkartenunternehmen verifiziert und eine Autorisierung für den Betrag erhält. Der gesamte Vorgang läuft typischerweise online ohne menschlichen Eingriff ab. Das Verfahren ist weitgehend dort wirksam, wo ein Lieferant Waren zur Adresse des Karteninhabers versendet, da ein potentieller Dieb nicht nur die Details des Karteninhabers stehlen, sondern auch die Lieferung der Waren abfangen müsste. Es ist weitaus weniger wirksam im Falle von Diensten, die keine physische Lieferung beinhalten.

[0011] Es ist also klar, dass die Benutzung von Kreditkarten in eCommerce zwar weit verbreitet, aber auf Transaktionen im kleinen Umfang beschränkt ist, potentiell mit Beträgen von beispielsweise bis $10.000. Für über diese Beträge hinaus gehende Transaktionen (deren Gesamtgeldwert den unterhalb dieses Betrags weit übersteigen), muss eine beidseitig vertrauenswürdige Drittpartei zum Feststellen von Identität und Vertrauen in Anspruch genommen werden.

[0012] Eine zentrale Rolle bei der Feststellung der Identität spielen digitale Zertifikate. Dem Kunden kann von einer vertrauenswürdigen Drittpartei ein digitales Zertifikat gegeben werden, das dann zum elektronischen ‚Signieren' von Kommunikationen verwendet wird. Nach dem Erhalt einer signierten Nachricht kann der Empfänger (in diesem Fall der Lieferant) positiv a) die Identität des Senders, b) die Tatsache, dass die Nachricht nicht verändert wurde, und c) die Tatsache, dass der Sender nachfolgend nicht bestreitet, dass er die Nachricht gesendet hat, feststellen. Anerkannte Normen für digitale Zertifikate sind im ITU-Dokument X.509, ihre Verwendung in Internet-Kommunikationen in den Internet-Standarddokumenten RFC2312, RFC2459, RFC2510, RFC2511, RFC2527, RFC2560, RFC2585 und RFC2632 beschrieben.

[0013] Es können gebührenpflichtige Drittparteidienste wie z. B. die von Valicert Inc. bereitgestellten zum Überprüfen benutzt werden, dass ein digitales Zertifikat nicht widerrufen wurde, z. B. wenn das Zertifikat auf irgendeine Weise kompromittiert wurde.

[0014] Wenn die Echtheit von Nachrichten festgestellt ist, kann der Lieferant eine andere Drittpartei mit der Feststellung der Vertrauenswürdigkeit beauftragen, oder dieselbe Drittpartei kann zum Feststellen von Echtheit und Vertauenswürdigkeit benutzt werden. So stellt z. B. „Identrus", ein Konsortium der weltweit größten Banken, ein System bereit, so dass ein Lieferant, der eine mit einem von Identrus ausgegebenen digitalen Zertifikat signierte Nachricht erhält, unabhängig prüfen kann, ob der Kunde ein gültiger Kontoinhaber mit gutem Ruf bei einer anerkannten Bank ist. Schließlich muss das System erweitert werden, so dass die Bank zusätzlich die Transaktion und somit die Bezahlung des Lieferanten garantiert. Man wird verstehen, dass die Begriffe „Kunde" und „Lieferant" für beliebige zwei Parteien einer Internet-Kommunikation gelten können.

[0015] Es ist ersichtlich, dass geeignete Kombinationen der beschriebenen Systeme ein sicheres Fundament für den Gebrauch des Internets und der darüber verfügbaren Dienste und Funktionen bietet. Wir haben jedoch erkannt, dass es in der Praxis von eCommerce nur mit diesen Systemen eine Reihe von Problemen gibt, die nachfolgend erörtert werden.

[0016] Bei den oben erwähnten sicheren Übertragungsprotokollen und beim Messaging werden Daten gewöhnlich vor der Übertragung verschlüsselt und vor dem Betrachten durch den beabsichtigten Empfänger entschlüsselt. So sind sie, falls die Daten bei der Übertragung abgefangen werden sollten, vor der Einsicht durch unbefugte Drittparteien sicher, es sei denn, dass diese den geheimen Verschlüsselungskey des Verschlüsselungsalgorithmus kennen oder ermitteln können.

[0017] Das Ver- und Entschlüsseln von Daten an jedem Ende einer sicheren Verbindung oder Nachricht erfordert erhebliche Verarbeitungsleistung. Zusätzlich müssen die sendende und die empfangende Partei im Besitz desselben Verschlüsselungskey des Verschlüsselungsalgorithmus, mit derselben kryptografischen Stärke, sein, damit das System erfolgreich arbeiten kann. Dies stellt häufig ein Problem dar, beispielsweise dann, wenn Vorschriften für den Import oder Export von Daten in ein oder aus einem Computersystem die Verwendung von stärkeren Algorithmen verbieten, so dass die Verbindung oder Nachricht mit einer geringeren kryptografischen Stärke verschlüsselt werden muss oder eine sichere Kommunikation insgesamt verhindert wird. Demzufolge werden sichere(s) Verbindungen und Messaging häufig nur dort verwendet, wo dies notwendig ist.

[0018] Bei Kommunikationen über das World Wide Web wird die Forderung zum Sichern von Übertragungen durch den Webserver ermittelt und initiiert. Wenn beispielsweise die Übertragung eines Auftragsformulars zum Ausfüllen durch den Kunden durch den Server bevorsteht, dann kann dieser eine sichere Verbindung herstellen, so dass die Auftragsinformationen vor der Rücksendung zum Server verschlüsselt werden. Ebenso kann der Server nach der Erledigung des Auftrags die sichere Verbindung beenden und zur normalen unverschlüsselten Kommunikation zurückkehren.

[0019] Typischerweise ist die einzige Anzeige, die der Benutzer hat, dass eine Verbindung gesichert ist, ein im Browser-Fenster erscheinendes Icon (gewöhnlich in Form eines Vorhängeschlosses). Wenn das Icon erscheint, kann der Benutzer den Browser gewöhnlich abfragen, um die Stärke des verwendeten Verschlüsselungsalgorithmus festzustellen, und kann entscheiden, ob er eintritt oder nicht, und kann dann empfindliche Informationen wie z. B. Kreditkarten- und Adressdetails senden.

[0020] In der Praxis prüfen jedoch Benutzer häufig nicht, ob die Verbindung sicher ist, und noch viel weniger, ob sie die geeignete kryptografische Stärke hat, um die übertragenen Informationen zu schützen. Zur Lösung dieses Problems bieten Email-Anwendungen wie z. B. „Gutlook" von Microsoft die Fähigkeit zum vorgabemäßigen Verschlüsseln aller Emails.

[0021] Durch die weit verbreitete Verwendung von Benutzernamen und Passwörtern ist ein Managementproblem für viele Internet-Benutzer aufgrund der riesigen Zahl entstanden, die man sich merken muss, besonders dann, wenn gute Sicherheitspraktiken ein häufiges Ändern von Passwörtern verlangen. Ebenso müssen Benutzer häufig viele verschiedene Benutzernamen benutzen, da jemand anders bereits auf einer bestimmten Site ihren ‚Favorit' benutzt hat. Möglichkeiten zum Merken und automatischen Ausfüllen von Benutzernamen- und Passwortfeldern bei nachfolgenden Gelegenheiten werden in Webbrowsern wie z. B. dem „Internet Explorer" von Microsoft und durch zusätzliche ‚Helper'-Dienstprogramme wie „Gator" von Gator.com bereitgestellt. Diese Einrichtungen führen typischerweise eine Datei von Benutzernamen, Passwörtern und der Webseite, für die sie gelten. Diese Dateien werden verschlüsselt, um zu gewährleisten, dass nur der richtige Benutzer darauf zugreifen kann. Wenn solche Benutzernamen- und Passwortdateien verloren gehen oder unverfügbar werden, z. B. dann, wenn der autorisierte Benutzer den Verschlüsselungskey vergessen hat oder nicht mehr erreichbar ist, um ihn zu geben, oder wenn die Datei versehentlich oder betrügerisch verloren, zerstört oder verfälscht wurde, dann kann der Zugang zu Internet-Konten und -Diensten verloren gehen und jede Site muss individuell besucht werden, um den/das notwendige(n) Benutzernamen und/oder Passwort zu ersetzen oder zurückzugewinnen. Dies kann ein sehr kostspieliges Problem für Firmen im Hinblick auf verlorenen Zugang und Administrationszeit bedeuten. Zudem sind solche gemerkten Benutzernamen und Passwörter nur für die Verwendung auf der Maschine verfügbar, auf der sie ursprünglich benutzt wurden. Wenn der Benutzer zu einer anderen Maschine geht oder mehrere Maschinen benutzt, dann sind die gespeicherten Benutzernamen und Passwörter für ihn von diesen anderen Maschinen aus nicht zugängig.

[0022] Alle Unternehmen, und viele individuelle Benutzer, sind gesetzlich verpflichtet, genaue Aufzeichnungen über die von ihnen unternommenen Transaktionen zu führen, aber für eCommerce-Transaktionen kann sich dies als schwierig erweisen. Unternehmen müssen Aufzeichnungen für Prüfzwecke führen, z. B. um im Falle eines Disputs die Bedingungen nachzuweisen, unter denen Waren bestellt wurden. Solche Aufzeichnungen lassen sich in einer eCommerce-Umgebung weitaus schwerer führen, die es erfordert, dass der Benutzer beispielsweise Kopien von per Email gesendeten Aufträgen aufbewahrt oder die Webseitenquittung von einem Website-Kauf ausdruckt. Für den Benutzer ist dies arbeitsaufwändig und es gibt keine Garantie, dass solche erzeugten Aufzeichnungen vollständig oder zuverlässig sind.

[0023] Eine automatisierte Lösung für das Führen von Aufzeichnungen von eCommerce-Transaktionen bietet die „Max Manager" Anwendung von Max Manager. Max Manager erfasst Quittungsseiten auf bekannten Websites, extrahiert Transaktionsinformationen von diesen Quittungsseiten und speichert dann lokal sowohl die Quittungsseite als auch die extrahierten Transaktionsinformationen auf der Maschine, auf der die Anwendung läuft. Um jedoch arbeiten zu können, müssen dem Max Manager die genaue Adresse und das genaue Layout der Quittungsseite gegeben werden. Max Manager stellt fest, dass eine eCommerce-Transaktion stattgefunden hat, indem er entweder die Adresse der Empfangsseite erfasst oder die gerade mit einem Browser betrachtete Seite mit dem Layout der Quittungsseite vergleicht, mit der er gefüttert wurde. Wenn er eine Quittungsseite identifiziert hat, dann werden die relevanten Transaktionsdetails von der Quittungsseite mit Hilfe des bekannten Layout der Seite als Schablone für Vergleichszwecke extrahiert. Ein erheblicher Nachteil mit Max Manager ist, dass er nur zum Extrahieren von Daten von den Seiten verwendet werden kann, für die er mit Details gefüttert wurde. Dazu kommt, wenn sich das Layout der Quittungsseite ändert, dann kann Max Manager Daten von der Seite erst dann sinnvoll extrahieren, wenn er mit einer neuen Schablone für das geänderte Layout gefüttert wird. Da sich Websites häufig ändern, muss Max Manager

ständig auf dem neuesten Stand gehalten werden, um solche Änderungen zu berücksichtigen. Dies ist im großen Maßstab unpraktisch und führt unweigerlich dazu, dass Transaktionen ausgelassen oder, was noch schlimmer ist, inkorrekt gemeldet werden.

[0024] Probleme entstehen auch durch die Tatsache, dass Computer-Terminals verteilt sind, was häufig bedeutet, dass sich Terminals und Benutzer an unterschiedlichen Orten befinden. In Multiuser-Umgebungen können Benutzermaschinen physisch miteinander verbunden sein, z. B. über ein Ortsnetz („LAN"), das als Gateway zur Verbindung mit dem Internet dient. Sie können auch mit lokalen Servern wie z. B. dem „Exchange Server" von Microsoft verbunden sein, der als zentrale Sammel- und Verteilungsstelle für Email-Nachrichten dient, und mit dem „Proxy Server" von Microsoft, der sowohl als Cache zum Verbessern der Leistung häufig besuchter Websites als auch als Filter zum Verhüten des Zugriffs auf bestimmte Websites dient, die möglicherweise als unerwünscht designiert wurden. Was den Austausch von Informationen betrifft, ausgenommen dann, wenn eine Nachricht zwischen zwei lokalen Benutzern gesendet wird, so arbeitet jedoch jeder Benutzer völlig isoliert von anderen am selben Ort. Dies bedeutet ein ernsthaftes Managementproblem für Firmen und andere Organisationen, die kein Mittel haben, um von zentraler Stelle aus Mitarbeiteraktivitäten zu kontrollieren, und sie können nicht von signifikanten Kosteneinsparungen profitieren, die durch die gemeinsame Nutzung von Informationen erzielt werden können. So könnten z. B. zwei Benutzer in einer Organisation unabhängig Email-Nachrichten empfangen, die vom selben Sender digital signiert wurden. Beide Empfänger müssen das digitale Zertifikat separat validieren, so dass zwei Validierungsgebühren anfallen, von denen wenigstens eine unnötig wäre.

[0025] Ein System und ein Verfahren zum Erzeugen, Bearbeiten und Verteilen von Regeln zum Verarbeiten von elektronischen Nachrichten ist aus dem US-Patent Nr, US 5,917,489 bekannt. Solche Regeln werden von Workstationbenutzern als Hilfe beim Löschen, Ablegen und Antworten auf ihre Nachrichten aufgestellt.

[0026] Die US 5,947,149 offenbart ein Steuersystem für Netzwerkressourcen-Sicherheitsdienste mit einem Event-Manager, der das Niveau an kryptografischer Komplexität ändert.

[0027] Die vorliegende Erfindung stellt zusätzliche Funktionalität für die oben erwähnten Systeme bereit, um deren inhärente Probleme abzumildern und ein einzelnes integriertes Informationsaustauschsystem bereitzustellen.

ZUSAMMENFASSUNG DER ERFINDUNG

[0028] Die Erfindung ist in den Hauptansprüchen dargelegt, auf die nunmehr Bezug genommen werden sollte. Vorteilhafte Merkmale der Erfindung sind in den Nebenansprüchen dargelegt.

[0029] Das Informationsmanagementsystem bietet viele Vorteile in der eCommerce-Umgebung für online handelnde Unternehmen, die davon profitieren können, dass sie die von ihrem Personal durchgeführten Transaktionen gemäß ihren in den Richtliniendaten codierten Anweisungen regulieren, Aufzeichnungen von Passwörtern und online getätigten Geschäften automatisch führen, die Bezahlung für unnötige Überprüfungen der Gültigkeit von digitalen Zertifikaten vermeiden und eine allzeit sichere Übertragung von Daten durch ihr Personal gewährleisten können.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0030] Die bevorzugte Ausgestaltung der Erfindung wird nachfolgend ausführlicher beispielhaft und mit Bezug auf die Begleitzeichnungen beschrieben. Dabei zeigt:

[0031] Fig. 1 eine schematische Darstellung der derzeitigen Anordnung von Systemen und Betriebsmitteln, aus denen sich das Internet zusammensetzt, gemäß dem Stand der Technik;

[0032] Fig. 2 eine schematische Darstellung der bevorzugten Ausgestaltung der Erfindung, in einer Firmenumgebung ausgeführt;

[0033] Fig. 3 eine schematische Darstellung des Betriebs eines Webbrowsers gemäß der bevorzugten Ausgestaltung der Erfindung;

[0034] Fig. 4 eine Darstellung eines von einem Webbrowser erzeugten typischen Eingabefensters;

[0035] Fig. 5 eine schematische Darstellung des Betriebs eines Email-Client gemäß der bevorzugten Ausgestaltung der Erfindung;

[0036] Fig. 6 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzugten Ausgestaltung der Erfindung zum Erfassen von Benutzernamen- und Passwortwerten, die von einem Benutzer zu einer fernen Website übertragen werden;

[0037] Fig. 7 eine Darstellung von beispielhaften Richtliniendaten, die Kontrollbedingungen zum Aufzeichnen von Daten vorgeben;

[0038] Fig. 8 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzug-

ten Ausgestaltung der Erfindung zum Erkennen von in Daten enthaltenen Kreditkartennummern, die zu oder von einem Webserver oder einem Email-Client übertragen wurden;

[0039] Fig. 9 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzugten Ausgestaltung der Erfindung zum Feststellen der Gültigkeit eines von einem Benutzer empfangenen digitalen Zertifikats;

[0040] Fig. 10 eine Illustration von beispielhaften Richtliniendaten zum Ermitteln, ob ein digitales Zertifikat verifiziert werden soll oder nicht;

[0041] Fig. 11 ein Fließschema, das illustriert, wie die in Fig. 10 gezeigten beispielhaften Richtliniendaten benutzt werden, um zu ermitteln, ob eine Verifizierung für ein digitales Zertifikat nötig ist oder nicht;

[0042] Fig. 12 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzugten Ausgestaltung der Erfindung zum Identifizieren von Übertragungen von einem Benutzer oder zu einem Benutzer, die einen Teil einer eCommerce-Transaktion beinhalten;

[0043] Fig. 13 eine Illustration von beispielhaften Richtliniendaten, die mit dem in Fig. 12 illustrierten Verfahren benutzt werden sollen, um eine Transaktion zu identifizieren;

[0044] Fig. 14 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzugten Ausgestaltung der Erfindung zum Aufzeichnen von Übertragungen, die als einen Teil einer einzelnen Transaktion umfassend identifiziert wurden, um einen Datensatz der Transaktion zu bilden;

[0045] Fig. 15 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzugten Ausgestaltung der Erfindung zum Zulassen oder Ablehnen von identifizierten Transaktionen auf der Basis einer vorbestimmten Richtlinieneinstellung; und

[0046] Fig. 16 eine Illustration von beispielhaften Richtliniendaten zum Ermitteln, ob eine identifizierte Transaktion eine Zulassung erfordert, und zum Identifizieren eines geeigneten Billigers (Approver);

[0047] Fig. 17 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzugten Ausgestaltung der Erfindung zum Ermitteln eines geeigneten Verschlüsselungsniveaus für eine Übertragung, und um es zuzulassen, dass die Übertragung nur dann erfolgt, wenn dieses Niveau gegeben ist;

[0048] Fig. 18 eine Illustration von beispielhaften Richtliniendaten, die die benötigte Verschlüsselungsstärke für verschiedene Datentypen vorgibt;

[0049] Fig. 19 eine Illustration von beispielhaften Richtliniendaten zum Steuern des Umleitens von abgehenden Nachrichten;

[0050] Fig. 20 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzugten Ausgestaltung der Erfindung zum Umleiten von abgehenden Nachrichten zu einer Drittpartei zum Prüfen vor der Übertragung anhand der in Fig. 19 gezeigten Richtliniendaten;

[0051] Fig. 21 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzugten Ausgestaltung der Erfindung zum Steuern des Heraufladens von Informationen auf eine firmenexterne Website anhand der in Fig. 19 gezeigten Richtliniendaten;

[0052] Fig. 22 eine Illustration von beispielhaften Richtliniendaten zum Steuern des Weiterleitens von Nachrichten zu firmeninternen oder -externen Empfängern;

[0053] Fig. 23 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß einer bevorzugten Ausgestaltung der Erfindung unter Anwendung der in Fig. 22 gezeigten Richtliniendaten;

[0054] Fig. 24 eine Illustration von beispielhaften Richtliniendaten zum Steuern, ob eine abgehende Nachricht digital signiert werden soll oder nicht; und

[0055] Fig. 25 ein den Betrieb eines Einsteckmoduls illustrierendes Fließschema gemäß der bevorzugten Ausgestaltung der Erfindung unter Anwendung der in Fig. 24 gezeigten Richtliniendaten.

BESCHREIBUNG DER BEVORZUGTEN AUSGESTALTUNG

[0056] Das bevorzugte System bietet Benutzern des Internets eine automatische Möglichkeit zum Verwalten des Flusses von Informationen auf einem Computersystem. Es stellt Einrichtungen zum Verwalten des Sicherheitsniveaus, auf dem Übertragungen stattfinden, Einrichtungen zum Aufzeichnen von Online-Transaktionen und zum Verweisen von vor der Ausführung stehenden Transaktionen an Drittparteien zur Billigung sowie Mittel zum Stoppen von Transaktionen bereit, wenn die Billigung verweigert wird; es bietet auch Einrichtungen zum Extrahieren und Aufzeichnen von relevanten Daten von empfangenen oder kurz vor dem Absenden stehenden Übertragungen und zum intelligenten Verwalten der Übertragung von Emails bereit.

[0057] Das bevorzugte System bietet Lösungen für

viele der Probleme, mit denen über das Internet handelnde eCommerce-Unternehmen konfrontiert werden; demzufolge betrifft die nachfolgende beispielhafte Erörterung vornehmlich die Implementation und Verwendung des Systems durch ein Unternehmen einer sinnvollen Größe, das wenigstens einige seiner Geschäfte über das Internet tätigt. Man wird verstehen, dass jedoch jedermann, inklusive Unternehmen jeder Größe oder Art und Privatpersonen, die das Internet benutzen, von den von dem bevorzugten System bereitgestellten Funktionen profitieren können.

[0058] Die Funktionalität des bevorzugten Systems wird über Code-Module implementiert, die in den Webbrowser oder den Email-Client ‚eingesteckt' werden. Diese ‚Einsteck'-Module können zum Steuern und Verändern des Verhaltens des Webbrowsers oder Email-Clients beim Betrieb verwendet werden.

[0059] Viele existierende Webbrowser und Email-Clients sind möglicherweise bereits mit solchen Einsteckmodulen integriert. Im Falle des Internet Explorer von Microsoft ist das Einsteckmodul als ‚Browser Helper' bekannt und ist in dem Dokument „Browser Helper Objects: The Browser the Way You Want It" von Dino Esposito umfassend beschrieben, herausgegeben von der Microsoft Corporation im Januar 1999. Im Falle von Microsoft Gutlook und Exchange-Email-Clients ist das Einsteckmodul als eine ‚Extension' bekannt und ist ausführlicher im Dokument „Microsoft Gutlook and Exchange Client Extensions" von Sharon Lloyd beschrieben, herausgegeben von der Microsoft Corporation im März 1998. Die Verwendung der Einsteckmodule ‚Browser Helper Object' und ‚Extension' im bevorzugten System wird nachfolgend ausführlicher beschrieben.

[0060] Die Verwendung von Browser- oder Email-Client-Einsteckmodulen zum Ausführen der Funktionalität des bevorzugten Systems hat den zusätzlichen Vorteil, dass, da eine Verschlüsselung von Nachrichteninhalt gewöhnlich durch den Browser oder Email-Client selbst erfolgt, eine Untersuchung des Übertragungsinhalts, um z. B. Passwortinformationen zu extrahieren oder das gewünschte Verschlüsselungsniveau zu bestimmen, stattfinden kann, bevor der Inhalt übertragungsbereit verschlüsselt wurde, oder sogar nachdem er empfangen und entschlüsselt wurde.

[0061] Fig. 1 zeigt die Beziehung zwischen Diensteanbietern, typischerweise Unternehmen, die Waren und Dienste über das Internet **10** verkaufen, und Benutzern, die solche Waren und Dienste kaufen möchten. Mit Webbrowsern **22**, **24** und **26** ausgestattete Benutzer können sich über das Internet zuschalten und Webseiteninformationen von Webservern **14** und **18** abrufen. Alternativ können Benutzer mit Email-Anwendungen **20**, **30** und **32** Email-Nachrichten mit abc.com und xyz.com über Email-Server **12** und **16** senden und empfangen.

[0062] In einem Firmenkontext wie z. B. dem, der in der rechten unteren Ecke von Fig. 1 illustriert ist, sind Webbrowser **24** und **26** eines Firmenbenutzers über einen Proxy-Server **28** mit dem Internet verbunden. Der Proxy-Server **28** dient zum Cachen von Webseiten und zum Steuern des Zugriffs -auf Websites. Ebenso hat das Unternehmen Email-Clients **30** und **32**, die mit dem Internet über den Email-Server **34** verbunden sind, der als eine zentrale Sammelstelle für am Unternehmen ankommende Emails dient und die Verteilung der Emails zu einzelnen Benutzern steuert. Man wird verstehen, dass Fig. 1 zwar abc.com und xyz.com als Verkäufer beschreibt, aber ein Unternehmen kann auch sowohl Käufer als auch Verkäufer sein, und die Käufer abc.com und xyz.com würden für die Zwecke dieser Beschreibung als Unternehmensbenutzer beschrieben.

[0063] Im Falle von Emails, die durch eine persönliche Email-Anwendung **20** gesendet und empfangen werden, ist zu bemerken, dass die Mail typischerweise von einem fernen Email-Server gesammelt und verteilt wird, der vom Anbieter des Internet-Verbindungsdienstes bereitgestellt wird, bei dem der persönliche Benutzer abonniert ist.

[0064] Während viele der Merkmale und Funktionen des vorliegenden Systems erhebliche Vorteile für einen individuellen Benutzer bieten, bietet das System den maximalen Vorteil, wenn es in einer Mehrbenutzer-Umgebung arbeitet, bei der Transaktionsinformationen von vielen Benutzern gesammelt werden. Fig. 2 zeigt ein schematisches Diagramm der bevorzugten Konfiguration des Systems in einer Mehrbenutzer-Umgebung. Das bevorzugte System umfasst einen zentralen Managementserver **40**, der mit einer Datenbank **42** und Operatorkonsolen **44** verbunden ist. Der zentrale Managementserver **40** ist auch mit Back Office Application Einsteckmodulen verbunden, die Anwendungsschnittstellen **50**, **52** und eine offene Anwendungsprogrammschnittstelle **54** umfassen, sowie mit Gateway-Komponenten **60**, **62** und **64**. In der Figur ist die Gateway-Komponente **62** als mit Benutzeranwendungseinsteckmodulen verbunden dargestellt, die sich auf einem oder mehreren Benutzermaschinen befinden, die die Einsteckmodule Internet Explorer **70**, Netscape Navigator **72**, Microsoft Gutlook **74** und Lotus Notes **76** umfassen. Diese Einsteckmodule bieten die Funktionalität des bevorzugten Systems in dem Hosting-Programm, in dem sie integriert sind. Es sind vier mögliche Hosting-Programme dargestellt, Internet Explorer, Netscape Navigator, Microsoft Gutlook und Lotus Notes, aber es kann auch jedes andere Programm mit der Fähigkeit benutzt werden, sich am Internet anzuschließen, vorausgesetzt, sein Verhalten kann zum Ausführen der Funktionalität des bevorzugten Systems modifiziert werden.

[0065] Der Anschluss an das Internet **10** erfolgt über die Benutzeranwendungseinsteckmodule und ihre jeweiligen Hosting-Programme.

[0066] Die Gateway-Komponenten **70**, **72** und **74** sind fakultativ, werden aber bevorzugt, da sie eine Skalierung des gesamten Systems ermöglichen, wobei jedes Gateway Informationen speichert und weiterleitet und es gestattet, dass eine beliebige Anzahl von Benutzern zugeschaltet wird.

[0067] Informationen von den mehreren Anwendungseinsteckmodulen **70**, **72**, **74** und **76** für die verschiedenen Anwendungen auf mehreren Benutzermaschinen werden vom zentralen Managementserver **40** gesammelt und in einer assoziierten Datenbank **42** gespeichert.

[0068] Die Back Office Application Einsteckmodule **50**, **52** und **54** ermöglichen eine Verbindung des Systems mit Drittpartei-Managementanwendungen wie z. B. Auftragsbearbeitungs- und Buchhaltungssystemen. So können Transaktionsinformationen von solchen Systemen automatisch eingegeben und verarbeitet werden.

[0069] Operatorkonsolen **44** werden für administrative Zwecke und insbesondere für die Zulassung von Transaktionen bereitgestellt. Während sie in Fig. 2 logisch als direkt mit dem zentralen Managementserver verbunden dargestellt sind, könnten solche Konsolen auf jeder vernetzten Maschine laufen. Wo ein Email- oder Webbrowser-Einsteckmodul ermittelt, dass eine bestimmte Transaktion eine Zulassung erfordert, wird eine Anforderung zum zentralen Managementserver gesendet und bis zur Zulassung durch einen autorisierten Operator in eine Warteschlange gesetzt.

[0070] Der Betrieb des Systems wird durch Richtliniendaten gesteuert, in denen die Vorschriften des Unternehmens in Bezug auf Sicherheit, Autorisierung und die Aktionen, die Benutzer ausführen dürfen, sowie Betriebsinformationen gespeichert sind. Die Richtliniendaten werden vorzugsweise in einer Richtliniendatei auf dem zentralen Managementserver für den Zugriff durch irgendeine der Operatorkonsolen **44**, Back Office Application oder Benutzeranwendungs-Einsteckmodule gespeichert. Der Systemadministrator oder Netzwerk-Supervisor kann eine oder mehrere Richtlinien oder Einstellungen der Richtliniendatei definieren und kann einzelne Benutzer oder Benutzergruppen unterschiedlichen Richtlinien zuordnen und so die Interaktionsfähigkeit eines Benutzers oder sogar die einer Workstation mit dem Internet steuern, ohne Notwendigkeit für ein direktes Einstellen von Parametern und Controls auf jeder Benutzermaschine. Ein Benutzer in der Buchhaltungsabteilung eines Unternehmens kann beispielsweise einer „Buchhaltungsrichtlinie" zugeordnet werden; jede nachfolgende Änderung an dieser Richtlinie führt dann automatisch zu einer Änderung der Fähigkeiten aller dieser Richtlinie zugeordneten Benutzer.

[0071] Es wird bevorzugt, dass die Fähigkeit zum Bearbeiten oder Festlegen der Richtliniendaten auf den Netzwerk-Supervisor oder eine oder mehrere andere autorisierte Personen beschränkt wird. Dies kann dadurch erzielt werden, dass eine oder mehrere Supervisor-Workstations im Netzwerk für einen Zugriff zum Bearbeiten der Richtliniendaten bestimmt werden, wie z. B. Operatorkonsolen **44**.

[0072] Die Richtlinie hat vorzugsweise eine baumartige Struktur, so dass Einstellungen zwangsweise abwärts zu individuellen Richtlinienknoten des Baums gelangen und globale Änderungen rasch vorgenommen werden können, z. B. dann, wenn der Geschäftsführer (CEO) wünscht, dass alle Käufe seine Zulassung erfordern, wenn der Bargeldfluss des Unternehmens zu einem Problem wird. Ein solches richtliniengestütztes System reduziert stark die Latenz, die sowohl in traditionellen Einkaufssystemen als auch in derzeitigen eCommerce-Kaufumgebungen inhärent sind.

[0073] Jeder Benutzer des Netzwerks hat seine eigene Darstellung von Richtliniendaten. Vorzugsweise werden nur die Zweige und Blätter der Richtlinie jedes Benutzers gespeichert, die sich von einer Master-Netzwerkrichtlinie unterscheiden, da dies Speicherplatz spart. Die Richtliniendaten werden zwar vorzugsweise in Dateiform auf dem zentralen Managementserver gespeichert, aber es ist nicht beabsichtigt, dass eine Speicherung der Richtliniendaten nur auf die Dateiform beschränkt ist. Im bevorzugten System kann jede andere Repräsentation oder Codierung von Richtlinieneinstellungen zum Einsatz kommen.

[0074] Die Implementation des Systems in einem Webbrowser oder in einem Email-Client wird nachfolgend ausführlicher beschrieben.

[0075] Benutzung des bevorzugten Systems in einem Webbrowser Fig. 3 zeigt den vereinfachten Betrieb eines Webbrowsers. Der Webbrowser wird in Schritt S100 als Reaktion auf eine Startanforderung entweder vom Benutzer oder automatisch von der Startdatei des Benutzercomputers gestartet. Die Startdatei enthält Befehle zum automatischen Abarbeiten bestimmter Programme beim Booten des Computers. Der Webbrowser fordert nach dem Start typischerweise eine ‚Homepage' an, die vorgabemäßige Ansichtswebseite, gemäß einer vorbestimmten Einstellung. Dies ist in Schritt S102 dargestellt.

[0076] Die Anforderung wird zum richtigen Webserver **90** gesendet, dessen genaue Internet-Adresse gewöhnlich durch Bereichsnamensdienste bestimmt

wird; der Webserver **90** antwortet mit den die Webseite definierenden geeigneten Daten. Dieser Vorgang wird jeweils als Schritte S104 und S106 repräsentiert, was in Schritt S108 resultiert.

[0077] Die die Webseite definierenden Daten bestehen aus dem HTML-Skript und anderen möglichen Datentypen wie XML oder ActiveX und Javascript, das ablauffähige Programme codiert. Der Browser interpretiert diese Daten, zeigt sie an und/oder arbeitet sie ab, je nachdem, was in Schritt S110 angemessen ist.

[0078] Der Browser wartet dann typischerweise auf eine Benutzereingabe in Schritt S112. Eine solche Eingabe kann das Ausfüllen von angezeigten Feldern, das Anklicken einer Hyperlink oder das Eingeben der URL-Adresse einer neuen Webseite beinhalten. Schließlich führen solche Aktionen dazu, dass in Schritt S114 und Schritt S116 eine weitere Anforderung zum Webserver **90** gesendet wird. Die Anforderung kann einfach eine andere Webseitenadresse sein oder sie kann zusätzliche Daten wie z. B. die enthalten, die der Benutzer in die angezeigten Felder eingetastet hat.

[0079] Fig. 4 zeigt ein Beispiel für eine Webseitenanzeige, in der dem Benutzer eine GUI dargeboten wird, um Benutzernamen und Email-Adresse zu empfangen. Wie aus Fig. 4 ersichtlich ist, hat der Benutzer bereits seinen Namen als ‚Fred Smith' in das vorgesehene Namensanforderungsfeld und seine Email-Adresse als ‚fsmith@xyz.com' in das Email-Adressfeld eingegeben.

[0080] Wenn der Benutzer die ‚Submit'-Schaltfläche im Anforderungsfenster anklickt, dann werden die eingegebenen Benutzerdetails in den zum Webserver **90** gesendeten Befehl einbezogen. Ein solcher Befehl könnte wie folgt lauten:
http:_//www.sample.com/_sample2.htm?
UserID=Fred
+Smith&email=fsmith@xyz.com&submit=submit

[0081] Aus dem Obigen ist ersichtlich, dass der Benutzername in den Befehl als Wert einer Variablen namens ‚UserID' integriert wird, und seine Email-Adresse wird als der Wert einer Variable namens ‚Email' integriert.

[0082] Der Befehl wird in Schritt S114 zusammengesetzt und in Schritt S116 zum Webserver **90** gesendet. In Schritt S116 können Benutzername und Email-Adressinformationen z. B. zum Senden von Produktinformationen zum Benutzer per Email oder zwecks Zugang zu anderen Webseiten benutzt werden.

[0083] Das von der bevorzugten Ausgestaltung der Erfindung bereitgestellte Einsteckmodul in Form eines Browser Helper Object (BHO) bietet zusätzliche Funktionalität zur Erweiterung der des standardmäßigen Webbrowsers. Das BHO wird zum Reagieren auf eine Reihe von signifikanten Events implementiert, die beim Arbeiten mit dem Webbrowser auftreten und die vom Benutzer zwecks Interaktion mit verschiedenen Websites und Seiten angewiesen wird.

[0084] Das BHO wird zum Überwachen von dem Webserver vom Browser submittierten Navigationsanforderungen und Daten und zum Identifizieren von für den Benutzer eindeutigen Daten implementiert. Dies kann einfach durch Absuchen des abgehenden Datenstroms nach vorbestimmten Wörtern oder Ausdrücken geschehen. In dem in Fig. 4 gezeigten obigen Fall kann nach zwei Variablendefinitionen ‚UserID' und ‚Email' gesucht werden und die darauf folgenden Daten können extrahiert und gespeichert werden. Alternativ kann das BHO nach dem ‚?' Symbol suchen, das das Ende der verbundenen URL-Adresse und die Tatsache anzeigt, dass danach Daten folgen. Das BHO kann auch den von der Webseite, mit der es verbunden ist, empfangenen eingehenden Datenstrom überwachen.

[0085] Das BHO kann auch zum Überwachen des Betriebs des Webbrowsers selbst verwendet werden. während des Betriebs des Webbrowsers erzeugt dieser ‚Events', um mitabhängigen Software-Modulen oder Objekten mitzuteilen, dass gerade etwas Signifikantes aufgetreten ist oder dass eine Aktion soeben beendet wurde. Der Name des Events ist gewöhnlich an sich beschreibend für das, was gerade aufgetreten ist; normalerweise sind auch zusätzliche Daten verfügbar, die das Event ausführlicher beschreiben. Das BHO wird zum Einfangen dieser Events und zum Treffen von Maßnahmen in Abhängigkeit davon implementiert.

[0086] Ein solches Event, für dessen Beantwortung das BHO implementiert wird, heißt ‚BeforeNavigate2', das der Webbrowser startet, wenn der Benutzer anfordert, dass der Browser zu einer neuen Seite navigiert. Das Event wird ausgegeben und kann vom BHO erkannt werden, bevor die angeforderte Seite heruntergeladen wird, so dass das BHO jede geeignete Maßnahme ergreifen kann, bevor der Benutzer die Seite sieht. Eine solche Aktion könnte die Aufzeichnung der Seite und eventueller Daten sein, die als Reaktion auf diese Seite in einer Datenbank submittiert wurden. Eine andere solche Aktion könnte die Identifikation der URL-Adresse der angeforderten Seite von dem Event oder das Verhüten des Herunterladens der Seite sein.

[0087] Ein anderes Event, das das BHO einfängt, ist das ‚DocumentComplete'-Event, das vom Webbrowser eingeleitet wird, wenn eine neue Seite vollständig von der Website in den Speicher heruntergeladen wurde. Die Seite wird in Form eines Document Object

codiert, entsprechend dem Document Object Model (DOM) von Microsoft. Das DOM bietet umfassenden Zugang zu den die Seite umfassenden Daten, so dass das BHO für es interessante Datenelemente extrahieren kann. So kann das BHO beispielsweise Daten vom DOM anfordern, um zu ermitteln, ob die Seite Teil einer eCommerce-Transaktion bildet. Es kann dies durch Absuchen von Objekten im DOM nach Begriffen wie ‚Quittung' oder ‚Kontonummer' tun.

[0088] Das BHO kann das DOM auch zum Ermitteln der Feldnamen oder Feldtypen von Daten benutzen, die auf einer Webseite angefordert werden. Die vom Benutzer in solche Felder eingegebenen Daten können dann vom DOM extrahiert und gespeichert oder es kann darauf reagiert werden. Feldnamen sind typischerweise für das Gespeicherte beschreibend; Passwörter werden beispielsweise oft in einem Feld namens ‚Passwort' gespeichert, daher kann auf einer Webseite danach gesucht werden. Nach Kreditkartennummern kann auf ähnliche Weise gesucht werden. Gewöhnlich sind Passwortfelder von einem solchen Typ, dass eingegebene Daten als Sternchen angezeigt werden. Auch dies kann anhand einer Analyse des DOM bestimmt und zum Identifizieren relevanter Daten verwendet werden.

[0089] In einer von einer Website heruntergeladenen Webseite würde es normalerweise keine Benutzerdaten geben, aber sie würden vom Benutzer in ein HTML-Formular eingegeben. Die potentiell empfindlichen Benutzerdaten werden gewöhnlich über den Webserver zur Website übertragen, wenn der Benutzer eine ‚Submit'-Schaltfläche anklickt. In dieser Stufe kann das BHO das vom Webbrowser ausgegebene ‚Submit'-Event einfangen und auf das DOM zugreifen, um die Benutzerdaten zu extrahieren, und kann bei Bedarf verhindern, dass diese Daten gesendet werden.

[0090] Ver- und Entschlüsselung auf einer sicheren Verbindung erfolgen jeweils nach Punkt C und vor Punkt A in Fig. 3. So kann das BHO die Daten analysieren, bevor sie verschlüsselt werden oder nachdem sie entschlüsselt wurden. Dies ist vorteilhaft, da es nicht nötig ist, dass das BHO selbst Daten codiert oder decodiert. Dies hat keinen Einfluss auf die Fähigkeit zu bestimmen, ob die Verbindung sicher ist oder nicht, da eine sichere Verbindung anhand der Protokollkennung „https" am Anfang der aktuellen URL-Adresse identifiziert werden kann. Es wird bevorzugt, dass eine Untersuchung des Inhalts der Übertragung vor der Verschlüsselung oder nach der Entschlüsselung stattfindet.

[0091] Erörterung des Betriebs eines Email-Clients Es werden nun der Betrieb eines typischen Email-Client und die Implementation der bevorzugten Ausgestaltung in einem Email-Client mit Bezug auf Fig. 5 der Zeichnungen beschrieben.

[0092] Fig. 5 zeigt den vereinfachten Betrieb eines Email-Clients. Empfang und Senden erfolgen typischerweise unabhängig und diese Operationen sind in Fig. 5 separat einander gegenüber liegend dargestellt, jeweils beginnend mit Schritt S120 und Schritt S130.

[0093] Die „Nachricht empfangen" Operation eines Email-Client wird in Schritt S120 eingeleitet. Dies erfolgt automatisch in vorbestimmten Intervallen, um den, Benutzer über eventuelle neu empfangene Nachrichten informiert zu halten, oder es kann als Reaktion darauf erfolgen, dass der Benutzer manuell ein ‚Nachrichten empfangen' Icon anklickt. Der Start dieser Operation hat zur Folge, dass der Email-Client den Email-Server **95** abruft und eventuelle neue Nachrichten auf die Maschine des Benutzers herunterlädt. In Schritt S122 wird eine Email-Nachricht vom Email-Client empfangen. Typischerweise wird eine neue Nachricht nach dem Empfang in eine ‚Inbox' gesetzt, wobei die empfangenen Nachrichtenköpfe (z. B. Name des Senders, Datum und Titel) zu einer Liste angeordnet sind. Der Benutzer klickt dann auf den entsprechenden Eintrag in der Liste, um die volle Nachricht zu lesen, so dass diese auf seinem Computerschirm erscheint. Die Email-Nachricht wird in Schritt S124 angezeigt.

[0094] Im Falle einer abgehenden Email wählt der Benutzer in Schritt S130 eine ‚Email verfassen' Option. Als Reaktion darauf stellt der Email-Client eine Schnittstelle bereit, die einen Texteditor umfasst, in dem der Benutzer den Haupttext der Nachricht und andere Informationen wie z. B. Zieladresse, Betreff usw. eingeben kann. Der Benutzer verfasst die Nachricht in Schritt S132 und weist dann das Absenden an, indem er ein Icon oder eine Menüoption wählt, das/die im Email-Client zum Ausgeben eines ‚Senden'-Befehls vorgesehen ist. Die Email wird in Schritt S134 zum Email-Server zur Übertragung zum Empfänger gesendet. Wenn der Email-Client eine Verschlüsselung durchführt, dann erfolgt dies in Schritt S134 vor der Übertragung.

[0095] In der bevorzugten Ausgestaltung wird zusätzliche Funktionalität für den Email-Client über ein Einsteckmodul bereitgestellt. Der Email-Client ist vorzugsweise einer der von Microsoft angebotenen, wie z. B. der Microsoft Exchange Client oder der Microsoft Gutlook Client, und das Einsteckmodul wird als eine Exchange Client Extension codiert. Diese sind in dem oben erwähnten Dokument „Microsoft Gutlook and Exchange Client Extensions" von Sharon Lloyd beschrieben.

[0096] Eine Exchange Client Extension ist ein Komponentenobjekt, das dem Component Object Model (COM) in Microsoft Windows entspricht und die Exchange IExchExt Schnittstelle verwendet. Diese Schnittstelle bietet eine Reihe von zusätzlichen

Schnittstellen zum Modifizieren des Betriebs des Exchange Email Client, wie z. B. die IExchExtCommands-Schnittstelle, die es zulässt, dass das existierende Client-Verhalten ersetzt oder modifiziert wird und dass neue Befehle zu den Client-Menüs hinzugefügt werden; und die IExchExtEvent-Schnittstelle, die es zulässt, dass das kundenspezifische Verhalten zum Handhaben von Client-‚Events' implementiert wird, wie z. B. die Ankunft neuer Nachrichten, Lesen, Schreiben, Senden von Nachrichten und Lesen und Schreiben von anhängenden Dateien. Auch die Schnittstellen IExchExtMessageEvents, IExchExtSessionEvents und IExchExtAttachmentEvents sind vorhanden und bieten zusätzliche Funktionalität für die in den einzelnen Schnittstellennamen angedeuteten spezielleren Aufgaben.

[0097] In der bevorzugten Ausgestaltung wird die Exchange Client Extension, die das Einsteckmodul bildet, zum Antworten auf Client-‚Events' implementiert, die vom Client-Programm ausgelöst werden, wenn dieses Operationen ausführt und Aktionen vollzieht. Die fraglichen ‚Events' werden von den oben erwähnten COM-Schnittstellen bereitgestellt. Die Überwachung des Email-Clients durch das Einsteckmodul kann daher als zu der Art und Weise analog angesehen werden, in der das BHO-Einsteckmodul den Betrieb des Webbrowsers überwacht.

[0098] Das Email-Client-Einsteckmodul wird beispielsweise zum Antworten auf das ‚OnDelivery'-Event implementiert, das ausgelöst wird, wenn eine neue Nachricht von dem assoziierten Mailliefersystem empfangen wird und bevor es für den Benutzer sichtbar ist. Das ‚OnDelivery'-Event enthält Informationen zum Zugreifen auf die verschiedenen Teile der Email-Nachricht, die heruntergeladen wurden und die sich im Speicher befinden. Der Nachrichtenkopf, der Nachrichtenhaupttext und eventuelle Nachrichtenanhänge werden im Speicher als Eigenschaften des Nachrichtenobjekts codiert, auf die separat durch MAPI-(Mail Application Program Interface)-Anrufe zugegriffen werden kann.

[0099] Anhand der als Teil des ‚OnDelivery'-Events gegebenen Informationen kann das Einsteckmodul auf den Nachrichtenkopf zugreifen und beispielsweise die Identität des Senders ausziehen. Ferner kann das Einsteckmodul von MAPI-Anrufen erhaltene Informationen zum Absuchen des Texts einer empfangenen Nachricht nach Schlüsselwörtern oder relevanten Daten benutzen. Es kann nach Anzeichen auf eine eCommerce-Transaktion suchen, indem es signifikante Wörter wie ‚Quittung' oder ‚Kontonummer' identifiziert. Die Nachricht kann dann für Prüfzwecke gespeichert werden. Im Falle eines unzugelassenen Senders oder eines schädlichen Nachrichteninhalts kann die Nachricht ungesehen gelöscht werden.

[0100] Die Analyse einer empfangenen Email erfolgt daher an Punkt A in Fig. 5, bevor sie vom Benutzer betrachtet wird. Die Email wird vorzugsweise untersucht, bevor sie in die Inbox gesetzt wird. Wo eine Nachricht nicht automatisch vor dem Setzen in die Inbox entschlüsselt wird, z. B. dort, wo der Benutzer einen Entschlüsselungskey eingeben muss, da wird die Nachricht unmittelbar nach der Entschlüsselung, aber vor der Einsicht untersucht. Digitale Zertifikate können als Anhänge an die Email enthalten sein und können vor der Einsicht leicht untersucht werden, so dass geeignete Aktionen wie z. B. eine Validierung ausgeführt werden können.

[0101] Ein weiteres signifikantes Client-Event, für dessen Beantwortung das Einsteckmodul implementiert wird, ist das ‚OnWriteComplete'-Event, das ausgelöst wird, wenn der Benutzer den ‚Senden'-Befehl selektiert und den Email-Client aufgefordert hat, eine neue Email-Nachricht zum Mailliefersystem zu übertragen. Dieses Event wird an Punkt B in Fig. 5 vor der Übertragung und vor einer Verschlüsselung ausgeführt. Die neue Nachricht, die übertragen werden soll, wird ebenfalls im Speicher als Objekt gespeichert, auf das mit MAPI-Anrufen zugegriffen werden kann. Das Einsteckmodul kann die MAPI-Anrufe zum Durchsuchen des Inhalts der abgehenden Email nach sensitiven Daten wie Kreditkartennummern benutzen und nachfolgend bewirken, dass die Nachricht aufgezeichnet oder sogar gesperrt wird.

Betrieb der Einsteckmodule

[0102] Die bevorzugte Implementation der Einsteckmodule Webbrowser und Email-Client wurde oben mit Bezug auf die Fig. 3 und Fig. 5 beschrieben. Als Nächstes wird die durch die Einsteckmodule gegebene Funktionalität ausführlich mit Bezug auf die Fig. 6 bis Fig. 18 beschrieben.

Identifizieren und Aufzeichnen von Benutzernamen, Passwörtern und anderen Informationen

[0103] Das bevorzugte System bietet Mittel zum automatischen Identifizieren, Sammeln und Speichern von Daten, die in Übertragungen zu und von einer Benutzerworkstation enthalten sind, insbesondere die Benutzernamen und Passwörter, die von einem Benutzer zum Zugreifen auf Website-Seiten, FTP-(File Transfer Protocol)-Sites und andere solche Sites auf dem Internet eingegeben werden.

[0104] Systeme, die derzeit über Einrichtungen zum Aufzeichnen von Passwörtern verfügen, tun dies derzeit nur dann, wenn ein Benutzer auf die Option ‚Remember Password' (Passwort merken) auf der GUI klickt. Das Passwort wird in einer geschützten lokalen Datei auf der Maschine des Benutzers gespeichert, die nur dann öffnet, wenn sich der Benutzer für diese Maschine authentifiziert, z. B. durch Eingeben seines Benutzernamens und des Passwortes beim Booten.

Die Passwort-merken-Option bewirkt, dass sich das System das Passwort beim nächsten Besuch des Benutzers gemerkt hat, da das Passwortfeld mit diesem Passwort vorausgefüllt ist, so dass der Benutzer es nicht jedes Mal, wenn es verlangt wird, neu einzugeben braucht. Der Nachteil des lokalen Speicherns dieser Passwortdatei ist, dass der Benutzer, wenn er zu einer anderen Maschine geht, keinen Zugang zu der gespeicherten Passwortdatei hat und das Passwort selbst neu eingeben muss.

[0105] Das bevorzugte System identifiziert Passwörter automatisch ohne Notwendigkeit für einen Befehl vom Benutzer und speichert die identifizierten Passwörter und Benutzernamen in einem Daten-Repository. Dies ist vorzugsweise eine zentrale Datenbank **42**. So können die Passwörter eines beliebigen Benutzers unabhängig von dem Terminal abgerufen werden, an dem sich der Benutzer einloggt, unter der Voraussetzung, dass das Terminal Zugang zu der zentralen Datenbank hat.

[0106] Identifizierte Passwörter und Benutzernamen werden in der Datenbank zusammen mit den Feldnamen, in denen sie auf der ursprünglichen Website gespeichert sind, und der Adresse der Internet-Site gespeichert, zu der sie übertragen und auf der sie benutzt werden. Site-Informationen können ganz einfach abgerufen werden, da sie in der HTTP-Anforderung enthalten sind, die die Passwort- und Benutzerinformationen dieser Site submittieren, sowie in der Darstellung der im Speicher befindlichen Webseite.

[0107] Die in der Datenbank gespeicherten Informationen sind sicherheitshalber vorzugsweise verschlüsselt, so dass nur eine ausgewählte Anzahl von Personen, wie z. B. Netzwerk-Supervisor, Systemadministratoren oder Unternehmensleiter, Zugang dazu haben. Sie können entweder durch eine Workstation im Netzwerk, durch Eingeben eines Benutzernamens oder eines Passwortes, um sich zu identifizieren, oder durch eine Supervisor-Workstation wie z. B. Operatorkonsolen **44** auf die Datenbank zugreifen.

[0108] Diese Speicherung von Benutzernamen und Passwörtern zusammen mit Adressdetails bietet einen erheblichen Vorteil für Unternehmen, die Online-Einrichtungen benutzen. Mit den derzeitigen Techniken kann, wenn ein Benutzer sein Authentifizierungspasswort vergisst, was einen Zugriff auf die geschützte Datei verhindert, oder das Unternehmen verlässt, ohne das Passwort mitgeteilt zu haben, nicht auf den Internet-Dienst zugegriffen werden. Eine ähnliche Situation entsteht, wenn die geschützte Datei beschädigt oder gelöscht wurde oder auf andere Weise verloren gegangen ist. Jeder Internet-Dienst muss dann nacheinander besucht werden, um das verlorene Passwort zu ersetzen oder zurückzugewinnen, was im Hinblick auf verlorene Zugriffs- und Administrationszeit sehr kostspielig sein kann. Mit dem bevorzugten System können die Passwortinformationen aus der zentralen Datenbank zurückgeholt werden, so dass der Zugang zu Websites nicht verloren geht.

[0109] Fig. 6 ist ein Fließschema, das den Betrieb eines Einsteckmoduls schematisch illustriert, das zum Extrahieren von Benutzernamen- und Passwortinformationen aus zu einem Webserver zu übertragenden Daten implementiert wird.

[0110] In Schritt S150 beginnt das Einsteckmodul mit dem Parsen der Daten, die als Nächstes vom Browser zum Webserver übertragen werden sollen. Dies erfolgt an Punkt ‚C' in dem in Fig. 3 illustrierten Vorgang. Die Steuerung geht dann zu Schritt S152, wo das Einsteckmodul ermittelt, ob die zu übertragenden Daten Benutzernamen- oder Passwortinformationen enthalten oder nicht.

[0111] Die Passwörter oder Benutzernamen können in der oben mit Bezug auf die Fig. 3, Fig. 4 und Fig. 5 beschriebenen Weise z. B. durch Identifizieren von Feldnamen in einem submittierten Befehl oder mit Hilfe des DOM identifiziert werden, um nach Feldnamen, Feldtypen oder dem zum Identifizieren der Daten auf Webseiten verwendeten Anzeigeverfahren zu suchen. Sie können auch von der HTML von Webseiten, den Einblendfenstern oder GUIs (grafische Benutzeroberflächen) abgerufen werden, die von fernen Servern oder Providern auf dem World Wide Web präsentiert werden, oder sogar durch Scannen des Inhalts von Email-Nachrichten.

[0112] Das Identifizieren von Passwörtern und Benutzernamen in übertragenen Befehlen oder im DOM einer Webseite von ihren Feldnamen stützt sich auf die Feldnamen, die ihren Zweck mit offensichtlichen Etiketten wie ‚Passwort' oder ‚Benutzername' beschreiben. Falls der Feldname an sich keine Bedeutung hat, kann die Natur von übertragenen Daten vom Feldtyp der Daten, d. h. ‚String' oder ‚Integer' usw., oder von dem zum Eingeben der Daten benutzten Anzeigeverfahren abgeleitet werden. Felder, die ein Passwort aufnehmen sollen, können anhand der Repräsentation beim Suchen nach einem ‚Passwort'-Feldtyp im DOM identifiziert werden. Textboxen auf einer Webseite, in die z. B. Passwortdaten eingegeben werden sollen, zeigen typischerweise jedes eingegebene Zeichen als ein Sternchen an; diese Eigenschaft kann anhand des DOM ermittelt und zum Inferieren benutzt werden, dass in die Textbox eingegebene Daten ein Passwort sind, selbst dann, wenn es keine anderen Anzeichen dafür gibt. Das Passwort wird zwar als eine Folge von Sternchen angezeigt, aber die Repräsentation im Speicher enthält weiter die Zeicheninformationen, die vom Benutzer eingegeben wurden. Das Passwort kann einfach durch Extrahieren der Eingabe aus dem Feld ent-

nommen werden.

[0113] Alternativ können Passwörter und Benutzernamen durch Verweis auf die identifiziert werden, die von anderen Programmen wie dem ‚Internet Explorer' von Microsoft gespeichert werden, wenn der Benutzer die Passwort-merken-Option gewählt hat. Solche Passwörter werden in einer lokalen geschützten Datei auf dem Computer des Benutzers gespeichert. Diese Datei wird dann ‚entsperrt', wenn sich der Benutzer auf dem Computer authentifiziert hat, und so kann vom Browser-Einsteckmodul des bevorzugten Systems zum Erhalten von Passwort- und Benutzernamensinformationen darauf zugegriffen werden.

[0114] Wenn das Einsteckmodul in den zu übertragenden Daten kein(en) Benutzernamen oder Passwort erfasst, dann geht die Steuerung zu Schritt S158, und an diesem Punkt verlässt das Modul die Routine und die Steuerung geht zurück zu Punkt ‚C' in Fig. 3. Der Browser kann dann die Daten zum Webserver senden. Wenn jedoch das Einsteckmodul in Schritt S152 ein(en) Benutzername oder Passwort erkennt, dann geht die Steuerung zu Schritt S154, wo die Werte des identifizierten Benutzernamens oder Passworts und die URL-Adresse oder eine andere Kennung der Webseite, zu der die Daten gesendet werden sollen, extrahiert werden. Die Steuerung geht dann zu Schritt S156, wo diese Werte und die URL-Adresse oder eine andere Kennung in einer vorbestimmten Systemdatenbank **42** gespeichert werden. Nach dem Speichern geht die Steuerung zu Schritt S158, wo das Modul die Routine verlässt und die Steuerung zurück zu Punkt ‚C' in Fig. 3 geht. Der Browser kann dann die Daten zum Webserver übertragen.

[0115] Die bevorzugte Ausgestaltung braucht nicht nur auf die Speicherung von Passwörtern oder Benutzernamen begrenzt zu sein, die aufgrund des sofortigen Vorteils, den ihre Speicherung bietet, als Beispiel benutzt wurden. Andere Datentypen, besonders solche in Bezug auf eCommerce-Transaktionen, z. B. Kreditkarteninformationen und digitale Zertifikate, können ebenfalls zum Erstellen einer Datenbank oder eines Datensatzes nutzbringend extrahiert und gespeichert werden. Das System zum Extrahieren von Informationen von Übertragungen kann auch auf Email-Systeme angewendet werden.

[0116] Die Informationen können auf die oben beschriebene Weise über das DOM oder über MAPI-Anrufe zur COM-Darstellung von Email-Inhalt extrahiert werden, oder sie können aus der Sprache extrahiert werden, in der eine Webseite codiert ist. Webseiten werden typischerweise in HTML (Hyper Text Markup Language) codiert, einer für den Menschen lesbaren textgestützten Sprache, die mittels konventioneller Textvergleichstechniken nach bekannten Schlüsselwörtern oder Indikatoren durchsucht werden können. In der bevorzugten Ausgestaltung kann das Aufzeichnen der Daten das Aufzeichnen nur von Passwort- und Benutzernamensinformationen, das Aufzeichnen der URL-Adresse einer betrachteten Webseite oder eines Email-Kontos, das Aufzeichnen beliebiger Daten, die zu den Feldern einer Webseite gesendet werden, und das Aufzeichnen der HTML einer Webseite beinhalten, so dass die Webseite später abgerufen und betrachtet werden kann.

[0117] Die in dem bevorzugten System enthaltenen Einsteckmodule arbeiten in Verbindung mit Richtliniendaten, die z. B. in einer Datei, einer Datenbank oder in Softwarecode aufgezeichnet werden können. Die Richtliniendaten geben einem Benutzer des bevorzugten Systems die Möglichkeit zum Befehlen des Betriebs jedes der Einsteckmodule, um dadurch deren Funktionalität zu steuern.

[0118] Eine beispielhafte Darstellung von Richtliniendaten, in Fig. 7 illustriert, zeigt, wie ein Benutzer den Betrieb des Einsteckmoduls zum Aufzeichnen von Passwort- und Benutzernamensinformationen zusammen mit anderen Datentypen steuern kann.

[0119] Die baumähnliche Struktur der Richtliniendaten ist deutlich in Fig. 7 zu sehen, die nur einen Hauptzweig der Richtliniendaten mit dem Titel ‚Recording' zeigt. Der Recording-Zweig ist in zwei Nebenzweige jeweils mit den Namen ‚Browser' und ‚Email' unterteilt, die Befehle für den Betrieb der Einsteckmodule Webbrowser bzw. Email-Client enthalten.

[0120] Der Browser-Zweig hat drei Nebenzweige mit den Bezeichnungen ‚DataToRecord', ‚WhenToStartRecording' und ‚WhenToStopRecording'. Der DataToRecord-Zweig gibt den Datentyp vor, der aus Übertragungen zu und von der Benutzerworkstation und einem Webserver extrahiert werden sollen. Es werden in der Illustration vier Datentypen genannt, nämlich die URL-Adresse der betrachteten Webseite, die HTML der betrachteten Webseite, die von einem Benutzer in Felder auf der Webseite eingegebenen Daten, die einer Website submittiert werden, und eventuelle vom Benutzer eingegebene Passwörter und Benutzernamen. Diese werden in vier getrennten Nebenzweigen des DataToRecord-Zweigs mit den Bezeichnungen ‚URL', ‚HTML', SubmittedFields' und ‚Passwords' genannt. Eine Ja/Nein-Option an jedem dieser Nebenzweige gibt an, ob die angezeigten Daten aufgezeichnet werden sollen oder nicht.

[0121] Der WhenToStartRecording-Zweig enthält eine Reihe von Bedingungen, die den Punkt angeben, an dem die im DataToRecord-Zweig vorgegebenen Daten aufgezeichnet werden sollen. In diesem Beispiel sind fünf Bedingungen illustriert, die jeweils auf einem anderen Zweig liegen, die jeweils mit

‚WhenBrowserIsOpened', ‚IfCreditCardNumberSubmitted', ‚IfPasswordSubmitted', ‚IfKeywordsReceived' und ‚IfKeywordsSent' bezeichnet sind. Ob diese Bedingungen benutzt werden sollen, um zu ermitteln, wann die Aufzeichnung beginnt, wird durch einen Ja/Nein-Marker auf jedem Zweig angezeigt.

[0122] Ebenso führt der WhenToStopRecording-Zweig drei Bedingungen auf, die zum Ermitteln des Punkts verwendet werden können, an dem die Aufzeichnung der im DataToRecord-Zweig vorgegebenen Daten gestoppt werden soll. Diese Bedingungen sind ‚WhenUserClosesBrowser', ‚WhenUserChangesSite' und ‚WhenUserChangesPage'. Der Ja/Nein-Status jeder der Bedingungen und für jeden aufzuzeichnenden Datentyp können leicht von einem Benutzer des bevorzugten Systems eingerichtet werden, um den Betrieb des Einsteckmoduls zu steuern.

[0123] Der Email-Zweig der Richtliniendaten ist in einen DataToRecord-Zweig und einen WhenToRecord-Zweig unterteilt. Jeder dieser Zweige ist in Zweige unterteilt, die sich mit gesendeter Mail und empfangener Mail befassen. Der Datentyp, der aufgezeichnet werden kann, ist im DataToRecord-Zweig angegeben und kann für gesendete Mail der Nachrichtentext, eventuelle Anhänge an die Nachricht und im Falle von mit einer digitalen Signatur signierten Nachrichten eine Kopie des die Signatur begleitenden digitalen Zertifikats sein. Bedingungen zum Aufzeichnen von gesendeten Mails und empfangenen Mails sind im WhenToRecord-Zweig dargelegt und können auf der Identifikation einer Kreditkartennummer, eines Schlüsselworts oder eines digitalen Zertifikats in der Mail basieren, die gesendet oder empfangen wird.

[0124] Die beschriebene baumähnliche Struktur ist die bevorzugte Form für die Richtliniendaten, da es mit ihr einfach ist, die Daten zu organisieren und darauf zu verweisen. Sie erlaubt es auch, verschiedene Benutzer unterschiedlichen Zweigen des Baums zuzuweisen, um verschiedene Richtlinien zu empfangen. Die baumähnliche Struktur wird zwar bevorzugt, aber es können auch andere Anordnungen möglich sein. Die in diesem Diagramm gezeigten Zweige sollen lediglich illustrativ sein.

Identifikation von Kreditkartennummern

[0125] Das bevorzugte System sucht auch nach Kreditkartennummern oder anderen Kontoinformationen in den zum Webserver oder Email-Client zu übertragenden Daten, indem es nach einer Folge von numerischen Ziffern sucht, typischerweise mit einer Länge zwischen 14 und 16. Es ermittelt dann, ob diese Ziffernfolge einen der Tests besteht, die universell von Kreditkartenunternehmen zum Validieren von Kreditkartennummern benutzt wird. Wenn eine Kreditkartennummer in der Übertragung gefunden wird, kann das bevorzugte System eine Reihe von Aktionen je nach den Einstellungen in der Richtliniendatei ausführen, wie z. B. überweisen der übertragung zu einer Drittpartei zur Billigung, Renegoziieren eines höheren Verschlüsselungsniveaus zum Sichern der Übertragung, wenn die Kreditkartennummer einem Unternehmen gehört, oder Verhindern, dass die Übertragung überhaupt stattfindet.

[0126] Der üblichste Test zum Identifizieren einer Kreditkartennummer ist im ANSI-Standard X4.13 definiert und ist üblicherweise als LUHN oder Mod 10 bekannt.

[0127] Die Luhn-Formel wird auf Kreditkartennummern angewendet, um eine Prüfziffer zu erzeugen, und kann somit zum Validieren von Kreditkarten benutzt werden, in diesem Fall wird die Prüfziffer als Teil der Formel einbezogen. Zum Validieren einer Kreditkartennummer mit der Luhn-Formel wird der Wert jeder zweiten Ziffer nach der ersten, beginnend von der rechten Seite der Nummer und nach links gehend, mit zwei multipliziert; alle Ziffern, sowohl die, die mit zwei multipliziert wurden, als auch die, die es nicht wurden, werden miteinander addiert; Ziffernwerte, die infolge der Verdopplung gleich oder größer als zehn werden, werden summiert, als wären sie zwei einstellige Werte, z. B.: ‚10' zählt als ‚1+0 = 1', ‚18' zählt als ‚1+8 = 9'. Wenn die Gesamtsumme durch zehn dividierbar ist, dann ist die Kreditkarte eine gültige Kreditkartennummer.

[0128] Fig. 8 ist ein Fließschema, das den Betrieb eines Einsteckmoduls illustriert, das Kreditkartennummern mit der oben beschriebenen Luhn-Formel in vor der Übertragung stehenden Daten erkennt. Wenn eine Kreditkartennummer identifiziert wird, dann führt das Einsteckmodul weitere richtliniengestützte Checks aus, und auf der Basis von deren Ergebnis kann das Einsteckmodul entscheiden, ob die die Kreditkartennummer enthaltenen Daten übertragen werden sollen oder ob eine Übertragung verhindert werden soll.

[0129] Das Modul beginnt mit dem Betrieb in Schritt S160, der auf Punkt ‚C' in dem in Fig. 3 illustrierten Vorgang im Falle einer Browser-Implementation folgt, oder auf Punkt B in dem in Fig. 5 illustrierten Vorgang im Falle einer Email-Client-Implementation. Die Steuerung geht von Schritt S160 zu Schritt S162, in dem das Modul die unmittelbar vor dem Senden zum Webserver oder Email-Server stehenden Daten absucht und daraus eine erste Folge von Stellen extrahiert, die wahrscheinlich eine Kreditkartennummer sind.

[0130] Dies wird durch Scannen der Daten erzielt, die die Übertragung von Ziffernfolgen über eine bestimmte Stellenlänge vergleicht. Kreditkartennummern bestehen gewöhnlich aus mehr als 12 Ziffern

und nicht mehr als 16 Ziffern. So kann jede Ziffernfolge in diesem Bereich als mögliche Kreditkartennummern identifiziert werden.

[0131] Nach dem Extraktionsschritt S162 geht die Steuerung zum Entscheidungsschritt S164, wo ein routinemäßiger Dateiende-Check ausgeführt wird. Wenn die Daten keinen Kreditkartennummernkandidaten enthalten und der Dateiende-Check erreicht wird, bevor ein erster Nummernkandidat gefunden wird, dann geht die Steuerung in Schritt S164 weiter zu Schritt S178, wo die Übertragung der Daten zugelassen wird, ohne dass weitere Checks erfolgen. Das Modul endet dann in Schritt S180. Die Steuerung nimmt dann den in Fig. 3 gezeigten Webbrowser-Betrieb ab Punkt ‚C' oder den in Fig. 5 gezeigten Email-Client-Betrieb ab Punkt B wieder auf.

[0132] Wenn eine erste potentielle Kreditkartennummer in den Daten in Schritt S162 gefunden wird, dann wird sie extrahiert und im Speicher gespeichert. Das Dateiende ist noch nicht erreicht, daher geht die Steuerung von Schritt S162 zu Schritt S164 und dann zu Schritt S166, wo eine Prüfsumme für die gespeicherte Kandidatennummer mit der Luhn-Formel berechnet wird. Die Steuerung geht dann zum Entscheidungsschritt S168, wo die Prüfsumme abgefragt wird.

[0133] Wenn die Prüfsumme anzeigt, dass die Kandidatennummer keine gültige Kreditkartennummer ist, dann geht die Steuerung zurück zu Schritt S162, wo die nächste potentielle Kreditkartennummer aus den Daten extrahiert wird. Wenn keine zweite Kreditkartennummer gefunden wird, dann wird das Ende der Datei erreicht und die Steuerung geht zu Schritt S178, wo die Übertragung stattfindet, und dann zu Schritt S180, wo das Modul die Routine verlässt.

[0134] Wenn die Prüfsumme jedoch anzeigt, dass die Kandidatennummer eine gültige Kreditkartennummer ist, dann geht die Steuerung zum Entscheidungsschritt S170, wo die Einstellungen der Richtliniendaten nach der richtigen durchzuführenden Aktion abgefragt werden. Die Aktion kann anhand von Faktoren wie die Nummer selbst, die Identität des die Nummer übertragenden Benutzers und die Adresse bestimmt werden, zu der sie gesendet werden soll. Die Richtliniendaten könnten beispielsweise vorgeben, dass Kreditkartennummern nicht zu übertragen sind oder dass eine höhere Verschlüsselungsstärke erforderlich ist, bevor die Übertragung erfolgen kann.

[0135] Mit diesem Richtlinienprüfschritt können Kreditkartentransaktionen auf einem höheren Level als dem des die Transaktion vornehmenden Benutzers gesteuert werden. So können finanzielle Entscheidungen schnell und leicht implementiert und automatisch ohne Notwendigkeit für Überwachung durchgesetzt werden. Eine Organisation möchte z. B. möglicherweise den Zugang zur Durchführung von Kredittransaktionen auf dem Konto der Organisation auf bestimmte autorisierte Personen oder Transaktionen für ein bestimmtes Konto insgesamt beschränken.

[0136] In Schritt S170 werden die Kreditkartennummer und andere Details der Transaktion mit den Einstellungen in der Richtliniendatei verglichen und es wird entschieden, ob eine Übertragung stattfinden kann oder nicht. Wenn bei den Richtlinienprüfungen aus irgendeinem Grund bestimmt wird, dass die Kreditkartennummer nicht übertragen werden soll, dann geht die Steuerung zu Schritt S172, wo die Übertragung der Daten unterbrochen wird, und dann zu Schritt S174, wo das Modul die Routine verlässt. Hier könnte das System dem Benutzer die Tatsache, dass die Anforderung abgelehnt wurde, durch eine Popup-Nachrichtenbox mitteilen. Die Steuerung kehrt dann bei einem Webbrowser zu Punkt A in Fig. 3 oder, bei einem Email-Client, zu Schritt S132 ‚Mail verfassen' in Fig. 5 zurück.

[0137] Wenn in Schritt S172 ermittelt wird, dass die Kreditkartennummer übertragen werden kann, dann geht die Steuerung zu Schritt S176, wo die Daten übertragen werden, und dann zu Schritt S180, wo das Modul die Routine verlässt. In diesem Fall wird die Steuerung ab Punkt C in dem in Fig. 3 illustrierten Webbrowser-Betrieb oder ab Punkt B in dem in Fig. 5 illustrierten Email-Client-Betrieb wieder aufgenommen.

[0138] Kreditkartennummern brauchen in Schritt S162 nicht nur durch Scannen des Inhalts der Übertragung identifizert zu werden. In Webbrowser-Implementationen kann die Kreditkartennummer beispielsweise direkt mit Bezug auf die Feldnamen von Variablen identifiziert werden, die übertragen werden sollen, oder auch von der Darstellung der Webseite im Speicher. Die obige Diskussion über die Identifikation von Passwörtern erläutert dies näher.

[0139] Das bevorzugte System kann auch so konfiguriert werden, dass es nach abgehenden Übertragungen für andere relevante Finanzdetails wie z. B. Kontonummern sucht. Firmenkontonummern, von denen Fonds deponiert werden können, können in einer separaten Datei gespeichert werden. Eventuelle wahrscheinliche Zeichen- oder Ziffernfolgen können dann aus den abgehenden Daten in der beschriebenen Weise extrahiert und mit den Einträgen in der Kontendatei verglichen werden, um zu ermitteln, ob die Kontonummer gültig ist oder nicht. Die Transaktion kann dann wie oben beschrieben zugelassen oder verweigert werden. Es wurde zwar auf Kreditkartennummern Bezug genommen, aber man wird verstehen, dass auch jeder andere Kartennummerntyp wie z. B. Debitkartennummern für Zahlungen verwendet werden kann.

[0140] Es wurde zwar auch die Identifikation von Kreditkartennummern mit Bezug auf Daten erläutert, die übertragen werden sollen, aber man wird verstehen, dass ähnliche Techniken auch zum Identifizieren und Extrahieren von Kreditkartennummern von Übertragungen verwendet werden können, die empfangen werden.

Validierungs- und Authentifizierungsunterstützung

[0141] Online-Transaktionen erfordern typischerweise eine Form von Authentifizierung, ob der Benutzer der ist, für den er sich ausgibt, und ob er in der Lage ist, für die bestellten Waren zu bezahlen. Diese Anforderungen werden gewöhnlich vom Käufer dadurch erfüllt, dass er dem Händler seine Kreditkartennummer und die Karteninhaberadresse angibt, die dann vom Verkäufer beim Kartenausgeber verifiziert werden. Es werden jedoch in zunehmendem Maße digitale Zertifikate vom Benutzer an elektronische Übertragungen angehängt, die es dem Empfänger in Verbindung mit einer digitalen Signatur gestatten zu prüfen, ob die Übertragung von der als Sender genannten Person stammt. Digitale Zertifikate von bestimmten Ausgabestellen wie z. B. Identrus können auch als Gewährleistung dienen, dass der Halter seiner Verpflichtung zur Zahlung eines bestimmten Geldbetrags nachkommen wird. Diese Zertifikate sind bei Online-Handelsgeschäften nützlich.

[0142] Digitale Signaturen sind ein weithin benutztes Mittel, um die Identität einer Person online festzustellen, wenn Informationen übertragen oder Transaktionen durchgeführt werden. Sie sind auch eine Garantie für den Empfänger von übertragenen Informationen oder Transaktionsdetails, dass diese Details und diese Informationen nicht von einer unbefugten Drittpartei auf der Strecke missbraucht werden.

[0143] Digitale Zertifikate werden an Personen, Organisationen oder Unternehmen von unabhängigen Zertifikatbehörden wie z. B. Verisign Inc. ausgegeben. Eine Organisation kann auch als ihre eigene Zertifikatbehörde fungieren, die ihre eigenen digitalen Zertifikate ausgibt, die von einem von einer anderen Zertifikatbehörde ausgegebenen ‚Root'-Zertifikat abgeleitet sein können oder auch nicht. Ein digitales Zertifikat enthält typischerweise den Namen des Inhabers, eine Seriennummer, ein Ablaufdatum, eine Kopie des Public-Key des Zertifikatinhabers und die digitale Signatur der Zertifikatausgabestelle. Auch ein Private-Key wird an den Zertifikatinhaber ausgegeben, der diesen an niemand anders weitergeben sollte.

[0144] Zertifikate sind für jeden Halter eindeutig und können von einem Ausgeber widerrufen werden, wenn der Halter nicht mehr gültig ist; ein Halter kann auch um einen Widerruf bitten, wenn sein Private-Key kompromittiert wurde.

[0145] Die Public- und Private-Keys können nicht zusammen zum Ver- oder Entschlüsseln einer Nachricht benutzt werden. Jedermann kann den Public-Key eines Zertifikatinhabers zum Verschlüsseln einer Nachricht benutzen, so dass sie nur vom Zertifikatinhaber nach dem Entschlüsseln der Nachricht mit seinem Private-Key gelesen werden kann.

[0146] Nachrichten können auch digital mit Software signiert werden, die den Inhalt der Nachricht in eine Hash genannte mathematische Zusammensetzung umwandelt. Der Hash wird dann mit dem Private-Key des Senders verschlüsselt. Der verschlüsselte Hash kann dann als digitale Signatur für die Nachricht verwendet werden, die übertragen wird. Die ursprüngliche Nachricht, die digitale Signatur und das digitale Zertifikat des Senders werden alle zu einem Empfänger gesendet, der zum Bestätigen, dass die von ihm empfangene Nachricht komplett und gegenüber ihrer ursprünglichen Form unverändert ist, dann einen Hash für die empfangene Nachricht erzeugen kann. Wenn der empfangene Hash nach dem Entschlüsseln mit dem Public-Key des Inhabers mit dem vom Empfänger produzierten Hash übereinstimmt, dann kann der Empfänger sicher sein, dass die Nachricht von der Person gesendet wurde, an die das Zertifikat ausgegeben wurde, und dass die Nachricht nicht auf der Strecke gegenüber ihrer ursprünglichen Form verändert wurde. Digitale Zertifikate sind daher von erheblicher und zunehmender Bedeutung für Firmen, die Geschäfte auf dem Internet tätigen.

[0147] In Fällen, bei denen ein Online-Händler digitale Zertifikate zum Gewährleisten der Identität seiner Kunden nutzt, muss beim Ausgeber geprüft werden, ob das Zertifikat weiterhin gültig ist, bevor eine Transaktion autorisiert wird. Solche Checks können online mit einem unabhängigen Verifikationsdienst wie z. B. dem von Valicert, Inc. angebotenen ausgeführt werden. Für solche Dienste wird gewöhnlich eine Gebühr erhoben.

[0148] Es kann vorkommen, dass individuelle Mitarbeiter einer Organisation jeweils Emails von einem einzigen Client, jeweils mit dessen digitalem Zertifikat signiert, zu separaten Zeitpunkten erhalten. Derzeit gibt es keine Möglichkeit, wie eine Information über Zertifikate, die von einem Mitarbeiter empfangen wurden, mit einem anderen Mitarbeiter gemeinsam genutzt werden kann, es sei denn, dass sie diese manuell untereinander austauschen, und infolgedessen könnten einzelne Mitarbeiter anfordern, dass dasselbe Zertifikat jedes Mal validiert wird, wenn sie es erhalten. Dies ist jedoch verschwenderisch, da ein Zertifikat, das von seinem Ausgeber widerrufen wird, nie wieder reaktiviert wird, so dass Validierungsgebühren, die bereits für einen Widerruf des Zertifikats ausgegeben wurden, unnötig sind. Zusätzlich möchte

der Empfänger möglicherweise ein geschäftliches Urteil darüber fällen, ob ein zuvor validiertes Zertifikat erneut geprüft werden soll oder nicht. Wenn beispielsweise an einem Tag ein digital signierter Auftrag im Wert von einer Million Dollar für Waren empfangen wird und das Zertifikat erfolgreich validiert wurde, und am nächsten Tag ein anderer Auftrag für $50 eingeht, mit demselben Zertifikat signiert, dann kann die Organisation einen zweiten Validierungscheck als unnötig ansehen und spart dadurch die Validierungsgebühr.

[0149] Das bevorzugte System stellt Mittel zum Aufzeichnen von Informationen über die empfangenen digitalen Zertifikate, den Status des Zertifikats beim letzten Check sowie, wo zutreffend, Transaktionsinformationen wie Client, Betrag, Datum, Waren usw. bereit. Diese Informationen werden in einer zentralen Datenbank gespeichert, zu der alle Benutzer des Systems Zugang haben. Das bevorzugte System stellt auch Mittel zum Benutzen der gespeicherten Informationen bereit, um zu entscheiden, ob ein Validierungscheck wünschenswert ist oder nicht, und um Übertragungen je nach dem Status des digitalen Zertifikats zu akzeptieren oder abzulehnen. So können Benutzer des Systems Übertragungen empfangen und überprüfen, ohne ihre Authentizität selbst feststellen zu müssen.

[0150] Fig. 9 illustriert den Betrieb eines Einsteckmoduls des bevorzugten Systems, das implementiert wird, um digitale Zertifikate von Übertragungen zu extrahieren, die von Unternehmensmitarbeitern empfangen wurden, und um sie in einer Datenbank zusammen mit ihrem Validitätsstatus und mit Einzelheiten über eventuelle assoziierte Transaktionen aufzuzeichnen, wie z. B. Datum, Betrag, Waren usw. Das Modul prüft zunächst, ob das Zertifikat offensichtlich ungültig ist und ob die Nachricht damit korrekt signiert wurde. Das Zertifikat ist z. B. dann offensichtlich ungültig, wenn sein Ablaufdatum überschritten wurde oder wenn es einen ungültigen ‚Fingerabdruck' enthält. Ein solcher Fingerabdruck kann beispielsweise eine Prüfsumme für das Zertifikat selbst sein. Die Nachricht wurde nicht korrekt signiert, wenn die Signatur nicht anhand der im Zertifikat enthaltenen Informationen überprüft werden kann. Einzelheiten über die Zertifikatvalidierung und die Nachrichtensignierung sind in den oben erwähnten ITU- und RFC-Dokumenten ausführlicher beschrieben. Das Modul prüft dann, ob das Zertifikat bereits in der Datenbank gespeichert ist oder nicht, und zeichnet nur diejenigen auf, die es nicht sind. Wo bereits eine Kopie des Zertifikats gespeichert ist, da prüft das Modul den Datenbankeintrag, um zu ermitteln, ob er bereits zuvor als widerrufen identifiziert ist, und in diesem Fall wird die Übertragung sofort abgelehnt. Ansonsten ermittelt das Modul gemäß Geschäftsregeln definierenden Richtlinien, ob das Zertifikat validiert werden soll oder nicht. Je nach den Ergebnissen einer solchen Validierung prüft es dann, ob das Zertifikat verlässlich ist und daher, ob die von dem digitalen Zertifikat signierte Übertragung abgelehnt oder akzeptiert werden soll. Das Modul wird in Schritt S190 gestartet, im Anschluss an den Empfang von Daten, die ein digitales Zertifikat enthalten. Digitale Zertifikate werden typischerweise als Anhänge an Nachrichten übertragen und können durch Untersuchen der ersten paar Bytes im Kopf des Anhangs identifiziert werden. Diese Bytes identifizieren den Typ der angehängten Datei und geben auch an, ob ein Anhang ein digitales Zertifikat ist oder nicht.

[0151] Der Startschritt S190 erfolgt nach Punkt A in Fig. 3, wenn das Modul in einem Webbrowser implementiert wird, und nach Punkt A in Fig. 5, wenn das Modul in einem Email-Client implementiert wird. Nach dem Start geht das Modul weiter zu Schritt S191, wo das Ablaufdatum des Zertifikats geprüft und die Signierung der Nachricht durch die digitale Signatur bestätigt wird. Wenn das Zertifikat abgelaufen ist oder wenn die Nachricht inkorrekt signiert wurde, dann geht das Modul weiter zu Schritt 198 und lehnt die Übertragung ab. Ansonsten geht das Modul zu Schritt S192, wo die Datenbank nach einer zuvor empfangenen Kopie des digitalen Zertifikats abgesucht wird. Die Steuerung geht dann zum Entscheidungsschritt S194. Wenn eine Kopie des Zertifikats in der Datenbank gefunden wird, dann geht die Steuerung weiter zum Entscheidungsschritt S196, wo das Modul ermittelt, ob das Zertifikat zuvor als widerrufen markiert wurde. Dies ist dann aufgetreten, wenn ein früherer Validitätscheck zu Tage gebracht hat, dass ein digitales Zertifikat widerrufen wurde. Wenn das Zertifikat nicht bereits in der Datenbank ist, dann geht die Steuerung von Schritt S194 zu Schritt S202, wo das neue Zertifikat und das Datum, an dem es empfangen wurde, zusammen mit zusätzlichen Details wie die Adresse, von der es gesendet wurde, und Details von eventuellen Transaktionen in Verbindung mit der Übertragung in der Datenbank gespeichert werden, wie z. B. ein Geldwert, die Kontonummer usw. Wenn das Zertifikat in Schritt S196 bereits als widerrufen markiert wurde, geht die Steuerung direkt zu Schritt S198, wo die das digitale Zertifikat umfassende Übertragung automatisch abgelehnt wird. Dies kann beispielsweise das Senden einer automatisch erzeugten Meldung zum Initiator der Übertragung beinhalten, dessen Zertifikat als ungültig gefunden wurde, um die Ablehnung zu erläutern und um zu verhindern, dass der Empfänger des digitalen Zertifikats weitere Schritte in Verbindung mit der abgelehnten Übertragung unternimmt. Das Modul verlässt dann die Routine in Schritt S200.

[0152] Wenn das Zertifikat jedoch nicht zuvor in Schritt S196 als widerrufen markiert wurde, dann geht die Steuerung zu Schritt S204, wo die Historie von Übertragungen, die durch das Zertifikat oder durch andere Zertifikate von demselben Unterneh-

men signiert oder zum Ausführen von Transaktionen auf demselben Konto verwendet wurden, mit Richtliniendaten verglichen werden, um zu ermitteln, ob ein Online-Validitätscheck des Zertifikats erforderlich ist. Die Steuerung geht auch zu Schritt S204, nachdem ein neues digitales Zertifikat zur Datenbank in Schritt S202 hinzugefügt wurde.

[0153] Die Richtliniendaten enthalten Befehle, die in Verbindung mit der Historie von zuvor empfangenen signierten Übertragungen und zuvor durchgeführten Widerrufchecks betrachtet anzeigen, ob das zum Signieren einer Übertragung benutzte Zertifikat bei dieser Gelegenheit geprüft werden soll oder nicht. Beispielhafte Richtliniendaten sind in Fig. 10 illustriert, auf die nun Bezug genommen werden sollte.

[0154] Die Richtliniendaten sind auf dem Zweig AcceptanceConfidenceRating auf dem DigitalCertificates-Zweig der Richtliniendatendarstellung gespeichert. Der AcceptanceConfidenceRating-Zweig ist in zwei separate Zweige unterteilt, die sich individuell mit ‚monetären' digitalen Zertifikaten befassen, wo ein Zertifikat zum Signieren einer Übertragung benutzt wird, die eine Transaktion mit dem Empfänger für einen Geldbetrag beinhaltet, und digitalen ‚Identitäts'-Zertifikaten, die keine monetäre Transaktion mit dem Empfänger der Übertragung beinhalten. Bestimmte Zertifikate werden nur für die Verwendung in Verbindung mit monetären Transaktionen ausgegeben, zum Beispiel das von einigen Online-Bankorganisationen wie Identrus ausgegebene ‚Warranty Certificate', das als eine Gewährleistung für den Empfänger der signierten Übertragung ausgegeben wird. Solche Gewährleistungszertifikate bezeugen, dass der Sender der Übertragung Kunde einer Identrus-Mitgliedsbank ist und dass die Bank die Haftung für eventuell von ihm nicht geleistete Zahlungen übernimmt.

[0155] Organisationen, die unterschiedliche Arten oder Klassen von digitalen Zertifikaten ausgeben, markieren jedes Zertifikat je nach seiner Klasse. Das Identifizieren eines Zertifikats als zu einer bestimmten Klasse gehörig ist dann eine Sache des Wissens, wie verschiedene Organisationen ihre Zertifikate klassifizieren, und des Suchens nach dem entsprechenden Indikator in dem empfangenen Zertifikat.

[0156] Aussteller von digitalen Zertifikaten können viele verschiedene, für verschiedene Zwecke geeignete Zertifikatklassen bereitstellen. Mit diesen können sich Richtliniendaten separat nach entsprechenden Unterzweigen des Richtliniendatenbaums befassen.

[0157] In dem Beispiel befasst sich die Richtlinie des ersten Zweigs namens ‚IdentityCertificates' mit Übertragungen, die keine monetäre Transaktion involvieren. Der Zweig umfasst vier separate Unterzweige. Der erste davon, ‚AlwaysAcceptFrom', enthält einen Verweis auf eine Tabelle, ‚Tabelle a', die die Namen von Personen und Organisationen aufführt, die als zuverlässig angesehen werden. Die in dieser Tabelle aufgeführten Namen sind diejenigen, die dem Unternehmen bekannt sind und denen das Unternehmen ausdrücklich vertraut, für die es nicht als notwendig erachtet wird zu ermitteln, ob ein digitales Zertifikat von seinem Aussteller widerrufen wurde oder nicht.

[0158] Der zweite Zweig, ‚AlwaysCheckFrom', enthält einen Verweis auf eine separate Tabelle, Tabelle b, in der die Namen von Organisationen und Personen gespeichert sind, für die digitale Zertifikate immer geprüft werden sollen. Der Inhalt von Tabelle a und Tabelle b hängt natürlich immer von der Erfahrung des Benutzers des bevorzugten Systems ab und es liegt am Benutzer, sie auszufüllen.

[0159] Der dritte Zweig, ‚CheckIfDaysSince CertificateReceivedFromCompany', gibt eine Zeitperiode nach dem Empfang eines gültigen digitalen Zertifikats von einem Unternehmen vor, innerhalb derer Checks weiterer von diesem Unternehmen empfangener digitaler Zertifikate nicht als notwendig erachtet werden. In diesem Fall ist die Zeitperiode auf 10 Tage eingestellt.

[0160] Der vierte Zweig, ‚CheckIfDaysSince LastReceivedThisCertificate', gibt eine ähnliche Zeitperiode im Falle eines individuellen digitalen Zertifikats vor. In dem gezeigten Beispiel geben die Richtliniendaten vor, dass Validierungschecks an einem gegebenen digitalen Zertifikat nur alle 30 Tage vorgenommen zu werden brauchen. Auch hier liegt es wieder am Benutzer des bevorzugten Systems, die Anzahl der Tage zu entscheiden, die auf beiden diesen Zweigen vorgegeben werden. Die Zeitmenge, die seit dem Empfang eines gültigen digitalen Zertifikats verstrichen ist, kann durch Bezugnahme auf digitale Zertifikate und assoziierte Daten bestimmt werden, die in der Datenbank gespeichert sind.

[0161] Indem digitale Zertifikate periodisch und nicht bei jedem Empfang geprüft werden, kann für die Durchführung von Checks ausgegebenes Geld eingespart werden.

[0162] Der MonetaryCertificate-Zweig enthält auch einen AlwaysAcceptFrom- und einen AlwaysCheckFrom-Zweig, die jeweils auf Tabelle x und y verweisen. Tabelle x führt alle Organisationen und Personen auf, für die kein Statuscheck eines digitalen Zertifikats erforderlich ist; Tabelle y führt alle die auf, für die ein Check immer erforderlich ist. Der MonetaryCertificate-Zweig enthält auch einen CheckIfAmountExceeds-Zweig, der einen Transaktionsschwellenbetrag vorgibt, jenseits dessen alle digitalen Zertifikate geprüft werden müssen, und schließlich einen

IfRecentlyChecked-Zweig, der zwei Bedingungen zum Ausführen von Checks an einem digitalen Zertifikat darlegt, das kürzlich empfangen und validiert wurde. Der IfRecentlyChecked-Zweig gestattet es dem Benutzer vorzugeben, dass für Transaktionen für einen geringen Betrag, in diesem Fall $5000, empfangene digitale Zertifikate, die innerhalb eines vorgegebenen Zeitraums, in diesem Fall 30 Tage, nach einem vorherigen Widerrufcheck, nicht validiert zu werden brauchen.

[0163] Fig. 11 illustriert den Einsteckmodulprozess, der mit den in Fig. 9 gezeigten Richtliniendaten interagiert. Dieser Prozess ist ein Subprozess des in Fig. 8 gezeigten, der in Schritt S204 abläuft und zum Entscheidungsschritt S206 führt, in dem das Einsteckmodul ermittelt, ob ein Online-Check des Status des empfangenen digitalen Zertifikats ausgeführt werden soll oder nicht. Der Subprozess beginnt in Schritt S220, von dem die Steuerung weiter zum Entscheidungsschritt S222 geht, in dem anhand der Klasse des zum Signieren der Nachricht verwendeten digitalen Zertifikats ermittelt wird, ob die Übertragung monetär ist. Wenn es sich um eine monetäre Übertragung handelt, dann geht die Steuerung zum Entscheidungsschritt S232, der der erste in einer Kette von Entscheidungsschritten ist, die den Zweigen im MonetaryCertificates-Zweig des AcceptanceConfidenceRating-Zweigs der Richtliniendaten entsprechen.

[0164] Wenn in Schritt S222 ermittelt wird, dass die Übertragung nicht monetär ist, dann geht die Steuerung zum Entscheidungsschritt 224, d. h. dem ersten Entscheidungsschritt in einer Kette von Entscheidungsschritten, die den IdentityCertificates-Zweigen des AcceptanceConfidenceRating-Zweigs der Richtliniendaten entsprechen. In jedem der Entscheidungsschritte in der Kette wird ein einfacher Check durchgeführt, um zu prüfen, ob die auf jedem Unterzweig des IdentityCertificates-Zweigs der Richtliniendaten vorgegebenen Bedingungen erfüllt sind. Je nach den Ergebnissen dieses Checks geht die Steuerung entweder zu Schritt 242, wo das Vertrauen in das digitale Zertifikat festgestellt und kein Online-Check des Status des digitalen Zertifikats als notwendig erachtet wird, oder zu Schritt S244, wo das Vertrauen nicht festgestellt wird und ein Online-Check als notwendig erachtet wird, oder zum nächsten Entscheidungscheck in der Kette.

[0165] So geht die Steuerung vom Entscheidungsschritt S224, wo ermittelt wird, ob der Sender des digitalen Zertifikats in Tabelle a aufgeführt ist, d. h. der ‚AlwaysAcceptFrom'-Tabelle, wenn der Sender des digitalen Zertifikats in Tabelle a aufgeführt ist, zu Schritt S242, wo das Vertrauen in das Zertifikat festgestellt wird, und der Subprozess endet mit der Rückkehr zu Schritt S208 in Fig. 8. Wenn der Sender in Tabelle a nicht aufgeführt ist, dann geht die Steuerung von Schritt S224 zum nächsten Entscheidungsschritt in der Kette, Schritt S226, in dem ermittelt wird, ob der Sender des digitalen Zertifikats in Tabelle b aufgeführt ist, d. h. in der ‚AlwaysCheckFrom'-Tabelle. Ebenso geht die Steuerung, wenn der Sender in dieser Tabelle aufgeführt ist, zu Schritt S244, wo ein Online-Check des Status des digitalen Zertifikats als notwendig erachtet wird. Die Steuerung kehrt von Schritt S244 im Subprozess zu Schritt S210 in Fig. 8 zurück.

[0166] Wenn der Sender des digitalen Zertifikats nicht in Tabelle b aufgeführt ist, dann geht die Steuerung vom Entscheidungsschritt S226 zum nächsten Entscheidungsschritt in der Kette weiter, der die nächste in den Richtliniendaten als Unterzweig aufgeführte Bedingung repräsentiert. So wird im Entscheidungsschritt S228 geprüft, ob dieses digitale Zertifikat in den letzten 30 Tagen validiert wurde. Dies beinhaltet das Nachschlagen des digitalen Zertifikats in der Datenbank von gespeicherten digitalen Zertifikaten und das Extrahieren des Datums aus den gespeicherten Informationen, an dem das digitale Zertifikat zuletzt geprüft wurde. Wenn der Status des digitalen Zertifikats in den letzten 30 Tagen geprüft wurde, dann geht die Steuerung zu Schritt S242, wo das Vertrauen festgestellt wird. Wenn die Informationen in der Datenbank von gespeicherten digitalen Zertifikaten anzeigen, dass das digitale Zertifikat in den letzten 30 Tagen nicht geprüft wurde, dann geht die Steuerung von Schritt S228 zum Entscheidungsschritt S230, wo geprüft wird, ob ein anderes digitales Zertifikat von demselben Unternehmen empfangen wurde und ob dieses digitale Zertifikat innerhalb der letzten 10 Tage geprüft wurde. Diese Ermittlung beinhaltet wiederum das Prüfen der Datenbank von gespeicherten digitalen Zertifikaten und von Informationen über diese digitalen Zertifikate. Wenn das andere digitale Zertifikat in den letzten 10 Tagen geprüft wurde, dann geht die Steuerung zu Schritt S242, wo das Vertrauen in das empfangene digitale Zertifikat festgestellt wird. Wenn nicht, dann geht die Steuerung zu Schritt S244.

[0167] Im Falle einer monetären Übertragung werden die in den Richtliniendaten dargelegten Bedingungen schrittweise in den Entscheidungsschritten S232 bis S240 durchlaufen. Wenn der Sender des digitalen Zertifikats im Entscheidungsschritt S232 nicht in Tabelle x gefunden wird, die die Namen von Unternehmen und Organisationen aufführt, für die keine Prüfung des Status des digitalen Zertifikats als notwendig erachtet wird, dann wird das Vertrauen festgestellt und die Steuerung geht zu Schritt S242. Ansonsten geht die Steuerung zum nächsten Entscheidungsschritt in der Kette, nämlich Entscheidungsschritt S234. Im Entscheidungsschritt S234 wird, wenn der Sender des digitalen Zertifikats nicht in Tabelle b, d. h. der ‚AlwaysCheckFrom'-Tabelle, gefunden wird, das Vertrauen nicht festgestellt und die

Steuerung geht zu Schritt S244. Ansonsten geht die Steuerung zum Entscheidungsschritt S236, wo ermittelt wird, ob der Betrag, für den die Transaktion durchgeführt wird, $10.000 übersteigt. Diese Ermittlung erfolgt mit Bezug auf die signierten Transaktionsdaten, die den Geldbetrag enthalten, entweder auf eine vom Aussteller des Zertifikats vorbestimmte Weise oder in der Email oder in assoziierten, die Transaktion bildenden Emails oder Übertragungen enthalten. Wenn gefunden wird, dass die Transaktion für einen Betrag von mehr als $10.000 ist, oder wenn der Betrag der Transaktion nicht anhand der übertragenen Daten festgestellt werden kann, dann wird das Vertrauen nicht festgestellt und die Steuerung geht zu Schritt S244.

[0168] Ansonsten geht die Steuerung zum Entscheidungsschritt S238, wo ermittelt wird, ob das digitale Zertifikate innerhalb der letzten 30 Tage geprüft wurde. Auch diese Ermittlung erfolgt wieder mit Bezug auf die Datenbank von gespeicherten digitalen Zertifikaten und Daten über digitale Zertifikate. Wenn das Zertifikat nicht innerhalb der letzten 30 Tage geprüft wurde, dann wird das Vertrauen nicht festgestellt und die Steuerung geht zu Schritt S244. Wenn es geprüft wurde, geht die Steuerung zum Entscheidungsschritt S240, wo, wenn der zuvor ermittelte Betrag der Transaktion als über $5000 liegend ermittelt wurde, das Vertrauen nicht festgestellt wird und die Steuerung zu Schritt S244 geht. Wenn der Betrag der Transaktion unter $5000 liegt, dann wird dies als ein akzeptables Risiko eingestuft, sich auf das digitale Zertifikat zu verlassen, das Vertrauen wird festgestellt und die Steuerung geht zu Schritt S242.

[0169] Diese beiden letzten Bedingungen erlauben es dem System, auf der Basis der kürzlichen Handelshistorie zu ermitteln, ob der Status des Zertifikats geprüft werden soll oder nicht. Wenn beispielsweise eine Transaktion von einer Partei für eine mäßige Summe durchgeführt werden soll, d. h. unter $5000, und die Suche nach der aufgezeichneten Transaktion und den Zertifikat-Details zu Tage bringt, dass vor relativ kurzer Zeit dieselbe Partei eine Transaktion durchgeführt hat und dabei ihr digitales Zertifikat als gültig festgestellt wurde, dann könnte man argumentieren, dass eine nochmalige Prüfung der Validität des Zertifikats der Partei so bald nach der ersten unnötig ist, und man wird bevorzugen, der Partei zu vertrauen, anstatt die Validierungsgebühr ein zweites Mal zu bezahlen.

[0170] Man wird verstehen, dass die Befehle in der Richtliniendatei so gestaltet werden können, dass sie das Vertrauensniveau reflektieren, das das Unternehmen in seine Kunden oder Lieferanten hat, auf der Basis der Erfahrungen von Personen innerhalb des Unternehmens, der Transaktionsbeträge, die ohne signifikantes Risiko als zulässig angesehen werden usw. Die Richtliniendatei kann auch zum Implementieren allgemeinerer Richtlinien eingerichtet werden, die in Verbindung mit einer Aufzeichnung von Transaktionsdetails für den Inhaber dieses digitalen Zertifikats verwendet werden sollen. So kann beispielsweise jede Transaktion, die vom Inhaber angeboten wird, mit dem Datensatz von den zuvor von ihm getätigten verglichen werden, um zu sehen, ob der Betrag und die bestellten Waren und Dienste mit seiner Handelshistorie im Einklang stehen. Wenn nicht, dann kann es wünschenswert sein, die Validität des Zertifikats zu prüfen, um zu bestätigen, dass es noch gültig ist und die Identität des Senders garantiert. Wenn es widerrufen wurde, dann hat sich möglicherweise eine Drittpartei den Private-Key des ursprünglichen Inhabers beschafft und versucht, betrügerische Transaktionen durchzuführen.

[0171] Nach dem Prüfen der Richtliniendaten in Schritt S204 wurde entweder das Vertrauen in das digitale Zertifikat festgestellt oder auch nicht. Im Entscheidungsschritt S206 geht die Steuerung, wenn das Vertrauen festgestellt wurde, zu Schritt S208, wo die die Transaktion enthaltende Übertragung akzeptiert wird. Die Steuerung geht dann zu Schritt S200, wo das Modul die Routine verlässt und die Steuerung zu Punkt A in Fig. 3 im Falle eines Webbrowsers oder zu Punkt A in Fig. 5 im Falle eines Email-Client geht.

[0172] Wenn in Schritt S206 das Vertrauen in das digitale Zertifikat nicht festgestellt wird, dann geht die Steuerung zu Schritt S210, wo ein Online-Validierungscheck an dem digitalen Zertifikat durchgeführt wird: Dies kann die Prüfung beinhalten, ob das digitale Zertifikat widerrufen wurde oder ob, im Falle einer eCommerce-Transaktion, der Ausgeber des digitalen Zertifikats eine Gewährleistung für den in der Transaktion versprochenen Betrag bestätigt. Die Steuerung geht als Nächstes weiter zu Schritt S212, wo der in der Datenbank für dieses Zertifikat gespeicherte Validitätsstatus auf den neuesten Standgebracht wird. Die Steuerung geht dann zum Entscheidungsschritt S214, wo die Steuerung, wenn das Zertifikat als ungültig gefunden wird, zu Schritt S198 geht, wo die Übertragung abgelehnt wird, oder zu Schritt S208, wo die Übertragung akzeptiert wird. Eine Ablehnung der Übertragung kann bedeuten, dass sie aus der Mailbox des Empfängers gelöscht wird, bevor sie geöffnet wird, oder dass die Übertragung mit dem Wort ‚abgelehnt' oder einem anderen Indikator markiert wird. Nach Schritt S198 oder S208 geht die Steuerung zu Schritt S200, wo das Modul die Routine verlässt. Wann immer eine Transaktion zugelassen wird, wird die Datenbank so aktualisiert, dass sie Informationen über die Transaktion wie z. B. Datum und Betrag enthält, damit die Informationen beim Ermitteln der Notwendigkeit für weitere Validierungschecks benutzt werden können.

Aufzeichnung von Informationen

[0173] Das bevorzugte System bietet auch einen Weg, um Transaktionsinformationen für online durchgeführte Transaktionen automatisch aufzuzeichnen. In diesem Zusammenhang sollen die Begriffe ‚Transaktion' und ‚eCommerce-Transaktion' eine Vereinbarung zwischen zwei Parteien über das Internet oder sogar über dasselbe Netzwerk eines Unternehmens bedeuten, in der Geld oder ein Geldwert versprochen wird. Normalerweise ist der Benutzer selbst zum Führen von Transaktionsinformationen verantwortlich, indem er Papierkopien der relevanten elektronischen Datensätze anfertigt oder indem er aktiv Kopien eventueller elektronischer Datensätze in Dateien auf seinem Computer speichert. Die Abhängigkeit von manuellen Methoden, um das Führen solcher Aufzeichnungen zu gewährleisten, ist eindeutig sowohl unzuverlässig als auch arbeitsaufwändig.

[0174] Das bevorzugte System andererseits sucht den Informationsgehalt aller vom System verarbeiteten Kommunikationen nach Anzeichen dafür ab, dass eine Transaktion begonnen hat oder stattfindet. Es gibt viele solcher Anzeichen. Das einfachste ist das, ob die Verbindung sicher ist oder nicht, da die meisten Webseiten vor dem Durchführen einer Transaktion eine sichere Verbindung negoziieren und diese Verbindung danach wieder schließen. Die Ermittlung, ob eine Verbindung sicher ist, erfolgt durch Untersuchen der URL-Adresse der Zielwebseite. Eine sichere Verbindung wird durch ein ‚s' nach dem Präfix ‚http' angezeigt. So besteht eine Betriebsart des bevorzugten Systems darin, alle zu einer Webseite gesendeten Seiten aufzuzeichnen, während eine Verbindung sicher ist. Das bevorzugte System führt auch Aufzeichnungen über Webseiten, die sichere Verbindungen negoziieren, aber keine eCommerce-Sites sind, d. h. solche, die zu anderen Zwecken als für Käufe angeschlossen sind und die keine zu diesen Seiten übertragenen Daten aufzeichnen. Eine solche Webseite könnte die Notmail-Webseite von Microsoft sein, die einen Email-Dienst bereitstellt.

[0175] Ein anderes Anzeichen könnte einfach die URL-Adresse der Site sein. In diesem Fall kann das bevorzugte System so konfiguriert werden, dass es alle zu einer Webseite übertragenen Daten aufzeichnet, die als die eines Online-Handelsunternehmens identifiziert wurden. Andere Anzeichen könnten eine identifizierte Kreditkartennummer, eine elektronische Quittung, eine Email-Bestätigung des Verkaufs, die Verwendung eines digitalen Zertifikats, insbesondere eines digitalen Garantiezertifikats, oder ein Kaufcode sein.

[0176] Wenn der Ablauf einer Transaktion identifiziert wurde, dann kann das bevorzugte System die Details der Transaktion sowohl durch Speichern der Gesamtheit jeder Kommunikation zwischen einem Benutzer und dem identifizierten Händler oder durch Scannen der Übertragungen und Extrahieren bestimmter Details wie z. B. Datum, Betrag, Warentyp, Menge usw. aufzeichnen.

[0177] Das Aufzeichnen von Transaktionsdaten kann gestoppt werden, wenn das Ende der Transaktion identifiziert wird oder wenn eine vordefinierte Anzahl von Übertragungen zwischen dem Käufer und dem Händler stattgefunden hat. Ebenso kann das bevorzugte System, wenn eine Transaktion identifiziert wurde, in der Datenbank eine vordefinierte Anzahl von gecachten Übertragungen aufzeichnen, die unmittelbar vor der ersten erkannten Übertragung der Transaktion stattgefunden haben.

[0178] Dies ist dann nützlich, wenn beispielsweise das erste Anzeichen dafür, dass eine Übertragung stattfindet, die Erkennung einer Kreditkartennummer oder einer elektronischen Quittung ist, da diese wahrscheinlich ganz am Ende einer Transaktion empfangen werden. Die vorherigen Übertragungen können beispielsweise aus Webseiten bestehen, die Informationen über die gekauften Waren oder Dienste enthalten, oder ein Austausch von Emails, wo Spezifikationen oder Lieferbedingungen vereinbart wurden. Man beachte, dass es vollkommen möglich ist, dass frühere Übertragungen vom selben Typ sind wie die, in denen die Transaktion erkannt wurde, oder von einem anderen Typ oder eine Mischung von Typen. So könnte beispielsweise ein Benutzer eine Website www.abc.com besuchen, Details von Waren einholen und diese dann in einer zu Orders@abc.com gesendeten Email bestellen.

[0179] Das bevorzugte System zeichnet die Transaktionsdetails in einer zentralisierten gemeinsamen Datenbank **42** auf. Zusätzlich kann die Datenbank eine lokale Datei oder ein Dienst auf einem Netzwerk sein. Die in der Datenbank gespeicherten Informationen können mit bekannten Verschlüsselungstechniken verschlüsselt werden, so dass nur eine Person mit ausreichender Autorisierung darauf zugreifen kann.

[0180] Fig. 12 ist eine Darstellung des Ablaufs eines Ausführungsbeispiels für ein Modul zum Identifizieren, wann eine elektronische Transaktion online durchgeführt wird. Fig. 14 illustriert den Vorgang, mit dem das bevorzugte System eine identifizierte Transaktion in der Datenbank aufzeichnet, und Fig. 15 illustriert, wie das bevorzugte System es zulässt, dass eine identifizierte Transaktion auf der Basis einer vorbestimmten Zulassungsrichtlinie zugelassen oder abgelehnt wird.

[0181] Als Nächstes wird mit Bezug auf Fig. 12 der Betrieb eines Moduls zum Identifizieren beschrieben, wann eine Online-Transaktion stattfindet.

[0182] Das Modul beginnt den Betrieb in Schritt S250 als Reaktion auf den Empfang von Daten oder als Reaktion darauf, dass ein Benutzer die Übertragung von Daten zu einem fernen Ort einleitet. Im Falle einer Webbrowser-Implementation ist dies nach Punkt A bzw. nach Punkt C, wie in Fig. 3 gezeigt; bei einer Implementation in einem Email-Client ist dies nach Punkt A bzw. B, wie in Fig. 5 gezeigt.

[0183] Die Steuerung geht dann zum Entscheidungsschritt S252, wo ermittelt wird, ob, im Falle eines Webbrowsers, eine sichere Verbindung zwischen der Daten übertragenden Site und der Daten empfangenden Site negoziiert wurde. Dies kann durch Abfragen der URL-Adresse erzielt werden, mit der die Verbindung aufgenommen wurde, wie oben erwähnt, oder durch Abfragen des Webbrowsers, um zu sehen, ob verschlüsselt wird. Bei einer Email-Nachricht fällt dieser Schritt weg und die Steuerung geht direkt zu Schritt S260. Da Online-Webbrowser-Transaktionen gewöhnlich die Übertragung von persönlichen Informationen wie Name und Adresse, Kreditkartennummer oder andere Kontokenninformationen beinhalten, werden sichere Verbindungen gewöhnlich ganz selbstverständlich negoziiert. So ist die Anwesenheit einer sicheren Verbindung allein ein guter Hinweis darauf, dass eine Transaktion stattfindet. Sichere Verbindungen können jedoch auch aus anderen Gründen als die Übertragung von Transaktionsdetails negoziiert werden. Wenn also in Schritt S252 festgestellt wird, dass die Verbindung sicher ist, dann geht die Steuerung zu Schritt S254, wo die Adresse der fernen Site, mit der die Verbindung hergestellt wurde, anhand einer Liste bekannter Sites geprüft wird, die keine Einrichtungen zum Durchführen von Online-Transaktionen bieten, aber die sichere Verbindungen herstellen. Browsergestützte Email-Sites wie z. B. die Hutmail-Site von Microsoft sind ein solches Beispiel. Die Steuerung geht dann zum Entscheidungsschritt S256, wo eine Ermittlung auf der Basis des vorherigen Checks erfolgt. Wenn die Site-Adresse als Non-eCommerce-Site identifiziert wird, d. h. eine, die die Ausführung einer Transaktion nicht ermöglicht, dann wird festgestellt, dass eine Transaktion möglicherweise stattfindet oder nicht, und die Steuerung geht zum Entscheidungsschritt S260, um weitere Checks über den Inhalt der Übertragung durchzuführen. Wenn in Schritt S256 die Site-Adresse nicht als eine bekannte Non-eCommerce-Site identifiziert wird, dann wird davon ausgegangen, dass eine Online-Transaktion stattfindet, und das Modul verlässt die Routine bei Schritt S258.

[0184] Wenn in Schritt S252 gefunden wird, dass keine sichere Verbindung hergestellt wurde, oder wenn eine sichere Verbindung hergestellt wurde, aber mit einer bekannten Non-eCommerce-Site gemäß Ermittlung in Schritt S256, oder wenn die Übertragung eine Email ist, dann geht die Steuerung zum Entscheidungsschritt S260. Im Entscheidungsschritt S260 erfolgt der erste einer Reihe von Checks über den Inhalt der Übertragung, um zu ermitteln, ob sie Teil einer Transaktion ist oder nicht. In Schritt 260 wird die Übertragung gescannt, um zu sehen, ob sie eine Kreditkartennummer enthält. Das Verfahren hierfür wurde mit Bezug auf Fig. 8 beschrieben. Wenn in der Übertragung eine Kreditkartennummer gefunden wird, dann wird davon ausgegangen, dass eine Transaktion stattfinden muss, und die Steuerung geht zu Schritt S258, wo das Modul die Routine verlässt. Wenn keine Kreditkartennummer gefunden wird, dann geht die Steuerung stattdessen zum Entscheidungsschritt S262, wo die Übertragung gescannt wird, um zu sehen, ob sie einen Kontocode enthält. Kontocodes können (zum Beispiel) in einer separaten Datei gespeichert werden, auf die das Modul bei der Ausführung dieses Schrittes zugreift, oder alternativ kann ein Kontocode anhand von beschreibenden Daten in der Übertragung identifiziert werden, wie z. B. ein Feldname wie ‚Kontonummer' oder ähnliche Zeichen, die im Text einer Nachricht erscheinen.

[0185] Wenn im Entscheidungsschritt S262 ein Kontocode gefunden wird, dann wird davon ausgegangen, dass die Übertragung Teil einer Transaktion ist, und die Steuerung geht zu Schritt S258, wo das Modul die Routine verlässt. Wenn kein Kontocode gefunden wird, dann geht die Steuerung zu Schritt S264, wo im Falle eines Webbrowsers die URL-Adresse mit einer Liste von bekannten, in einer Datei oder in einer Datenbank gespeicherten eCommerce-URL-Adressen verglichen wird. Im Entscheidungsschritt S266 erfolgt eine Ermittlung an diesem Vergleich. Wenn gefunden wird, dass die URL-Adresse auf einer bekannten eCommerce-Seite oder Teil eines bekannten Satzes von eCommerce-Seiten ist, dann wird festgestellt, dass eine eCommerce-Transaktion stattfindet, und die Steuerung geht zu Schritt S258, wo das Modul die Routine verlässt. Ebenso kann, bei einer Email, die Zieladresse mit einer Liste bekannter eCommerce-Email-Adressen verglichen werden, z. B. ‚orders@abc.com', und im Falle einer Übereinstimmung wird festgestellt, dass eine eCommerce-Transaktion stattfindet, und die Steuerung geht zu Schritt S258, wo das Modul die Routine verlässt.

[0186] Die soeben beschriebenen Checks sind lediglich für die möglichen Checks repräsentativ, die vorgenommen werden könnten, um zu ermitteln, ob eine Übertragung wahrscheinlich Teil einer eCommerce-Transaktion ist oder nicht, und sollen nicht erschöpfend sein. Ferner hat die Reihenfolge, in der die Checks illustriert wurden, keine besondere Bedeutung. Die Reihenfolge ist lediglich von der Struktur der Richtliniendaten abhängig, wie mit Bezug auf Fig. 13 ersichtlich ist.

[0187] In Schritt S268 ist ein allgemeiner Check illustriert, der zusätzlich zu den oben beschriebenen eventuelle weitere Checks nach einem Hinweis auf eine Transaktion repräsentiert, die ein Unternehmen als wünschenswert ansieht, wie z. B. die Suche nach Kaufcodes oder eingebetteten Codes in den Daten. Es wird bevorzugt, dass es der Webbrowser oder der Email-Client, der im bevorzugten System verwendet wird, dem Benutzer erlaubt, Übertragungen mit einem eingebetteten Code zu markieren, um anzuzeigen, dass die Übertragung Teil einer Transaktion und aufzuzeichnen ist. Auch könnte der eingebettete Code dadurch in die Daten gesetzt werden, dass die Website oder der Email-Client einige der Transaktionsdaten zur Workstation des Benutzers sendet.

[0188] Die Steuerung geht nach Schritt S266 zu diesem Schritt, wenn die Site nicht als bekannte eCommerce-Site erkannt wird, und wenn ein solcher Transaktionsindikator in Schritt S268 gefunden wird, dann wird festgestellt, dass eine Transaktion stattfindet und die Steuerung geht zu Schritt S258, wo das Modul die Routine verlässt. Wenn in Schritt S268 kein solcher Indikator gefunden wird, dann wird davon ausgegangen, dass keine Transaktion stattfindet, und das Modul verlässt die Routine in Schritt S258. Nach dem Verlassen können die Daten nach Punkt C und B in Fig. 3 bzw. Fig. 5 übertragen oder nach ihrem Empfang an Punkt A in den Fig. 3 und Fig. 5 verarbeitet werden.

[0189] Ziel in dem beschriebenen Beispiel ist es, das Aufzeichnen von Übertragungen und möglichen Transaktionsdetails zu beginnen, wenn auch nur der Verdacht besteht, dass eine Transaktion stattfindet. Es wird davon ausgegangen, dass es vorzuziehen ist, Daten aufzuzeichnen, auch wenn sie nicht Teil einer Transaktion sind, anstatt eine Transaktion überhaupt nicht aufzuzeichnen. Fig. 13 ist eine Illustration der Richtliniendaten, die zum Identifizieren verwendet werden, dass eine eCommerce-Transaktion stattfindet, und um die Art und Weise zu steuern, in der die Transaktionsdaten aufgezeichnet werden. Die Richtliniendaten werden durch einen Transaktionszweig des Richtliniendatenbaums repräsentiert, der in zwei separate Unterzweige mit der Bezeichnung ‚Identification' und ‚Termination' unterteilt wird. Der Identification-Zweig wiederum ist in fünf Unterzweige unterteilt, die den Feststellungen entsprechen, die in dem in Fig. 12 illustrierten Prozess vorgenommen wurden. Der erste dieser Unterzweige mit der Bezeichnung ‚IfConnectionGoesSecure' erlaubt es einem Benutzer vorzugeben, ob die Aufzeichnung beginnen soll, wenn das Einsteckmodul erfasst, dass die Verbindung zum Webserver sicher geworden ist. Die auf diesem Unterzweig vorgegebene Bedingung entspricht dem in Fig. 12 gezeigten Entscheidungsschritt S252. Man wird mit Bezug auf die Fig. 12 und Fig. 13 verstehen, dass der in Fig. 12 gezeigte Steuerfluss dem Layout der Bedingungen entspricht, die auf den in Fig. 13 gezeigten Zweigen des Richtliniendatenbaums vorgegeben sind. Der ExcludedSites-Zweig des IfConnectionGoesSecure-Zweigs enthält einen Verweis auf eine Tabelle q, in der die Websites aufgeführt sind, die bekanntlich sichere Sites negoziieren, von denen aber bekannt ist, dass sie keine eCommerce-Websites sind. Auf Tabelle q wird in Schritt S256 des in Fig. 12 gezeigten Prozesses verwiesen.

[0190] Der nächste Unterzweig des Identification-Zweigs heißt ‚IfCreditCardNumberPresent' und erlaubt es dem Benutzer vorzugeben, ob die Erfassung einer Kreditkartennummer zum Einleiten des Aufzeichnens von übertragenen oder empfangenen Daten verwendet werden soll oder nicht. Dieser Unterzweig entspricht dem Entscheidungsschritt S260. Der PreviousPages-Unterzweig des IfCreditCardNumberPresent-Zweigs führt die Zahl von Webseiten vor der Webseite auf, in der die Kreditkartennummer erfasst wurde, die ebenfalls aufzuzeichnen sind. Da Kreditkartennummern normalerweise am Ende der Transaktion submittiert werden, können mit diesem Unterzweig vorherige Webseiten, die wahrscheinlich die Details und die Anforderung der Transaktion enthalten, abgerufen und gespeichert werden. Diese Webseiten werden kontinuierlich durch das bevorzugte System gecacht, so dass im Falle der Identifikation einer Transaktion diese aus dem Cache abgerufen und in der Datenbank gespeichert werden kann. Dies wird mit Bezug auf Fig. 14 näher erläutert.

[0191] Der nächste Unterzweig des Identification-Zweigs heißt ‚IfAccountsCodePresent' und ermöglicht es einem Benutzer vorzugeben, ob die Erkennung eines Kontocodes in den übertragenen oder empfangenen Daten als ein Indikator zum Einleiten des Aufzeichnens der Daten anzusehen ist. Die Kontocodes werden in dem in Fig. 12 gezeigten Schritt S262 durch Verweis auf Tabelle r identifiziert. Der Verweis auf diese Tabelle befindet sich im AccountCodes-Unterzweig des IfAccountCodePresent-Zweigs. Man beachte, dass diese Tabelle auch die Zahl vorheriger aufzuzeichnender Seiten ähnlich wie die oben für die Kreditkartenidentifikation beschriebene zeigt, aber in diesem Fall wird die Zahl der aufzuzeichnenden vorherigen Seiten in Tabelle r gespeichert, so dass eine andere Anzahl von Seiten für jeden erfassten Kontencode vorgegeben werden kann.

[0192] Mit dem IfKnownECommerceSite-Zweig kann der Benutzer eine Liste von Sites, Teilen von Sites oder sogar einzelnen Seiten entsprechenden URL-Adressen erstellen, wo bekanntlich eCommerce-Transaktionen stattfinden. Die URL-Adresse der aktuellen Seite wird mit Einträgen in dieser Liste verglichen, um zu ermitteln, ob eine Transaktion stattfindet. Der KnownSites-Unterzweig enthält einen Verweis auf Tabelle s, in der die URL-Adressen bekann-

ter eCommerce-Sites gespeichert sind. Die Ermittlung, ob die URL-Adresse der Website eine bekannte eCommerce-Site ist, erfolgt im Entscheidungsschritt S266 nach Schritt S264 von Fig. 12. Schließlich bietet der IfOtherIndicatorPresent-Zweig dem Benutzer eine Möglichkeit, um vorzugeben, ob die Ermittlung anderer Indikatoren als Anfangspunkt für das Aufzeichnen von Daten benutzt werden soll oder nicht. Zwei Unterzweige dieses Zweigs namens Keywords und PreviousPages geben mögliche erkennbare Indikatoren an, in diesem Fall die in Tabelle t aufgeführten Schlüsselwörter, und auch die Zahl der vorherigen Seiten, die gespeichert werden müssen, wenn Schlüsselwörter erkannt werden.

[0193] Der Termination-Zweig des Transactions-Zweigs teilt sich in vier Unterzweige auf, die Bedingungen zum Beenden des Aufzeichnens von gesendeten oder empfangenen Daten angeben. Jeder Unterzweig gibt eine Bedingung an, anhand derer das Ende der Transaktion definiert werden kann. Mit dem ersten Zweig, ‚IfConnectionGoesInsecure', kann der Benutzer vorzugeben, dass das Aufgeben einer sicheren Verbindung durch den Webbrowser das Ende einer Transaktion anzeigt, so dass die Aufzeichnung gestoppt werden sollte. Die anderen Unterzweige geben vor, dass die Aufzeichnung jeweils zu stoppen ist, wenn sich die Website ändert, wenn eine digitale Quittung empfangen wird, sowie nach dem Empfang von 20 Webseiten nach der Identifikation, dass eine Transaktion stattfindet.

[0194] Es muss hervorgehoben werden, dass Richtliniendaten, die insbesondere in diesem Diagramm, aber auch in den anderen Diagrammen dargestellt sind, für jeden Benutzer individuell sind. Ein Benutzer kann nicht nur vorgeben, ob auf bestimmte Bedingungen zu reagieren ist oder nicht, indem er die Ja- oder Nein-Variable entsprechend einstellt oder z. B. die Anzahl der Seiten ändert, die aufgezeichnet werden sollen, sondern auch die Struktur und Anordnung von Zweigen und die auf diesen Zweigen vorgegebenen Bedingungen können sich von Benutzer zu Benutzer unterscheiden. Man wird verstehen, dass das Richtlinienbeispiel zwar das Aufzeichnen von Transaktionen in einer Webbrowser-Umgebung beschreibt, aber eine ähnliche Richtlinie würde auch die Email-Umgebung steuern, die Sichere-Verbindung-Option weglassen, aber die Definition einer Richtlinie zum Aufzeichnen von Emails nach dem Erkennen von Kreditkartennummern, Kontocodes oder anderen identifizierbaren Informationen darin zulassen, oder wo Emails zu bekannten eCommerce-Adressen gesendet werden.

[0195] Von dem Verfahren zum Identifizieren einer Transaktion kann dann voll profitiert werden, wenn das Verfahren zusammen mit Mitteln zum Aufzeichnen von Übertragungen zwischen einem Benutzer des bevorzugten Systems und einer fernen Site angewendet wird. So können Aufzeichnungen aller von einem Benutzer ausgeführten Transaktionen automatisch geführt werden. Die Datensätze können auf dem neuesten Stand gehalten werden, ohne Papierkopien jeder empfangenen oder gesendeten Übertragung anfertigen zu müssen. Dies macht die Buchführung eines Unternehmens wesentlich einfacher und genauer.

[0196] Fig. 14 illustriert den Betrieb eines Moduls zum Aufzeichnen von Übertragungen, die eine Transaktion umfassen. Das Modul beginnt in Schritt S270.

[0197] Wenn das Modul als Teil eines Webbrowsers implementiert wird, dann beginnt Schritt S270 in Punkt A in Fig. 3 nach dem Empfang von Daten oder nach Punkt C in Fig. 3 unmittelbar vor dem Senden von Daten zu einer fernen Site. Bei einer Implementation des Moduls als Teil eines Email-Client erfolgt Schritt S270 nach Punkt A in Fig. 5, nachdem eine Email empfangen wurde, oder nach Punkt B in Fig. 5, unmittelbar bevor eine vom Benutzer verfasste Email zu einem Empfänger gesendet wird.

[0198] Nach Schritt S270 geht die Steuerung zu Schritt S272, wo der Test zum Identifizieren einer Transaktion, oben mit Bezug auf Fig. 9 beschrieben, durchgeführt und ermittelt wird, ob eine eCommerce-Transaktion stattfindet oder nicht. Die Steuerung geht dann zum Entscheidungsschritt S274, wo nach der Feststellung, dass keine Transaktion stattfindet, die Steuerung direkt zu Schritt S276 geht, wo das Modul die Routine verlässt.

[0199] Wenn jedoch festgestellt wird, dass eine Transaktion stattfindet, dann geht die Steuerung zu Schritt S278, wo die Richtlinie anhand eines oder mehrerer Erkennungsmittel, die Identität des Senders, der Betrag der Transaktion geprüft wird, oder andere Parameter zum Bestimmen, welche vorherigen Übertragungen ggf. mit der identifizierten Übertragung gespeichert werden sollten und wie detailliert die Übertragung aufgezeichnet werden soll. Die Richtlinie könnte beispielsweise verlangen, dass eine Transaktion für eine große Geldsumme ausführlicher aufgezeichnet wird als eine Transaktion für eine kleine Summe. Ein Betriebsbeispiel hierfür könnte die Aufzeichnung jeder Webseite sein, auf die beim Durchführen einer Transaktion auf der Website eines Online-Händlers bei Transaktionen für große Geldsummen zugegriffen wird, wobei aber nur die Übertragung aufgezeichnet wird, die eine elektronische Quittung für Transaktionen für kleinere Beträge beinhaltet.

[0200] Die Richtliniendatei könnte außer der zu speichernden Datenmenge auch den Charakter der aufzuzeichnenden Daten bestimmen. Die gesamte Übertragung oder Webseite kann als eine Serie von

Schnappschüssen der Transaktion ebenso aufgezeichnet werden, wie beispielsweise Webseiten in Cache-Speichern gespeichert werden, oder alternativ können individuelle Datenelemente, wie z. B. Datum, Identität des Händlers, Betrag usw., aus der Übertragung oder Webseite extrahiert und entweder alleine oder zusammen mit den Schnappschussdaten gespeichert werden.

[0201] Auf diese Weise kann Speicherplatz am effektivsten genutzt werden, um sicherzustellen, dass genügend Platz zum Aufzeichnen der wichtigsten Transaktionen vorhanden ist.

[0202] Die Menge der aufzuzeichnenden Transaktionsdaten kann auch von der Identität des Händlers, vom geografischen Ort, der Handelshistorie mit dem Unternehmen des Benutzers sowie den angebotenen Waren und Diensten abhängig sein.

[0203] In Fig. 13 zeigen die Richtliniendatenbeispiele ein einfaches Szenario, in dem die aufzuzeichnende Datenmenge im Hinblick auf die Zahl der Webseiten vorgegeben wird, die von den im Memory gecachten Seiten abzurufen sind. Die Anzahl unterscheidet sich je nachdem, ob eine Kreditkartennummer, ein Kontocode oder ein Schlüsselwort identifiziert wird. Ferner zeigt Tabelle r, dass sich die Zahl der zu speichernden vorherigen Webseiten mit der Erkennung unterschiedlicher Kontocodes unterscheiden kann, je nach der relativen Bedeutung des Kontos.

[0204] Die Erweiterung dieses einfachen Falls auf einen weiter entwickelten kann dadurch erzielt werden, dass in den Richtliniendaten ein höheres Detail-Level gegeben wird. Weitere Zweige am Richtliniendatenbaum könnten Firmen- oder Personennamen oder Schlüsselwörter in Bezug auf Waren und/oder Dienste vorgeben; ebenso die gemäß diesen Schlüsselwörtern aufzuzeichnende Datenmenge und Namen.

[0205] Auch die Tabellen könnten so erweitert werden, dass sie auf die Menge an unterschiedlichen Datentypen verweisen, die gespeichert werden sollen. Daten wie z. B. der Firmenname, was verkauft wird, die Menge usw. könnten aus dem Email-Text, dem die Webseite definierenden HTML-Text oder aus der DOM-Repräsentation der Webseite extrahiert und in der Datenbank gespeichert werden.

[0206] Es können alle im Cache gespeicherten Webseiten oder Informationen abgerufen werden, oder das System kann nur Seiten abrufen, die mit der anfangs als Teil einer Transaktion identifizierten Seite gemeinsame Details haben.

[0207] Alternativ kann dem Benutzer eine Liste aller gespeicherten Nachrichten vorgelegt werden, aus der der Benutzer solche Übertragungen manuell auswählen kann, die sich auf die identifizierte Transaktion beziehen.

[0208] Nach dem Ermitteln, wie viele Daten aufgezeichnet werden sollen, geht die Steuerung zum Entscheidungsschritt S280. Wenn in Schritt S280 frühere Übertragungen zu speichern sind, geht die Steuerung zu Schritt S282, wo die im lokalen Cache gespeicherten Übertragungen abgerufen werden. Bei einem Webbrowser kann dies eine vorbestimmte Anzahl früherer Seiten sein, wie oben beschrieben. Wo die Transaktion in einem Webbrowser erkannt wurde, da kann eine Richtlinie auch diktieren, dass der Cache nach früheren Email-Nachrichten in Bezug auf die Transaktion durchsucht wird, die z. B. von derselben Organisation gesendet oder empfangen wurde. Dies kann durch Vergleichen der Teile der URL-Adresse des Browsers mit Teilen der Email-Adressen ermittelt werden. Ebenso können in Email-Nachrichten erkannte Transaktionen bewirken, dass sowohl frühere Emails als auch frühere Webseiten aus dem Cache abgerufen werden. Die Steuerung geht dann zu Schritt S284, wo die identifizierte Transaktion und evtl. abgerufene frühere Übertragungen in der Systemdatenbank **42** gespeichert werden.

[0209] In Schritt S280 geht die Steuerung, wenn keine früheren Übertragungen benötigt werden, direkt zu Schritt S284, wo die als Transaktion identifizierte Übertragung in der Systemdatenbank aufgezeichnet wird. Zur selben Zeit, in der die Übertragungen in Schritt S284 gespeichert werden, können auch verwandte Daten wie die Benutzeridentität, der Betrag und die andere Transaktionspartei in der Systemdatenbank registriert werden, so dass ein kompletter Datensatz entsteht, obwohl dies von den Anweisungen in den Richtliniendaten abhängig ist. Die Steuerung geht dann zu S286 und das Modul verlässt die Routine.

[0210] Nach Schritt S276, wenn das Modul die Routine verlassen hat, können die Daten nach Punkt A in den Fig. 3 und Fig. 5 übertragen oder nach dem Empfang an den Punkten C und B jeweils in den Fig. 3 und Fig. 5 verarbeitet werden.

[0211] Nach der Identifikation einer Übertragung können alle Übertragungen zwischen dem Benutzer und der anderen Partei aufgezeichnet werden, bis das System erkennt, dass die Transaktion komplett ist. Die Erkennung des Endpunkts einer Transaktion und das Stoppen des Aufzeichnens können auf eine Weise ähnlich wie die erfolgen, die oben zum Identifizieren beschrieben wurde, ob eine Transaktion stattfindet. Die einfachste Implementation besteht darin, Übertragungsinformationen aufzuzeichnen, bis eine elektronische Quittung oder ein Versandauftrag eingegangen ist. Alternativ kann bewirkt werden,

dass das Aufzeichnen von Übertragungen nach einer vorbestimmten Anzahl von Übertragungen zwischen dem Benutzer und der anderen Partei oder nach dem Verstreichen einer bestimmten Zeit seit der Identifikation der Transaktion gestoppt wird.

[0212] Übertragungen können vereinfacht werden, wenn der Cache nach jeder Änderung einer Website durch den Benutzer geleert wird. Dies hält den Speicherbedarf für den Cache-Memory klein und reduziert die Zahl der zu durchsuchenden vorherigen Übertragungen, wenn Suchtechniken angewendet werden sollen.

[0213] Man wird verstehen, dass die oben beschriebenen Methoden auch zum Aufzeichnen von assoziierten Übertragungen angewendet werden können, die nach dem Erkennen und Aufzeichnen einer Transaktion stattfinden. So folgt auf eine mit einem Webbrowser durchgeführte Transaktion typischerweise eine vom Verkäufer zum Käufer gesendete Bestätigungsemail. Diese Email kann als Teil der Transaktion erkannt werden, da sie gemeinsame Charakteristiken wie Auftragsnummer, Kontonummer, Warenbeschreibung, Preis usw. enthält. Sie kann auch von einer Adresse gesendet werden, die der Website-Adresse ähnlich ist, z. B. ‚customerservices@abc.com', wenn die für den Kauf benutzte ursprüngliche Website ‚abc.com' war. Vorzugsweise wird ein Zeitelement benutzt, so dass nur Folgeübertragungen als mit der ursprünglichen Transaktion assoziiert angesehen werden, die innerhalb einer gegebenen Zeitperiode auftreten.

[0214] Es kann vorteilhaft sein, über Transaktionsinformationen hinaus auch andere Informationen aufzuzeichnen, damit das Management das Verhalten seiner Kunden analysieren kann, z. B. um zu gewährleisten, dass die Organisation durch die Nutzung des elektronischen Handels in der Tat echte Produktivitätsvorteile erzielt. Solche Informationen sind nicht auf die Produktivität des Benutzers selbst begrenzt, sondern auf den gesamten Prozess, so dass beispielsweise ein Vergleich von Einkaufs-Websites angestellt werden kann, um zu ermitteln, welche im Hinblick auf den Verkaufsprozess am effizientesten sind, und somit welche den größten Nutzen im Hinblick auf eine Senkung der Einkaufskosten bringen. Das bevorzugte System ermöglicht dies durch Aufzeichnen von zusätzlichen Informationen, wie z. B. die für den Kauf benötigte Menge an Zeit, die Anzahl der Tastenanschläge und Mausklicke, die zum Abwickeln eines Kaufs erforderlich sind, die Menge an ‚Untätigkeits'-Zeit, während der Benutzer auf das Herunterladen von Seiten oder den Empfang von Antworten wartet. Diese Informationen können mit dem Transaktionsdatensatz in der Datenbank aufgezeichnet werden, so dass eine statistische Analyse über einen Bereich von Transaktionen ausgeführt werden kann.

[0215] Die für eine Transaktion benötigte Zeit kann durch Assoziieren eines Zeitstempels mit jeder der empfangenen Übertragungen ermittelt werden. Wenn festgestellt wird, dass die Transaktion komplett ist, dann wird der mit der ersten Übertragung (die evtl. aus dem Cache in Schritt S282 zurückgewonnen wurde) assoziierte Zeitstempel von dem mit der letzten Übertragung assoziierten Zeitstempel subtrahiert und das Ergebnis, das die Gesamtdauer der Transaktion sein wird, wird in der Datenbank in Schritt S284 gespeichert. Alternativ könnten der erste und der letzte Zeitstempel in der Datenbank aufgezeichnet und die Transaktionsdauer später berechnet werden. Die Zahl der Tastenanschläge und Mausklicke kann in einem System auf der Basis von Microsoft Windows mit Hilfe von standardmäßigen Windows-‚Hooks' in das Betriebssystem ermittelt werden. Solche Techniken sind ausführlicher in dem Dokument „Win 32 Hooks" von Kyle Marsh von der Microsoft Developer Network Technology Group vom 29. Juli 1993 beschrieben, erhältlich von der Microsoft Corporation Website (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnmgmt/html/msdnhooks32.asp).

[0216] Das bevorzugte System führt einen Zähler für die Anzahl der Tastenanschläge (mit dem WH KEYBOARD Hook) und Mausklicke (mit dem WH MOUSE Hook), die jeweils zwischen empfangenen Übertragungen auftreten, und assoziiert diese Summen mit der empfangenen Übertragung. Die Tastenanschläge und Mausklicke, die auftreten, während eine andere Anwendung im Fokus ist (z. B. wenn der Benutzer vorübergehend auf eine andere Anwendung umschaltet), werden ignoriert. Wenn festgestellt wird, dass die Transaktion komplett ist, dann werden die Summen der Tastenanschläge und Mausklicke, die zwischen der ersten Übertragung (die möglicherweise aus dem Cache in Schritt S282 zurückgewonnen wurde) und der letzten Übertragung aufgetreten sind, miteinander addiert, und das Ergebnis, das die Gesamtzahl der Tastenanschläge und Mausklicke während der gesamten Transaktion ist, wird in der Datenbank in Schritt S284 gespeichert. Ebenso kann die Reaktionszeit der Website-Transaktion durch Notieren des Zeitpunkts, an dem jede abgehende Übertragungsanforderung gesendet wurde, und Subtrahieren des Ergebnisses von dem Zeitpunkt, an dem die Antwortübertragung empfangen wurde, gemessen werden. Das Anhäufen der Reaktionszeiten zwischen dem Anfang und dem Ende der Transaktion ergibt die Gesamtzeit, die der Benutzer mit dem Warten auf die Website verbracht hat. Ebenso misst das bevorzugte System auch die Reaktionszeit des Benutzers, d. h. die Zeit zwischen dem Empfang einer Übertragung und dem Moment des Sendens einer Antwort.

[0217] Das bevorzugte System berechnet auch, wie

groß der Anteil der Reaktionszeit des Benutzers ist, der mit dem Eingeben von Daten verbraucht wird, so dass die Zeit, die der Benutzer braucht, um die eingehende Übertragung zu ‚verdauen' (die Differenz), ermittelt werden kann. Die mit dem Eingeben von Daten verbrachte Zeit wird mittels einer ‚Stoppuhr' ermittelt. Die Stoppuhr wird nach jedem Empfang einer neuen Übertragung zurückgestellt und wird sofort neu gestartet, wenn der Benutzer eine Taste anschlägt oder die Maus anklickt. Falls der Benutzer eine vorbestimmte Zeit lang keine Taste anschlägt oder die Maus anklickt, z. B. 5 Sekunden, dann nimmt das System an, dass der Benutzer jetzt Details der vorherigen Übertragung verdaut, und stoppt die Uhr. Die Uhr wird auch dann gestoppt, wenn der Tastenanschlag oder Mausklick das Senden einer abgehenden Übertragung bewirkt. Die Summe der mit dem Eingeben von Daten verbrachten Zeit zwischen dem Anfang und dem Ende der Transaktion ergibt die Gesamtzeit, die der Benutzer mit dem Eingeben von Daten auf der Website verbracht hat. Die Zeitsummen können in der Datenbank in Schritt S284 zur weiteren Analyse gespeichert werden.

[0218] Das bevorzugte System stellt auch ein Mittel zum Überwachen von durchgeführten Transaktionen und zum automatischen Verweisen der Transaktion zur Billigung bereit, wenn diese als notwendig erachtet wird. Dieser Vorgang lässt es zu, dass ein großes Unternehmen die von seinen Mitarbeitern vorgenommenen Transaktionen mit einem einzigen Satz von in den Richtliniendaten dargelegten Kriterien überwacht und steuert. Auf die Richtliniendaten kann jedes Mal Bezug genommen werden, wenn eine Transaktion identifiziert wird, um zu ermitteln, ob der Benutzer befugt ist, diese Transaktion selbst durchzuführen, oder ob er eine Autorisierung von einer höheren Stelle in dem Unternehmen benötigt. Der Vorgang ist in Fig. 15 illustriert, auf die nunmehr Bezug genommen werden sollte.

[0219] Das diesen Vorgang ausgestaltende Modul wird in Schritt S290 gestartet. Dieser Start erfolgt vorzugsweise, sobald alle zu beachtenden relevanten Details der Transaktion ermittelt sind und bevor die Transaktion kommittiert wird. Bei einer Email-Transaktion befinden sich Details wie Waren und Preise typischerweise in einer einzigen Email und können vor der Übertragung dieser Email betrachtet werden. Bei einer Webbrowser-Transaktion kann die Existenz einer Transaktion erkannt werden, bevor alle Details bekannt sind, und in diesem Fall erfolgt der Start erst dann, wenn sie es sind. Dies bedeutet normalerweise kein Problem, da eine endgültige Verpflichtung erst ganz am Ende des Transaktionsprozesses stattfindet, lange nachdem alle relevanten Details bekannt sind. Die Erkennung der Transaktion und der relevanten Details kann in der oben mit Bezug auf Fig. 12 beschriebenen Weise ermittelt werden. Kurz mit Bezug auf die Fig. 3 und Fig. 5, dort ist zu sehen, dass Schritt S290 nach Punkt C in Fig. 3 bei einer Webbrowser-Implementation oder nach Punkt A in Fig. 5 bei einer Email-Client-Implementation stattfindet, wenn die benötigten Details bekannt sind.

[0220] Die Steuerung geht von Schritt S290 zum Entscheidungsschritt S292, wo die Details der Transaktion mit den Richtlinieneinstellungen verglichen werden, um zu ermitteln, ob eine Zulassung erforderlich ist oder nicht. Die Ermittlung kann auf der Identität oder Stellung des die Transaktion vornehmenden Mitarbeiters, dem Betrag der Transaktion oder der anderen Transaktionspartei basieren. In einigen Fällen könnte eine Zulassung immer erforderlich sein, wie z. B. dann, wenn der Finanzdirektor eines Unternehmens jede Transaktion überprüfen möchte, bevor sie getätigt wird.

[0221] Fig. 16 zeigt ein Beispiel für Richtliniendaten, die zum Ermitteln, ob eine Transaktion von einer Drittpartei genehmigt werden muss oder nicht, und auch zum Ermitteln der Identität eines geeigneten zu beanspruchenden Billigers (Zulassungsstelle) verwendet werden können. In diesem Fall geben Bedingungen in den Richtliniendaten je nach dem Transaktionsbetrag und der URL-Adresse der anderen Partei der Transaktion vor, ob eine Zulassung erforderlich ist.

[0222] Die relevanten Richtliniendaten sind im Transactions-Approval-Zweig des Richtliniendatenbaums dargelegt. Dieser Zweig teilt sich in vier Unterzweige auf. Der erste Zweig, ‚MaximumUnapprovedTransactionAmount', definiert einen Schwellenbetrag für Transaktionen. Transaktionen für Beträge über diesem Schwellenwert müssen vor der Durchführung von einem Billiger genehmigt werden.

[0223] Der zweite Unterzweig, ‚MaximumUnapproved MonthlyAmount', definiert einen maximalen Betrag für Transaktionen, die ein Benutzer innerhalb eines Monats tätigen darf. In diesem Fall erfordert jede Transaktion, die von dem Benutzer getätigt wird, die zur Folge hätte, dass der monatliche Gesamtbetrag $2500 übersteigt, eine Zulassung von einer Drittpartei, wie auch weitere Transaktionen, die nach dem Erreichen dieses Schwellenbetrags getätigt werden sollen.

[0224] Der dritte Zweig, ‚ExcludedSites', bezieht sich auf eine Tabelle, die Website- und Email-Adressen aller Sites aufführt, die immer von einer Drittpartei genehmigt werden müssen, bevor eine Transaktion getätigt werden kann. Schließlich bezieht sich der letzte Zweig, ‚Approvers', auf eine Tabelle, in der die Namen möglicher Drittpartei-Billiger aufgeführt sind. Neben jedem Namen steht der Höchstbetrag für Transaktionen, für die der Billiger zulassungsbefugt ist, sowie eine Liste von ausgeschlossenen Sites, für die dieser Billiger eine Transaktion nicht genehmigen

darf. Im einfachsten Fall sind Billiger andere Computer-Benutzer, die am selben Netzwerk angeloggt sind wie der Benutzer, der die Transaktion durchführt, z. B. Abteilungsleiter oder Supervisors. Die Zulassungsstellen werden, gemäß der Natur ihrer Rolle, Mitglieder des Handelsunternehmens sein, die die Autorität haben, die Verantwortung für die finanziellen Transaktionen zu übernehmen, die das Unternehmen tätigt. Es ist auch möglich, dass Billiger aus einer Gruppe von Personen genommen werden, die primär für diese Rolle angestellt sind, wie z. B. nur Personen in der Finanzabteilung.

[0225] Wenn die Bedingungen auf den ersten drei Unterzweigen des Transaktionszweigs anzeigen, dass eine Zulassung erforderlich ist, dann kann ein entsprechender Billiger durch Scannen der Tabelle von Zulassungsstellen gefunden werden, bis ein Billiger gefunden wird, dessen Transaktionslimit gleich oder höher ist als die vorgeschlagene Transaktion, und dem es nicht untersagt ist, Transaktionen auf dieser relevanten Site zu genehmigen.

[0226] Man wird verstehen, dass die beispielhaften Richtliniendaten in Fig. 16 Richtliniendaten sind, die für einen einzelnen Computerbenutzer oder eine Benutzergruppe in dem Netzwerk spezifisch sind. Andere Benutzer oder Gruppen können andere Einstellungen und eine andere Liste von Zulassungsstellen haben.

[0227] Man wird verstehen, dass die Bedingungen zum Ermitteln eines geeigneten Billigers durch Erzeugen neuer Unterzweige auf dem Richtliniendatenbaum geschaffen werden können.

[0228] Der Ablauf des Zulassungsprozesses kann beispielsweise außer auf solche, die eine eCommerce-Transaktion umfassen, auch auf jede Übertragungsart erweitert werden. Ein solcher Vorgang kann dadurch implementiert werden, dass die Bedingungen definiert werden oder die Unterzweige der Richtliniendaten z. B. Benutzernamen, Adressen oder Schlüsselwörter vorgeben, die in der Übertragung identifiziert und auf die reagiert werden muss. So kann bewirkt werden, dass alle Email-Übertragungen zu einer bestimmten Firma oder Person billigungspflichtig sind oder alle Emails, die vorbestimmte Informationen enthalten, per Schlüsselwortidentifikation erkannt werden.

[0229] Wenn in Schritt S292 ermittelt wird, dass keine Billigung erforderlich ist, dann geht die Steuerung direkt zu Schritt S294, wo das Modul die Routine verlässt. Nach Schritt S294 wird die Übertragung der Transaktion zugelassen und die Transaktion kann ablaufen. Die Steuerung kehrt von Schritt S294 zu Punkt C in Fig. 3 oder zu Punkt B in Fig. 5 zurück.

[0230] Wenn jedoch in Schritt S292, nach dem Konsultieren der Richtlinieneinstellungen, ermittelt wird, dass die Transaktion billigungspflichtig ist, dann geht die Steuerung zu Schritt S296, wo die Einzelheiten der Transaktion zum Ermitteln eines geeigneten Billigers für die Transaktion benutzt wird. Der Billiger kann ein Firmenmitarbeiter sein, der an seiner Workstation oder an einer Workstation mit einer dedizierten Zulassungsfunktion wie z. B. Operatorkonsolen **44** wie in Fig. 2 gezeigt angeloggt ist, oder er kann sogar ein automatisierter Prozess sein. Bei einem großen Unternehmen mit einer Reihe von Abteilungen kann es vorteilhaft sein, für jede Abteilung eine Gruppe von Billigern zu haben, wobei jede Gruppe die Konten der Abteilung überwacht. So können Transaktionen abgelehnt werden, bevor sie getätigt werden, wenn beispielsweise der Leiter der Abteilung beschließt, alle Käufe oder eine bestimmte Art von Käufen vorübergehend zu suspendieren.

[0231] Die Steuerung geht von Schritt S296 nach der Ermittlung eines geeigneten Billigers zu Schritt S298, wo ein Zulassungsantrag über eine Systemzulassungswarteschlange **100** zum designierten Billiger übertragen wird. Nach Schritt S298 geht die Steuerung zum Entscheidungsschritt S300, wo ermittelt wird, ob eine Antwort von dem Billiger empfangen wurde. In dem Moment, in dem ein Zulassungsantrag vorgelegt wird, wird eine Zeituhr gestartet. Wenn in Schritt S300 keine Antwort empfangen wurde, dann geht die Steuerung zu Schritt S302, wo anhand der Zeituhr ermittelt wird, ob eine Auszeitperiode verstrichen ist oder nicht. Vorausgesetzt, die Periode ist nicht verstrichen, geht die Steuerung von Schritt S302 zurück zu S300, wo das System weiter auf eine Antwort von dem Billiger wartet. So bilden die Entscheidungsschritte S300 und S302 eine Schleife, in der das System wartet, bis eine Antwort empfangen wird oder bis die Auszeit abläuft. Im Entscheidungsschritt S300 geht die Steuerung, wenn eine Antwort empfangen wurde, zu Schritt S304, wo eine Aktion je nachdem stattfindet, ob die Transaktion zugelassen oder abgelehnt wurde.

[0232] Wenn die Transaktion zugelassen wurde, geht die Steuerung von Schritt S304 zu Schritt S294, wo das Modul die Routine verlässt und die Übertragung stattfinden kann. Wenn jedoch die Übertragung nicht zugelassen wird, dann geht die Steuerung von Schritt S300 zu Schritt S306, wo das Modul die Routine verlässt. Das Verlassen in Schritt S306 verhindert jedoch die Übertragung der Transaktion und bringt den Benutzer zu Punkt A in Fig. 3 bei einer Webbrowser-Implementation oder zu Schritt S132 „Email verfassen" in Fig. 5 bei einer Email-Client-Implementation zurück.

[0233] Ebenso geht die Steuerung, wenn in Schritt S302 festgestellt wird, dass die ‚Auszeitperiode' ohne Eingang einer Antwort von dem Billiger abgelaufen ist, direkt zu Schritt S306, wo das Modul die Routine

verlässt.

[0234] Die rechte Seite von Fig. 15 zeigt die für den Billiger beteiligten Schritte. Der Zulassungsprozess beginnt in Schritt S310, von wo die Steuerung zu Schritt S312 geht, in dem die Maschine des Billigers die Systemzulassungswarteschlange nach eventuellen neuen Zulassungsanträgen abfragt. Die Steuerung geht dann zum Entscheidungsschritt S314. In Schritt S314 geht die Steuerung, wenn kein Antrag ansteht, zu Schritt S312 zurück, wo die Systemwarteschlange erneut abgefragt wird. Diese Schritte werden so lange wiederholt, bis ein Zulassungsantrag eingeht oder bis der Billiger den Zulassungsprozess deaktiviert.

[0235] In Schritt S314 geht die Steuerung, wenn ein Zulassungsantrag eingeht, zu Schritt S316, wo der Zulassungsantrag von der Systemwarteschlange heruntergeladen wird und der Billiger selbst entscheidet, ob dem Antrag stattgegeben oder ob er abgelehnt wird. Die Steuerung geht dann zu Schritt S318, wo die Antwort des Billigers zurück in die Systemzulassungswarteschlange und von dort zurück zur Benutzerworkstation übertragen wird.

[0236] Die Steuerung geht von Schritt S318 zurück zu Schritt S312, wo die Systemzulassungswarteschlange nach neuen Zulassungsanträgen abgefragt wird. Man wird verstehen, dass der Zulassungsprozess unter Umständen auch vollkommen automatisiert werden könnte. So könnten beispielsweise Transaktionen automatisch abgelehnt werden, wenn das Unternehmen nicht genügend Mittel besitzt, wenn sie verursachen würden, dass die Budgetbeträge überschritten würden oder wenn sie einfach über einem Höchstbetrag liegen. Eine solche Automatisierung könnte alternativ als Teil des Benutzerprozesses vorgesehen werden, so dass noch nicht mal ein Zulassungsantrag gestellt würde.

[0237] Bei der Ermittlung, ob eine gegebene Transaktion genehmigt werden soll, sollte die Genehmigungsstelle diese idealerweise vollständig betrachten können, z. B. so, dass sie genau sehen kann, was gekauft wird, anstatt einfach Zusammenfassungsinformationen wie Gesamtpreis und Lieferant zu sehen. Das bevorzugte System stellt dies dadurch bereit, dass die oben beschriebenen Merkmale der Aufzeichnung von Übertragungen mit dem Zulassungsmerkmal kombiniert werden. Der in Schritt S298 vorgelegte Zulassungsantrag wird mit einem Verweis auf den Ort in der Datenbank ergänzt, in der die Transaktionsinformationen in Schritt S284 gespeichert wurden. Der Billiger empfängt die Ortsdetails in Schritt S316 und das System ruft die die Transaktion konstituierenden Übertragungen aus der Datenbank ab und zeigt sie auf geeignete Weise an, so dass der Billiger sie beim Fällen seiner Zulassungsentscheidung berücksichtigen kann. Die Operation geht dann normalerweise mit Schritt S318 weiter. Es ist natürlich wichtig, dass der Aufzeichnungsschritt S284 stattfindet, bevor der Zulassungsantrag in Schritt S298 erfolgt, da die aufgezeichneten Informationen sonst noch nicht zur Verfügung stehen. Da die Transaktion in Schritt S284 bereits identifiziert wurde, aber noch nicht abgeschlossen ist (da sie noch nicht gebilligt wurde), muss die in Schritt S284 vorgenommene Datenbankaufzeichnung einen Flag enthalten, der die Transaktion als „anhängig" identifiziert. Dieser Flag kann in Schritt S316 aktualisiert werden, so dass er zeigt, dass die Transaktion zugelassen oder abgelehnt wurde, alternativ kann der Datenbankdatensatz, falls die Zulassung verweigert wurde, gelöscht werden, da die Transaktion nicht stattgefunden hat.

Sicherheit

[0238] Das bevorzugte System bietet Mittel zum Zuweisen einer angemessenen Sicherheitsbewertung zu der Übertragung in Abhängigkeit vom identifizierten Charakter der übertragenen Daten. Die zugewiesene Sicherheitsbewertung kann vom Benutzer des Systems im Einklang mit seinen Erfordernissen anhand der Richtliniendaten eingestellt werden.

[0239] Die einfachste Implementation der Richtliniendaten ist in diesem Falle eine Liste, die in einer ersten Spalte mögliche Datentypen wie z. B. Mitarbeiterpasswörter, Arbeitgeberpasswörter, Kreditkartennummern, Bankdetails usw. und in einer zweiten Spalte die gewünschte Verschlüsselungsstärke (z. B. in Key-Bits) enthält, die als für den jeweiligen Datentyp angemessen angesehen wird. Man wird verstehen, dass auch andere Möglichkeiten zum Zuweisen von Sicherheitsniveaus in Abhängigkeit vom bestimmten Charakter der Daten im Rahmen der Erfindung angewandt werden können.

[0240] Fig. 17 zeigt eine beispielhafte Illustration von Richtliniendaten, die geeignete Verschlüsselungsstärken für verschiedene Datentypen definieren. Die Richtliniendaten haben die Form einer Reihe von Key-Wertepaaren, die auf separaten Zweigen des Richtliniendatenbaums angeordnet sind. Der Key gibt den Datentyp an, der übertragen wird, wie z. B. Passwörter, Kreditkartennummern, submittierte Schlüsselwörter und einen allgemeinen Key für sonstige submittierte Daten. Die Werte, die diesen Keys entsprechen, sind die Verschlüsselungsstärke in Bits, die als für die Übertragung der im Key angegebenen Daten geeignet angesehen wird. Die Key-Wertepaare sind auf mehreren Zweigen des RequiredEncryptionLevel-Zweigs des TransmittedDataSecurity-Zweigs des Richtliniendatenbaums angeordnet. So ist in dem Beispiel ersichtlich, dass Passwörter eine gewünschte Verschlüsselungsstärke von 40 Bits haben, sowohl Firmenkreditkartennummern als auch persönliche Kreditkartennummern eine gewünschte Verschlüsselungsstärke von 128 Bits haben, submit-

tierte Schlüsselwörter eine gewünschte Verschlüsselungsstärke von 40 Bits haben und sonstige submittierte Daten keine Verschlüsselung brauchen.

[0241] Der SubmittedKeyword-Zweig bezieht sich auf bestimmte Wörter oder Ketten oder Text, die als sensitiv designiert wurden und eine Form von Verschlüsselung benötigen. Dies können Benutzernamen, Adressinformationen, finanzielle Informationen oder vorgewählte Wörter wie z. B. ‚vertraulich' oder ‚geheim' sein. Die submittierten Schlüsselwörter können durch Bezugnahme auf eine Tabelle oder Datei erkannt werden, in der sie gespeichert sind.

[0242] Ferner kann sich jeder Zweig der Richtliniendaten, anstatt eine allgemeine Verschlüsselungsstärke anzugeben, auf eine Tabelle beziehen, in der beispielsweise verschiedene Passwörter oder Kreditkartennummern zusammen mit Verschlüsselungsstärken aufgeführt sind, die für jedes Passwort oder jede Nummer spezifisch sind.

[0243] Nach dem Zuweisen einer Sicherheitsbewertung fragt das Einsteckmodul entweder den Webbrowser ab, um die Sicherheit der Verbindung zu ermitteln, die vom Webbrowser mit dem Webserver zur Übertragung dieser Informationen eingerichtet wurde, oder, bei einer Email-Übertragung, die Verschlüsselungseinstellungen, die der Benutzer oder die Anwendung bestimmt hat, werden auf die Nachricht angewendet. Dies ist typischerweise die kryptografische Stärke des zum Codieren der Daten zur Übertragung verwendeten Verschlüsselungsalgorithmus. Solche Übertragungsdetails werden vom Webbrowser als Teil des ‚elektronischen Quittungsaustauschs' vom Webdiensteanbieter empfangen.

[0244] Eine sichere Verbindung wird gewöhnlich in einem Browser-Fenster durch ein geschlossenes Vorhängeschloss-Icon in der rechten unteren Ecke angezeigt. Ein Benutzer kann das Icon anklicken, um das Sicherheitsniveau abzufragen, das durch den Quittungsaustausch bereitgestellt wurde. Dabei kann er eine Benachrichtigung der Form ASSL-gesichert empfangen (128 Bits). Der erste Teil der Benachrichtigung beschreibt den Typ der verwendeten Verschlüsselung, während der zweite Teil die Verschlüsselungsstärke beschreibt. Das Einsteckmodul wird implementiert, um diese Daten automatisch vom Browser zu erhalten, so dass sie zum Ermitteln verwendet werden können, ob das Sicherheitsniveau für eine vorgeschlagene Übertragung ausreicht oder nicht. Ebenso bestimmt bei einer Email-Nachricht das Einsteckmodul die Verschlüsselungseinstellungen, die der Benutzer oder die Anwendung vor der Übertragung der Nachricht zur Verwendung vorgegeben hat.

[0245] Das Modul vergleicht die vorgegebene Verschlüsselungsstärke mit der der Verbindung oder der Nachricht und führt je nach dem Ergebnis des Vergleichs eine der folgenden Aktionen aus:

a) wenn die Sicherheit der Verbindung für die Natur der übertragenen Informationen geeignet ist, dann lässt das Modul die Übertragung der Informationen zu;

b) wenn die Sicherheit der Verbindung höher ist als für die Übertragung der Informationen erforderlich, dann kann das Modul entweder die Übertragung der Informationen auf diesem Sicherheitsniveau zulassen, mit dem Webserver und dem Webbrowser automatisch ein neues geeignetes Sicherheitsniveau negoziieren und die Informationen auf diesem Niveau übertragen oder den Benutzer darauf hinweisen, dass das vorliegende Sicherheitsniveau unnötig ist, und ihn zur Durchführung einer Aktion auffordern;

c) wenn die Sicherheit der Verbindung für die Natur der übertragenen Informationen nicht ausreicht, dann kann das Modul entweder die Übertragung verhindern und den Benutzer warnen und auffordern, automatisch mit dem Webserver und dem Webbrowser ein neues geeignetes Sicherheitsniveau zu negoziieren und die Informationen dann auf diesem Niveau zu übertragen, oder im Falle einer Email automatisch die Einstellung der Verschlüsselungsstärke erhöhen oder den Benutzer anweisen, dass das vorliegende Sicherheitsniveau nicht ausreicht, und ihn auffordern zu bestätigen, dass er die Übertragung weiterhin wünscht.

[0246] Man wird verstehen, dass das Einsteckmodul auch so konfiguriert werden könnte, dass es auf eine Differenz zwischen dem ermittelten gewünschten Sicherheitsniveau und dem gegebenen auf verschiedene Weisen reagiert, und dass die oben erwähnten Aktionen lediglich illustrativ sind.

[0247] Weitere Maßnahmen, die das System ergreifen kann, könnten z. B. die Anforderung des Herunterladens einer anderen Webseite auf die Maschine des Benutzers oder das Modifizieren der submittierten Felddaten beinhalten, so dass empfindliche Informationen nicht übertragen werden.

[0248] Der Betrieb eines Browsers oder Email-Einsteckmoduls zum Überwachen der durch einen Benutzer des bevorzugten Systems übertragenen Daten ist in Fig. 18 illustriert, auf die nunmehr Bezug genommen werden sollte. Der Betrieb des Moduls beginnt mit Schritt S320 an Punkt C in Fig. 3 unmittelbar vor der Übertragung der Daten zu einem Webserver, oder an Punkt B in Fig. 5 unmittelbar vor der Übertragung einer Email. Die Steuerung geht dann zu Schritt S322, wo das Modul die vor der Übertragung stehenden Daten parst und nach Kreditkartennummern sucht. Ein mögliches Verfahren hierfür wurde zuvor mit Bezug auf Fig. 8 beschrieben. Wenn keine Kreditkartennummer in den Daten erkannt

wird, geht die Steuerung zu Schritt S314, wo das Modul nach Passwörtern in den vor der Übertragung stehenden Daten sucht. Ein Verfahren hierfür wurde oben mit Bezug auf Fig. 6 beschrieben. Wenn in den Daten kein Passwort gefunden wird, dann geht die Steuerung zu Schritt S316, wo das Modul nach Firmenkonten- oder Kaufcodes in den Daten sucht. Konten- oder Kaufcodes können erkannt werden, indem die Codes des Unternehmens in einer Datei gespeichert und versucht wird, diese Codes mit in den abgehenden Daten gefundenen Ziffernfolgen zu vergleichen. Wenn kein Kontencode gefunden wird, dann geht die Steuerung zu Schritt S318, wo das Modul nach Anzeichen für andere sensitive Daten in den vor der Übertragung stehenden Daten sucht. Solche Anzeichen müssen im Voraus definiert werden, vorzugsweise in einer zur Erfassung verwendeten separaten Datei, und ist von den Anforderungen der Benutzer des bevorzugten Systems abhängig. Beispiele könnten vorgegebene Schlüsselwörter über Projekte sein, die das Unternehmen durchführt, die Projekttitel selbst, persönliche Details wie die Adresse des Empfängers der Daten, oder des Senders, oder sogar das in den Daten selbst enthaltene Wort ‚vertraulich' oder ‚privat'.

[0249] Wenn keine solchen Anzeichen gefunden werden, dass die Daten sensitiv sind und einen stärkeren Schutz benötigen, bevor sie übertragen werden, dann wird die Übertragung auf dem aktuellen Verschlüsselungsniveau zugelassen. Dies kann bedeuten, dass die Übertragung stattfindet, ohne dass irgendeine Verschlüsselung angewendet wird.

[0250] Wenn jedoch einer der Checks in den Schritten S322 bis S328 Daten zu Tage bringt, die als sensitiv angesehen werden, dann geht die Steuerung zu Schritt S332, wo den erfassten Daten eine Sicherheitsbewertung zugewiesen wird. Dies wird durch Vergleichen der erkannten Daten mit vorbestimmten Einträgen in den Richtliniendaten erzielt.

[0251] Jeder Eintrag auf dem Zweig der Richtliniendaten hat ein zuvor zugewiesenes Verschlüsselungsniveau, das das Mindestniveau ist, das für die Übertragung dieser Daten benutzt werden darf. Die Einträge in der Tabelle und das zugewiesene Verschlüsselungsniveau werden, wie alle Richtlinieneinstellungen, von dem Unternehmen mit dem bevorzugten System in Abhängigkeit von deren Anforderungen entschieden. Die Zuweisung einer Sicherheitsbewertung ist dann einfach eine Sache des Nachschlagens von Passwort, Kreditkartennummer oder sonstigen Daten in den Richtliniendaten und das Ablesen der entsprechenden Bewertung. Verweise auf Tabellen auf einem Unterzweig der Richtliniendaten können zum Zuordnen verschiedener Verschlüsselungsstärken zu unterschiedlichen Passwörtern, Kreditkartennummern usw. verwendet werden.

[0252] Nach dem Ermitteln des geeigneten Sicherheitsniveaus in Schritt S332 geht die Steuerung zu Schritt S334, wo das Modul das Verschlüsselungsniveau erfasst, das mit dem Webserver negoziiert wurde, zu dem die Daten übertragen werden, oder das von der Email-Anwendung vor dem Übertragen der Nachricht anzuwenden ist. Dies kann durch Abfragen des Webbrowsers oder der Email-Anwendung oder durch Einstellen von Verschlüsselungsstärke-Variablen zu der Zeit erzielt werden, zu der die Verbindung hergestellt wird oder die Email-Verschlüsselungsanforderungen bestimmt werden, was beides vor der Übertragung stattfindet.

[0253] Die Steuerung geht dann zum Entscheidungsschritt S336, in dem das gewünschte Sicherheitsniveau, d. h. die Verschlüsselungsstärke, mit dem im vorangegangenen Schritt ermittelten verglichen wird. Wenn das gewünschte Verschlüsselungsniveau gleich oder niedriger ist als das in Schritt S334 ermittelte, dann wird dies als ein ausreichender Schutz für die zu übertragenden Daten angesehen und die Steuerung geht zum Endschritt S330, wo das Modul die Routine verlässt. Nach Schritt S330 kehrt die Steuerung entweder zu Punkt C in Fig. 3 oder zu Punkt B in Fig. 5 zurück, je nachdem, ob das Modul in einem Webbrowser oder einem Email-Client implementiert wird. Die Übertragung der Daten erfolgt dann in der gewöhnlichen Weise.

[0254] Wenn jedoch in Schritt S336 das gewünschte Verschlüsselungsniveau höher ist als das gerade eingestellte, dann lässt das Modul eine Übertragung erst dann zu, wenn das richtige Verschlüsselungsniveau negoziiert wurde. Die Steuerung geht dann zum Entscheidungsschritt S338, wo das Modul ermittelt, ob es die Verschlüsselungsstärke erhöhen kann, und wenn ja, dann geht die Steuerung zu Schritt S340, wo eine neue, stärker verschlüsselte Verbindung negoziiert oder, bei einer Email, eine höhere Verschlüsselungsstärke eingestellt wird.

[0255] Das höchste verfügbare Verschlüsselungsniveau hängt von der sowohl vom Webserver als auch vom Webbrowser verwendeten Software oder, im Falle einer Email, von der Email-Sende- und -Empfangsanwendung ab. Es kann dann Fälle geben, in denen das richtige Verschlüsselungsniveau für eine andere Partei nicht verfügbar ist und die Daten niemals übertragen werden können. Ferner können bestimmten Datentypen Sicherheitsbewertungen gegeben werden, die anzeigen, dass kein Verschlüsselungsniveau jemals für ihren Schutz ausreicht, d. h. es wird verhindert, dass Daten jemals übertragen werden.

[0256] Nachdem versucht wurde, die Verbindung erneut herzustellen oder die Email-Verschlüsselungseinstellungen auf eine höhere Verschlüsselungsstärke zu ändern, geht die Steuerung zurück zu

Schritt S334, um zu gewährleisten, dass die Verbindungen oder Einstellungen jetzt auf einer geeigneten Stärke sind. Wenn das geeignete Verschlüsselungsniveau in Schritt S338 nicht neu negoziiert werden kann oder ein Versuch, die Verschlüsselungsstärke in Schritt S340 zu erhöhen, nicht erfolgreich war, dann wird eine Übertragung der Daten als unsicher angesehen und die Steuerung geht zum Endschritt S342, wo das Modul die Routine verlässt. Nach dem Verlassen der Routine in Schritt S342 kehrt die Steuerung zu Punkt A in Fig. 3 oder zu Schritt S132 in Fig. 5, ‚Email verfassen', zurück, so dass der Benutzer die Übertragung neu betrachten und bearbeiten oder abbrechen kann. Dem Benutzer kann auch eine geeignete Nachricht angezeigt werden, die die Gründe für die Nichtübertragung erläutert.

[0257] Das bevorzugte System stellt somit einen Weg bereit, um zu gewährleisten, dass die Übertragung von Daten so sicher wie möglich ist. Es schließt die Möglichkeit aus, dass ein Benutzer vergisst, eine Übertragung zu sichern, und negoziiert ein geeigneteres Sicherheitsniveau, wenn das benutzte nicht ausreicht.

[0258] Webbrowser können ähnliche Einrichtungen bereitstellen, um den Benutzer zu warnen, dass bevorsteht, dass vom Benutzer eingegebene Daten über eine unsichere Verbindung gesendet werden, oder um Einrichtungen zum vorgabemäßigen Verschlüsseln aller Nachrichten bereitzustellen. Das bevorzugte System bietet jedoch die Möglichkeit, den Inhalt von zu übertragenden Daten zu untersuchen, um deren Sicherheitserfordernis zu ermitteln, die Übertragung auf der Basis solcher Sicherheitserfordernisse und des bestimmten Sicherheitsniveaus der Verbindung (Verschlüsselungsstärke) zuzulassen oder zu verhindern. Man wird verstehen, dass das bevorzugte System ein erheblich verbessertes System für sichere Übertragungen bereitstellt, das die Möglichkeit menschlicher Fehler reduziert.

Überwachung abgehender Emails auf sensitive Informationen

[0259] Zusätzlich zu dem Problem des Abfangens sensitiver Daten durch eine Drittpartei zwischen Sender und Empfänger besteht für Organisationen ein erhebliches Risiko einer absichtlichen Weitergabe sensitiver Informationen durch ihre Benutzer. So ist z. B. die Praxis des ‚elektronischen' Stehlens von Kopien vertraulicher Dokumente wie Kundenlisten durch einen Mitarbeiter einer Organisation, bevor er sie verlässt, eine einfache Sache, die praktisch nicht erkennbar und demzufolge weit verbreitet ist. Der Benutzer braucht dazu lediglich das Dokument zu seiner eigenen privaten Email-Adresse zum späteren Abrufen zu senden. Das Dokument braucht noch nicht einmal über das eigene Email-System der Organisation gesendet zu werden, da ein Internet-Mail-Service wie z. B. „Hotmail" verwendet werden kann, so dass das unautorisierte ‚Leck' mit derzeitigen Mitteln praktisch nicht ermittelt werden kann.

[0260] Zusätzlich zur Bereitstellung von Mitteln zum Gewährleisten, dass ein geeignetes Verschlüsselungsniveau auf Nachrichten angewendet wird, erlaubt das bevorzugte System die Identifikation von Nachrichten als potentiell sensitiv, um automatisch umgeleitet oder ohne Wissen des Benutzers auf einen anderen Zielort kopiert zu werden. Beim Ermitteln, ob solche Nachrichten umgeleitet werden sollen, berücksichtigt das bevorzugte System eine Reihe von Faktoren einschließlich der Identität des Senders, der Identität des beabsichtigten Empfängers, der Natur der Adressen der beabsichtigten Empfänger, der Natur des Nachrichteninhalts, der Natur und Existenz eventueller Nachrichtenanhänge, des Mittels, mit dem die Nachricht übertragen werden soll, und ob die Nachricht und/oder eventuelle Anhänge verschlüsselt sind oder nicht.

[0261] Die Natur der Nachricht kann durch Scannen der Nachricht nach einem oder mehreren Schlüsselwörtern oder Schlüsselwortkombinationen oder mit Hilfe von standardmäßigen ‚natürlichsprachliche Abfrage'-Techniken ermittelt werden. Die Natur der Adresse der beabsichtigten Empfänger kann durch Bezugnahme auf eine Liste von bekannten Internet-Mailservice-Bereichen ermittelt werden. So werden beispielsweise „hotmail.com", „yahoo.com" und „aol.com" alle vornehmlich von Personen und nicht von Unternehmen benutzt. Ebenso kann die Adresse nach Ähnlichkeiten mit dem Namen des Senders untersucht werden. So könnte z. B. eine Email, die bekanntlich von Fred Smith zur Adresse „smith900@aol.com" gesendet wird, durch den Einschluss sowohl von „smith" als auch „aol.com" in der Empfängeradresse als verdächtig angesehen werden. Eine weitere Untersuchung der Nachricht kann die Wahrscheinlichkeit unterstützen, dass dies eine unautorisierte Weitergabe von vertraulichen Daten ist, z. B. dann, wenn die Nachricht nur aus Dateianhängen besteht und der Nachrichtentext und die Betreffzeile leer gelassen wurden, ein wichtiger Hinweis, weil es wenig wahrscheinlich ist, dass der Sender Text eingeben wird, den nur er lesen wird. Die Mittel, mit denen die Nachricht übertragen wird, sind ein wichtiger Faktor, so kann beispielsweise eine mit einem Internet-Mailservice wie Hotmail gesendete Übertragung weitaus verdächtiger sein als eine Nachricht, die über das gewöhnliche Firmenemailsystem gesendet wird.

[0262] In der Tat ist das ‚Heraufladen' von Dateien auf einen Internet-Mailservice potentiell so verdächtig, dass die bevorzugte Ausgestaltung Mittel enthält, um das Heraufladen von Dateien auf solche Dienste ganz zu verbieten.

[0263] Beim Umleiten von Mail fügt das bevorzugte System zusätzlichen Text zum Anfang der Mail hinzu, z. B. „----Redirected Mali----", zusammen mit den Adressen der ursprünglich beabsichtigten Empfänger, so dass der neue Empfänger feststellen kann, dass die Nachricht zu ihm umgeleitet wurde, sowie den Empfänger, zu dem sie ursprünglich gesendet wurde.

[0264] Wenn die weitergeleitete Nachricht verschlüsselt werden soll, dann kann das bevorzugte System die Nachricht verschlüsselt oder unverschlüsselt zu der Drittpartei weiterleiten. Der Verschlüsselungskey des Senders wird vorzugsweise mit der Nachricht gesendet und es sind Mittel vorgesehen, damit die Drittpartei die Nachricht entschlüsseln kann, wenn sie bereits verschlüsselt war, und die Nachricht mit dem Verschlüsselungskey des ursprünglichen Senders zur Übertragung verschlüsseln kann.

[0265] Das bevorzugte System identifiziert auch eingehende Mails, die umgeleitet wurden (d. h. zu einem Benutzer gesendet wurden, der nicht der ursprünglich beabsichtigte Empfänger ist), indem der Text nach „----Redirected Mail----" durchsucht wird. Auf eine solche Mail kann der neue Empfänger beispielsweise mit speziellen Icons aufmerksam gemacht werden, oder es kann eine Nachrichtenbox eingeblendet werden, um ihn zu benachrichtigen. Es können auch Mittel vorgesehen werden, um es zuzulassen, dass der neue Empfänger die Nachricht leicht ‚genehmigt' und sie zu dem/den ursprünglich beabsichtigten Empfänger(n) senden lässt. Dies kann beispielsweise dadurch erzielt werden, dass eine „Zulassen"-Schaltfläche vorgesehen wird. Wenn auf diese Schaltfläche geklickt wird, dann erzeugt das bevorzugte System eine neue Nachricht auf dieselbe Weise, als wenn der Benutzer auf die normale „Weiterleiten"-Schaltfläche geklickt hätte. Anstatt des Hinzufügens von Text zu der Nachricht, um darauf hinzuweisen, dass sie weitergeleitet wurde, extrahiert das System jedoch im Falle der „Zulassen"-Schaltfläche die Liste der ursprünglich beabsichtigten Empfänger aus der Nachricht und zieht dann die Umleitungsdetails heraus, um die Nachricht in ihrem ursprünglichen Zustand zu lassen. Die Zielfelder „An", „Cc" und „Bcc" werden dann automatisch mit den extrahierten Adressen der ursprünglichen Empfänger ausgefüllt, und das „Von"-Feld (das für jede Nachricht existiert, selbst dann, wenn sie nicht normal angezeigt wurde) wird mit dem Namen/der Adresse des ursprünglichen Senders ausgefüllt. Das Datum/Zeit-Feld kann auch das/die Datum/Uhrzeit der ursprünglichen Nachricht eingestellt werden. Dann wird die Nachricht gesendet, entweder automatisch oder wenn der Benutzer die „Senden"-Schaltfläche drückt. Auf diese Weise kann durch Anklicken von nur einer oder zwei Schaltflächen die umgeleitete Mail zugelassen und gesendet werden, und erscheint nach der Ankunft wie vom ursprünglichen Empfänger gekommen, so als wenn keine Umleitung stattgefunden hätte.

[0266] Beispielhafte Richtliniendaten zum Steuern des Betriebs eines zum Umleiten von Mail implementierten Einsteckmoduls sind in Fig. 19 dargestellt, eine beispielhafte Illustration des Betriebs eines solchen Einsteckmoduls ist in Fig. 20 dargestellt. Fig. 19 ist ein Richtliniendatenbaum mit einer Reihe von Zweigen, die Entscheidungsschritten in Fig. 20 entsprechen.

[0267] Das Einsteckmodul wird in Schritt S350 gestartet, der Punkt B in der Illustration des Betriebs des Email-Client in Fig. 5 entspricht. Nach dem Starten durchläuft das Einsteckmodul sechs Schritte, die verschiedene Details der abgehenden Email-Nachricht ermitteln. Erstens, in Schritt S351 wird die Identität der die Email sendenden Person mit Einträgen in einer vorbestimmten Liste von Namen und Adressen geprüft. Emails von Benutzern auf dieser Liste werden so angesehen, dass sie die Autorität haben, Emails direkt zum beabsichtigten Empfänger unabhängig vom Inhalt der Nachricht und unabhängig vom Empfänger zu übertragen. Die Emails von jedem, der nicht auf der Liste aufgeführt ist, können je nach ihrem Inhalt umgeleitet werden oder auch nicht. So geht die Steuerung im Entscheidungsschritt S351, wenn der Name oder die Adresse des Benutzers auf der Liste steht, zu Schritt S364, wo zugelassen wird, dass die Email ohne weitere Interaktion übertragen wird. Wenn der Benutzer jedoch nicht auf der Liste steht, dann geht die Steuerung zu Schritt S253 für weitere Checks. In Schritt S352 wird der Empfänger der abgehenden Email-Nachricht anhand der Lookup-Tabelle s gemäß den auf dem Recipients-Zweig der in Fig. 19 gezeigten Richtliniendaten geprüft. Im nachfolgenden Entscheidungsschritt S354 werden der die Email-Nachricht umfassende Text und eventuelle Anhänge an der Email-Nachricht mit Einträgen in einer Lookup-Tabelle t verglichen. Auf Tabelle t wird im Keywords-Zweig der Richtliniendaten verwiesen und sie enthält Wörter, die anzeigen, dass die Natur der Email-Nachricht möglicherweise für das Unternehmen sensitiv ist. Im nächsten Schritt S356 wird die Email-Nachricht geprüft, um zu sehen, ob sie verschlüsselt werden muss oder nicht. Man wird sich erinnern, dass eine Verschlüsselung erst dann erfolgt, wenn die Email übertragen wird, daher wird in dieser Phase die Email nur zur Verschlüsselung markiert. Im nächsten Entscheidungsschritt S358 wird ermittelt, ob die Email-Nachricht Anhänge enthält oder nicht, und im folgenden Entscheidungsschritt S360, ob die Email-Nachricht Text zum Begleiten der Anhänge enthält, d. h. ob das Haupttextfeld der Email-Nachricht leer ist.

[0268] In jedem der Entscheidungsschritte S352, S354 oder S362, wo eine Lookup-Tabelle konsultiert wird, bedeutet eine Übereinstimmung zwischen ei-

nem Eintrag in der Lookup-Tabelle und einem Eintrag in der Email, dass die Email zu einer Drittpartei zwecks Prüfung umgeleitet werden soll, bevor sie aus dem Unternehmen hinaus gesendet wird. Wenn beispielsweise in Schritt S354 gefunden wird, dass die Email die Wörter ‚vertraulich' oder ‚geheim' enthält, dann reicht dies als Rechtfertigung dafür aus, dass die Email von einer Drittpartei geprüft wird, bevor sie zum beabsichtigten Empfänger geliefert wird. Dies stellt sicher, dass keine sensitiven Informationen ohne Kenntnis des Unternehmens aus diesem hinausgesendet werden. Die Steuerung geht daher von diesen Schritten zu Schritt S364, wo Text, der anzeigt, dass die Email umgeleitet wurde, 'zur Nachricht hinzugefügt wird, und die Empfängeradresse wird auf die der verifizierenden Partei geändert, zu der die umgeleitete Nachricht gesendet werden soll. Die Steuerung geht dann zu Schritt S366, wo die Email übertragen wird. Wenn die Email-Nachricht in Schritt S336 zum Umleiten markiert wurde, dann wird sie natürlich zur verifizierenden Partei zur Überprüfung anstatt zum ursprünglichen Empfänger der Nachricht gesendet.

[0269] Im Entscheidungsschritt S356 wird, wenn eine Verschlüsselung der Nachricht erfasst wird, dies als ausreichend angesehen, um das Umleiten der Nachricht zu einer Drittpartei zur Überprüfung zu rechtfertigen. Demgemäß geht die Steuerung, wenn die Nachricht verschlüsselt werden soll, von Schritt S356 zu Schritt S364, wo die Nachricht zum Umleiten modifiziert wird. Im Falle einer zur Verschlüsselung markierten Nachricht wird der Verschlüsselungsflag vorzugsweise weggenommen, so dass die Nachricht umgeleitet wird, ohne verschlüsselt zu werden, damit sie der neue Empfänger lesen kann. Der der Nachricht hinzugefügte Umleitungstext enthält vorzugsweise auch den Verschlüsselungskey (der im Allgemeinen der Public-Key des beabsichtigten Empfängers und daher nicht sensitiv ist), so dass die Nachricht vor dem Übertragen neu verschlüsselt werden kann.

[0270] Alternativ könnte das gesamte digitale Zertifikat des beabsichtigten Empfängers in der umgeleiteten Nachricht enthalten sein. Der Public-Key oder das Zertifikat, je nachdem, würde dann durch den oben beschriebenen automatisierten Zulassungsprozess entfernt.

[0271] Wenn die Email in Schritt S358 keine Anhänge enthält, dann wird die Email so angesehen, dass sie wahrscheinlich keine Dokumente oder Dateien mit potentiell sensitiven Informationen enthält, und es wird zugelassen, dass die Email ohne weitere Eingriffe in Schritt S364 übertragen wird. Wenn die Email Anhänge enthält und in Schritt S360 ermittelt wird, dass die Email im Hauptteil oder im Betreff der Nachricht keinen Text enthält, dann wird die Nachricht als eine erkannt, die wahrscheinlich zu einem anderen Konto des Senders gesendet wird. Die Email wird dann in Schritt S362 und S364 zum Prüfen zu einer Drittpartei weitergeleitet.

[0272] Fig. 21 zeigt den Betrieb des Einsteckmoduls zum Sperren des Heraufladens von Informationen vom Computersystem des Unternehmens zu einer externen Site. Es erfolgt ein einfacher zweistufiger Check, der einen Check der externen Site-Adresse in S372 nach dem Start in Schritt S370 und einen Check von sensitiven Schlüsselwörtern in den in Schritt S374 heraufgeladenen Informationen enthält. Vorausgesetzt, die externe Site-Adresse wird in Schritt S373 nicht als eine verbotene Site ermittelt und es werden in Schritt S374 keine sensitiven Schlüsselwörter erfasst, wird das Heraufladen in Schritt S376 zugelassen, sonst wird das Heraufladen in Schritt S378 gesperrt.

[0273] Die Richtliniendaten zum Steuern des Betriebs des Einsteckmoduls zum selektiven Sperren des Heraufladens von Informationen sind einfach und sind unten in Fig. 19 aufgeführt.

[0274] Auf diese Weise können abgehende Übertragungen, die sensitive Informationen enthalten, die aus nicht im Interesse des Unternehmens liegenden Gründen übertragen werden sollen, vor der Übertragung verifiziert und eine Übertragung falls nötig verhindert werden.

Verwalten des Weiterleitens von Emails

[0275] Email-Anwendungen bieten ein Mittel zum ‚Weiterleiten' eingehender Mails zu einem oder mehreren Benutzern. Der Benutzer klickt typischerweise eine „Weiterleiten"-Schaltfläche an, die bewirkt, dass eine Kopie der eingehenden Mail automatisch in das Mail-Verfassungsfenster eingegeben wird, so als wenn sie der Benutzer selbst eingetastet hätte. Dann braucht der Benutzer lediglich die Namen der beabsichtigten Empfänger der weitergeleiteten Mail einzugeben und die „Senden"-Schaltfläche anzuklicken. Dies ist ein nützliches Merkmal, mit dem ein Benutzer den Inhalt einer empfangenen Email leicht mit anderen gemeinsam nutzen kann.

[0276] Ein Problem kann jedoch im Falle einer Mail entstehen, die sensitive Informationen enthält, besonders dann, wenn die sensitive Natur der Mail nicht sofort offensichtlich ist, z. B. dann, wenn die sensitiven Informationen weiter unten in der Email erscheinen, so dass der Benutzer durch das Betrachtungsfenster rollen muss, um sie zu lesen. Benutzer leiten Emails häufig weiter, sobald sie die ersten paar Zeilen, oder in einigen Fällen auch nur die Betreffzeile, gelesen haben, besonders dann, wenn sie große Mengen an Emails verarbeiten müssen. Demzufolge werden sensitive Informationen häufig unabsichtlich weitergegeben, sowohl innerhalb als auch, was noch

gefährlicher ist, außerhalb der Organisation. Es hat mehrere High-Profile-Fälle gegeben, bei denen infolgedessen erhebliche Summen verloren gegangen sind.

[0277] Das bevorzugte System stellt daher Mittel zum Steuern des Weiterleitens von Emails bereit. Zu solchen Steuerfunktionen gehören Warnhinweise für den Benutzer, bevor eine weitergeleitete Email übertragen wird, und das Verhindern, dass die Email überhaupt weitergeleitet wird. Es können auch Mittel vorgesehen werden, um die Email vor der Übertragung zuzulassen oder um zu einem anderen Benutzer umzuleiten, wie oben beschrieben.

[0278] Eine Weiterleitung erfolgt vorzugsweise gemäß dem Inhalt der Email und der Adressen der Empfänger, zu denen sie bereits gesendet wurde. So kann beispielsweise die sensitive Natur der Email mit einer Reihe von Methoden ermittelt werden, wie z. B. Scannen nach Schlüsselwörtern wie „vertraulich" oder Prüfen, ob das Sensitivitätsattribut auf „persönlich", „privat" oder „vertraulich" gesetzt ist. Mittel für den ursprünglichen Verfasser der Nachricht, diese als für eine spätere Weiterleitung ungeeignet zu markieren, werden ebenfalls durch Einfügen vorbestimmter Zeichenketten bereitgestellt, wie z. B. „<NOFORWARD>" (was jede Weiterleitung verhindert) oder „<NOFORWARDEXTERNAL>" (was eine Weiterleitung außerhalb der Organisation verhindert). Solche Mittel könnten auch in Form eines zusätzlichen Attributs zu der Nachricht vorgesehen werden.

[0279] Zusätzlich zu inhaltsgestützten Faktoren fragt das bevorzugte System die Liste von vorherigen Empfängern der Nachricht ab. Wenn die Email bereits vom ursprünglichen Verfasser aus der Organisation hinaus gesendet wurde, dann kann sie beispielsweise als sicher angesehen werden, so dass sie auch weiter extern weitergeleitet werden kann. Ebenso kann festgestellt werden, wenn die ursprüngliche Email nur zu einem einzigen Empfänger gesendet wurde, dass der ursprüngliche Verfasser keine große Verbreitung beabsichtigt, und es kann eine entsprechende Warnung ausgegeben werden. Der Aktionsverlauf als Reaktion auf die beschriebenen Faktoren kann im Einklang mit den Richtlinien bestimmt werden.

[0280] Die Tatsache, dass eine Email, die vor der Übertragung steht, eine weitergeleitete Email ist, kann leicht durch Absuchen der Email nach Zeichenketten wie „----Original Message----„ festgetellt werden, die automatisch zu Beginn der ursprünglichen Mail vom Email-Programm hinzugefügt wird. Ebenso kann die Liste früherer Empfänger durch Scannen nach den Zeichenketten „An:" und „Cc:" ermittelt werden, die auf die ursprüngliche Nachrichtenfolge folgen. Die Liste von Empfängern befindet sich unmittelbar hinter diesen Zeichenketten. Interne und externe Empfänger können leicht anhand der Bereichsnamen (ggf.) unterschieden werden. So ist beispielsweise ein Empfängername „Fred Smith" gewöhnlich intern, während „fsmith@xyz.com typischerweise extern ist.

[0281] Richtliniendaten zum Anweisen des Betriebs eines implementierten Einsteckmoduls zum Steuern des Weiterleitens von Email-Nachrichten sind in Fig. 22 dargestellt, der Betrieb eines solchen Moduls in Fig. 23.

[0282] Der Richtliniendatenbaum enthält eine Reihe von Unterzweigen, die Parameter vorgeben, anhand derer Befehlswerte eingestellt werden können. So weist beispielsweise der erste Unterzweig „PreventAll", wenn er auf ‚JA' gesetzt ist, das Modul an, die Weiterleitung aller Emails zu verhindern. Der nächste Unterzweig WarnAll verlangt, wenn er auf JA gesetzt ist, dass das Modul dem Email-Client-Benutzer immer einen Warnhinweis gibt, wenn eine Email vor der Weiterleitung steht. Die nächsten beiden Unterzweige PreventExternal und WarnExternal enthalten entsprechende Parameter nur für externe Emails und lassen es zu, dass der Benutzer des Email-Client zwischen Regeln, die das Weiterleiten von Emails innerhalb des Unternehmens beeinflussen, und solchen unterscheidet, die das Weiterleiten von Emails zu Personen außerhalb des Unternehmens betreffen. Der „PreventKeywords"-Zweig gibt eine Lookup-Tabelle vor, in der Schlüsselwörter gespeichert sind, die sensitive Informationen anzeigen. Solche Schlüsselwörter können vordefinierte Zeichenketten wie <NOFORWARD> oder <NOFORWARDEXTERNAL> oder ein oder mehrere vorbestimmte Wörter sein.

[0283] Die Email wird vor der Übertragung gescannt und wenn ein Schlüsselwort im Text der Email oder in einem der Anhänge der Email gefunden wird, dann wird eine Weiterleitung der Email nicht zugelassen. Die letzten beiden Unterzweige PreventIfNotSentExternally verhindern, wenn sie auf JA gesetzt sind, eine Übertragung der weitergeleiteten Email außerhalb des Unternehmens, wenn sie bis dahin noch nie außerhalb des Unternehmens übertragen wurde. In der Praxis kann die weitergeleitete Email zu allen Empfängern innerhalb des Unternehmens gesendet werden und die externen Empfänger werden einfach aus der Empfängerliste gelöscht, alternativ kann vom Benutzer verlangt werden, die Adressliste vor der Übertragung so zu ändern, dass sie keine externen Empfänger enthält.

[0284] Schließlich verhindert der Parametersatz auf dem PreventIfSingleRecipient-Zweig, wenn er auf JA gesetzt ist, eine Weiterleitung von Email-Nachrichten, wenn der ursprüngliche Empfänger der Nachricht eine Einzelperson war.

[0285] Der Betrieb des Einsteckmoduls ist in Fig. 23 illustriert. Das Einsteckmodul wird in Schritt S380 gestartet, wieder an Punkt B in Fig. 5. Im Entscheidungsschritt S382 wird die Email vorgescannt, um zu sehen, ob sie die Zeichenkette „----Original Message----„ enthält, da diese Zeichenkette automatisch zu Beginn der ursprünglichen Mail vom Email-Programm beim Erzeugen einer Nachricht zum Weiterleiten hinzugefügt wird. Wenn die Email-Nachricht diese Zeichenkette nicht enthält, dann kann davon abgeleitet werden, dass die Email-Nachricht eine ursprüngliche Nachricht ist und nicht weitergeleitet wird, und die Nachricht kann in Schritt S384 übertragen werden.

[0286] Wenn jedoch in Schritt S382 gefunden wird, dass die Nachricht die Zeichenkette „----Original Message----„ enthält, dann ist klar, dass die Email-Nachricht eine weitergeleitete Nachricht ist und das Modul unternimmt weitere Schritte, um zu ermitteln, ob es die Übertragung der weitergeleiteten Nachricht zulassen soll oder nicht. Die Steuerung geht dann zu Schritt S386, wo die Empfänger der weitergeleiteten Nachricht geprüft werden, um zu sehen, ob einige davon extern zu dem Online-Unternehmen sind. Wenn es einen externen Empfänger gibt, dann scannt das Einsteckmodul in Schritt S388 die Email-Nachricht, um zu sehen, ob die Email schon einmal zu einem Empfänger außerhalb des Unternehmens weitergeleitet wurde. Wenn nicht, dann wird in Schritt S390 verhindert, dass die Nachricht weitergeleitet wird, und der Benutzer des Email-Client wird benachrichtigt. Wenn die Email-Nachricht jedoch bereits einmal aus dem Unternehmen hinaus gesendet wurde, dann wird dem Benutzer in Schritt S392 ein Warnhinweis gegeben, wonach die Email-Nachricht entweder vom Benutzer übertragen oder zwecks Revision der beabsichtigten Empfänger zum Benutzer zurückgesendet werden kann.

[0287] Wenn die weitergeleitete Nachricht in Schritt S386 nicht zu einer Adresse außerhalb des Unternehmens gesendet werden soll, dann geht die Steuerung zu Schritt S394, wo ermittelt wird, ob der Benutzer der einzige Empfänger der ursprünglichen Nachricht war. Wenn ja, dann kann es der Fall sein, dass der ursprüngliche Verfasser der Nachricht nicht beabsichtigt hat, dass diese weit verbreitet werden soll. Demgemäß geht die Steuerung zu Schritt S390, wo die Übertragung der weitergeleiteten Email-Nachricht gesperrt wird. Dies entspricht den in Fig. 22 gezeigten Richtliniendaten, die eine solche Aktion vorgeben.

[0288] Alternativ kann ein Warnhinweis an den Benutzer ausgegeben werden, der versucht, die Nachricht weiterzuleiten.

[0289] Der letzte Check erfolgt im Entscheidungsschritt S396, wo der Inhalt der Nachricht und eventueller Anhänge daran mit Einträgen in einer Schlüsselworttabelle verglichen werden. Wenn es Übereinstimmungen zwischen Einträgen in der Email und denen in der Tabelle gibt, dann wird die Nachricht so angesehen, dass sie sensitive Informationen enthält, und wird nicht weitergeleitet. Das Modul endet dann in Schritt S390. Wenn keine sensitiven Schlüsselwörter gefunden werden, dann wird zugelassen, dass die Email in Schritt S384 weitergeleitet wird.

Verwalten des Signierens von abgehenden Übertragungen

[0290] Die Möglichkeit, ein digitales Zertifikat zum Signieren einer Nachricht zu benutzen, ist für den Empfänger der Nachricht beim Feststellen der Identität des Senders und für beide Parteien beim Sicherstellen, dass nicht betrügerisch in die Nachricht eingegriffen wurde, deutlich wertvoll. Der Sender der Nachricht sollte sich jedoch der Tatsache bewusst sein, dass eine digital signierte Nachricht potentiell einen bindenden Vertrag darstellt, der nach dem Senden nicht verweigert oder widerrufen werden kann. Es ist daher zwingend notwendig, beim digitalen Signieren eines Dokuments vorsichtig zu sein, genau wie wenn eine schriftliche Unterschrift auf ein Papierdokument gesetzt wird. Email-Anwendungen wie z. B. „Gutlook" von Microsoft bieten Mittel, um Nachrichten automatisch digital zu signieren, und während dies aus den oben beschriebenen Gründen für den Empfänger zum Bestätigen der Identität des Senders wertvoll ist, ist es auch potentiell gefährlich und verlangt vom Benutzer äußerste Vorsicht beim Umgang mit dem Nachrichteninhalt.

[0291] Das bevorzugte System stellt Mittel zum Steuern des Signierens von abgehenden Nachrichten gemäß Richtliniendaten bereit. Fig. 24 zeigt ein Beispiel für Richtliniendaten. Zu solchen Steuerungen gehören:
das Erzwingen des Signierens einer Nachricht;
das Nahelegen dem Benutzer, dass eine Nachricht signiert werden sollte;
das Nahelegen dem Benutzer, dass eine Nachricht NICHT signiert werden sollte; und
das Verhindern des Signierens einer Nachricht.

[0292] Beim Feststellen des durchzuführenden Aktionsverlaufs berücksichtigt das bevorzugte System eine Reihe von Faktoren, einschließlich der Natur des Nachrichteninhalts (einschließlich eventueller Anhänge), der Identität des beabsichtigten Empfängers und/oder seiner Organisation, der Identität des Senders, der Natur des verwendeten digitalen Zertifikats (ob die Nachricht bereits für eine Signatur markiert wurde) und der Natur des/der digitalen Zertifikats/e, das/die zum Signieren der Nachricht zur Verfügung steht/stehen.

[0293] Die Natur der Nachricht kann durch Scannen der Nachricht nach einem oder mehreren Schlüsselwörtern oder Schlüsselwortkombinationen oder durch Anwenden von standardmäßigen ‚natürlichsprachliche Abfrage'-Techniken ermittelt werden. Ebenso kann die Natur der beabsichtigten oder verfügbaren digitalen Zertifikate durch Bezugnahme auf den Ausgeber und den Typ des Zertifikats ermittelt werden.

[0294] Fig. 25 illustriert den Betrieb eines Einsteckmoduls zum Sicherstellen, dass eine Email ordnungsgemäß digital signiert wird. Das Modul wird in Schritt S400 an Punkt B in dem in Fig. 5 illustrierten Betrieb des Email-Client gestartet. Die Steuerung geht dann zum Entscheidungsschritt S402, wo die abgehende Email gescannt wird, um zu sehen, ob sie bereits zur Signatur markiert wurde. Das eigentliche ‚Signieren' der Nachricht erfolgt erst unmittelbar vor der Übertragung. Wenn sie nicht für eine Signatur markiert wurde, dann geht die Steuerung zu Schritt S404, wo das Modul in einer Empfänger-Lookup-Tabelle (Tabelle f) nachschlägt, um zu ermitteln, ob der Empfänger der abgehenden Email als einer identifiziert ist, zu dem Emails immer digital signiert werden müssen. Wenn der Empfänger in Tabelle f aufgeführt ist, dann geht die Steuerung zu Schritt S406, wo der Benutzer des Email-Client benachrichtigt wird, dass die Email nur dann gesendet wird, wenn sie digital signiert wird. Alternativ kann das Einsteckmodul die Email mit dem digitalen Zertifikat des Email-Autors automatisch digital signieren.

[0295] Wenn der Empfänger der abgehenden Email in Schritt S404 nicht in der Lookup-Tabelle steht, dann geht die Steuerung zum Entscheidungsschritt S408, wo die Keywords-Tabelle auf dem EnforceSigning-Zweig des Richtlinienbaums befragt wird. Falls die Schlüsselwörter aus Tabelle g im Text der Email oder in einem der Anhänge der Email stehen, dann ist eine digitale Signatur der Email erforderlich und die Steuerung geht wie zuvor zu Schritt S406. Man wird verstehen, dass die Entscheidungsschritte S404 und S406 Lookup-Befehlen zum Nachschlagen in den Recipients- und Keywords-Lookup-Tabellen auf dem EnforceSigning-Zweig der Richtliniendaten entspricht.

[0296] Solche Schlüsselwörter können vorbestimmte Wörter wie „vertraulich", „geheim", „Vertrag", „Angebot", „Auftrag" usw. wie in Fig. 24 illustriert sein.

[0297] Wenn die Empfänger der Email nicht in Tabelle f stehen und die Email keine in Tabelle g aufgeführten Schlüsselwörter enthält, dann geht die Steuerung zum Entscheidungsschritt S410, der einem Lookup-Befehl auf dem SuggestSigning-Zweig des Richtliniendatenbeispiels entspricht. Im Entscheidungsschritt S410 wird die Adresse des Empfängers mit der in der Lookup-Tabelle h verglichen, um zu ermitteln, ob eine Signierung der Email angeraten ist. Wenn der Name des Empfängers in Tabelle h steht, dann geht die Steuerung zu Schritt S412, wo der Benutzer des Email-Client benachrichtigt wird, dass eine digitale Signierung der abgehenden Email-Nachricht wünschenswert ist. Es ist aber nicht unbedingt erforderlich, dass der Benutzer des Email-Client die Email-Nachricht digital signiert, und die Email kann daher ohne Signatur übertragen werden, wenn der Benutzer dies wünscht. Nach dem Entscheidungsschritt S410 geht die Steuerung, wenn der Name des Empfängers nicht in Tabelle h steht, zum Entscheidungsschritt S414, wo der Email-Text wie zuvor nach einer Reihe von Schlüsselwörtern durchsucht wird, die anzeigen könnten, dass er sensitive Daten enthält und eine digitale Signatur benötigt. Je nachdem, ob die Email solche sensitiven Schlüsselwörter enthält, wird der Benutzer des Email-Client entweder in Schritt S412 benachrichtigt, dass es wünschenswert ist, die Nachricht digital zu signieren, oder alternativ wird die Email-Nachricht in Schritt S416 ohne Signatur übertragen.

[0298] Wenn in Schritt S402 nach dem Starten des Einsteckmoduls gefunden wird, dass die Email für eine Signatur markiert wurde, dann geht die Steuerung zum Entscheidungsschritt S418. Im Entscheidungsschritt S418 konsultiert das Einsteckmodul die Lookup-Tabelle m im DenySigning-Zweig, vorgegeben unter dem DenySigning-Zweig der Richtliniendaten. Tabelle m ist auf dem CertificatesUsed-Zweig unter dem DenySigning-Zweig vorgegeben und gibt den Aussteller, den Typ, die Zertifikatnummer oder den Signierungskey der digitalen Zertifikate an, die als von Interesse angesehen werden. Falls sich das digitale Zertifikat oder der Signierungskey, das/der zum Signieren der abgehenden Email benutzt werden soll, in Tabelle m befindet, erfolgen weitere Checks in Bezug auf den Empfänger und die Natur der abgehenden Email, um zu ermitteln, ob eine Signierung der Nachricht angemessen ist oder nicht. Die Steuerung geht zu Schritt S420, wo der Empfänger der abgehenden Email anhand der Recipient-Tabelle n geprüft wird, und dann zum Entscheidungsschritt S422, wo der Text der Email und eventuelle Anhänge nach verschiedenen Schlüsselwörtern abgesucht werden. Wenn in einem der Entscheidungsschritte S420 oder S422 der Empfänger oder ein eventueller Text in der Nachricht mit dem in den Lookup-Tabellen definierten übereinstimmt, dann geht die Steuerung zu Schritt S424, wo die Übertragung der Email gesperrt wird. Der Benutzer des Email-Client kann dann zur Email-Texteingabestufe zurückgeführt werden und es kann von ihm verlangt werden, die Nachricht ohne digitale Signierung neu zu übertragen.

[0299] Wenn in einem der Schritte S418 oder S422 gefunden wird, dass das Zertifikat oder der Signierungskey nicht von Interesse ist, und wenn im Text der Email keine sensitiven Wörter gefunden werden,

dann geht die Steuerung zu Schritt S426, der dem ersten Unterzweig auf dem SuggestNotSigning-Zweig des Richtliniendatenbaums entspricht. Was den DenySigning-Zweig des Richtliniendatenbaums angeht, so entsprechen die drei Entscheidungsschritte S426, S428 und S430 den Lookup-Befehlen zum Prüfen des mit der Email verwendeten digitalen Zertifikats oder Signierungskeys, des Empfängers der abgehenden Email und des Texts der abgehenden Email mit vorbestimmten sensitiven Einträgen jeweils in den Lookup-Tabellen j, k und l. Wenn gefunden wird, dass das zum Signieren der abgehenden Email benutzte Zertifikat in Schritt S426 von Interesse ist, und wenn in Schritt S426 oder in Schritt S430 gefunden wird, dass der Empfänger oder der Text der abgehenden Email mit Einträgen in den vorgegebenen Lookup-Tabellen übereinstimmt, dann geht die Steuerung zu Schritt S432, wo der Benutzer des Email-Client benachrichtigt wird, dass es wünschenswert ist, die abgehende Email-Nachricht nicht digital zu signieren. Der Benutzer kann die signierte Email-Nachricht jedoch weiterhin senden, wenn er dies wünscht.

[0300] Wenn in einem der Entscheidungsschritte S426, S428 und S430 keine Übereinstimmung gefunden wird, dann wird die Email in Schritt S416 normal gesendet.

Instant-Messaging- und Telefonieanwendungen

[0301] Zusätzlich zu Browser- und Email-Aktivitäten werden auch zusätzliche Anwendungen wie Instant Messaging (auch als ‚Chatten' bekannt) und digitale Telefonieanwendungen (wie „Voice Over OP") in Geschäftssituationen immer populärer. Instant-Messaging-Standards sind in RFC 2778 und 2779 und von der IETF SIMPLE Arbeitsgruppe definiert. Voice Over-IP-Standards sind in der ITU-T Empfehlung H.323 (1998) definiert. Viele Aspekte der vorliegenden Erfindung können auf von solchen Anwendungen gesendete und empfangene Daten angewendet werden. Instant Messaging ist von der Idee her einer Reihe von gesendeten und empfangenen Emails ähnlich, mit der Ausnahme, dass die ‚Konversation' ‚live' erfolgt, wobei beide Parteien ständig anwesend sind. Für die Zwecke der vorliegenden Erfindung sind die Prozeduren jedoch identisch. Fig. 5 der Zeichnungen kann Instant Messaging durch Ersetzen des Wortes „Email" in den Schritten S122, S124, S132 und S134 durch das Wort „Nachricht" repräsentieren. Die „Email-Server"-Beschreibung **95** wird durch „Nachrichtenrelais" ersetzt. Die bevorzugte Ausgestaltung ist zum Abfangen an den Punkten A und B wie zuvor gestaltet, indem ein Einsteckmodul zur Internet Messaging Anwendung bereitgestellt oder indem eine Instant Messaging Anwendung entwickelt wird, die die Einsteckfunktionalität enthält. Alternativ wird man verstehen, dass das Abfangen auf Protokollebene erfolgen könnte, wobei Netzwerkpakete abgefangen werden, bevor sie die Benutzermaschine verlassen oder wenn sie an der Benutzermaschine ankommen.

[0302] VOIP (Voice Over Internet Protocol) ist vom Konzept her dem Instant Messaging ähnlich, mit der Ausnahme, dass der Nachrichteninhalt aus digitalisierter Sprache besteht, die codiert und sofort übertragen wird. Eine Analyse des Nachrichteninhalts ist unpraktisch, aber Mittel zum Aufzeichnen der Nachricht und zum Setzen von Controls auf ‚Anruf'-Ebene sind durchführbar und werden auf ähnliche Weise implementiert, entweder als Einsteckmodul zur Voice-Messaging-Anwendung oder auf Netzwerkprotokollebene, beide innerhalb der Benutzermaschine.

[0303] Es wurde zwar die Implementation des bevorzugten Systems mit Bezug auf Einsteckmodule für existierende Anwendungen beschrieben, aber die Erfindung kann auch durch Bereitstellen von Webbrowsern, Email-Clients, Instant-Messaging-Anwendungen oder Voice Over IP Anwendungen implementiert werden, bei denen die Funktionalität der hier beschriebenen Einsteckmodule bereits von Anfang an codiert wird.

Patentansprüche

1. Informationsmanagementsystem, das Folgendes umfasst:
eine oder mehrere Workstations für den Anschluss an ein Computernetz (**10**), wobei jede Workstation einen Speicher aufweist;
eine Anwendung, die in dem genannten Speicher jeder Workstation gespeichert ist, um abgehende Daten' zu dem genannten Netz zu senden und eingehende Daten von dem genannten Netz zu empfangen;
einen Analysator, der in die Anwendung integriert ist und die Aufgabe hat, in Verbindung mit Richtliniendaten Folgendes auszuführen:
a) Überwachen der genannten abgehenden Daten und Ermitteln, beim Einleiten des Sendens der abgehenden Daten und gemäß Richtliniendatenregeln, einer geeigneten Verschlüsselungsstärke für die abgehenden Daten; und
b) Steuern des Sendens der genannten abgehenden Daten von der genannten Anwendung in Abhängigkeit von der genannten Ermittlung einer geeigneten Verschlüsselungsstärke;
wobei die Richtliniendaten zentral definiert werden und Regeln enthalten, die eine geeignete Verschlüsselungsstärke für abgehende Daten vorgeben, wobei die Verschlüsselungsstärke vom Inhalt der Daten abhängig ist.

2. System nach Anspruch 1, wobei die genannten Regeln in den genannten Richtliniendaten vertrauliche Daten definieren, die nicht gesendet werden dürfen, wobei der genannte Analysator die Aufgabe

hat, in Verbindung mit den genannten Richtliniendaten zu verhindern, dass die genannten vertraulichen Daten von der genannten Anwendung gesendet werden.

3. System nach Anspruch 1 oder 2, wobei der genannte Analysator ferner die Aufgabe hat, die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden der genannten abgehenden Daten zu ermitteln; und wobei der genannte Analysator das Senden der genannten abgehenden Daten von der genannten Anwendung sowohl in Abhängigkeit von der genannten Ermittlung einer geeigneten Verschlüsselungsstärke als auch in Abhängigkeit von der genannten Ermittlung der aktuellen Verschlüsselungsstärke beim Gebrauch steuert.

4. System nach Anspruch 3, wobei dann, wenn der Analysator ermittelt, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, der genannte Analysator das Senden der genannten abgehenden Daten von der genannten Anwendung verhindert.

5. System nach Anspruch 3, wobei dann, wenn der Analysator ermittelt, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, der genannte Analysator das Senden der genannten abgehenden Daten für die genannte Anwendung verhindert und die genannte Anwendung so steuert, dass sie eine Verschlüsselungsstärke zum Senden neu negoziiert, die geeignet ist.

6. System nach Anspruch 3, wobei dann, wenn der Analysator ermittelt, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, der genannte Analysator die abgehenden Daten so modifiziert, dass die aktuelle Verschlüsselungsstärke eine geeignete Verschlüsselungsstärke zum Senden der modifizierten abgehenden Daten ist.

7. System nach Anspruch 3, wobei dann, wenn der Analysator ermittelt, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, der genannte Analysator die genannte Anwendung so steuert, dass sie einen Benutzer der genannten Anwendung avisiert, dass die Verschlüsselungsstärke beim Gebrauch nicht ausreicht.

8. System nach einem der vorherigen Ansprüche, wobei der Analysator ferner die Aufgabe hat, Kreditkartennummern in den genannten abgehenden Daten zu identifizieren.

9. System nach Anspruch 8, wobei der Analysator ferner die Aufgabe hat, einen vorbestimmten Satz von Kreditkartennummern von anderen Kreditkartennummern zu unterscheiden, wobei die genannten Regeln der genannten Richtliniendaten andere geeignete Verschlüsselungsstärken für abgehende Daten, die Kreditkartennummern in dem vorbestimmten Satz enthalten, definieren als für andere Kreditkartennummern.

10. System nach Anspruch 9, wobei die genannten Regeln der genannten Richtliniendaten vorgeben, dass es keine geeignete Verschlüsselungsstärke für einen vorbestimmten Satz von einer oder mehreren Kreditkartennummern gibt.

11. System nach einem der vorherigen Ansprüche, wobei der genannte Analysator ferner die Aufgabe hat, ein oder mehrere Kreditkartennummern, Kontocodes, Benutzernamen, Passwörtern, Namen und Adressen und/oder andere vorbestimmte Schlüsselwörter im Inhalt der genannten abgehenden Daten zu identifizieren.

12. System nach einem der vorherigen Ansprüche, wobei die genannten Regeln in den genannten Richtliniendaten eine geeignete Verschlüsselungsstärke für die genannten abgehenden Daten vorgeben, d. h. in Abhängigkeit von der Adresse, zu der die genannten abgehenden Daten gesendet werden sollen.

13. System nach einem der vorherigen Ansprüche, wobei die genannte Anwendung ein Web-Browser ist.

14. System nach Anspruch 13, wobei der genannte Analysator ein Einsteck-Modul (**70**, **72**) des genannten Web-Browsers ist.

15. System nach Anspruch 14, wobei der genannte Web-Browser der Microsoft Internet Explorer ist und der genannte Analysator ein Browser Helper Object ist.

16. System nach einem der Ansprüche 1 bis 12, wobei die genannte Anwendung ein Email-Client ist.

17. System nach Anspruch 16, wobei der genannte Analysator ein Einsteck-Modul (**74**) des genannten Email-Client ist.

18. System nach Anspruch 17, wobei der genannte Email-Client der Microsoft Gutlook Email-Client ist und der genannte Analysator eine Microsoft-Client-Erweiterung ist.

19. System nach einem der Ansprüche 1 bis 12, wobei die genannte Anwendung eine Instant-Messaging-Anwendung ist.

20. System nach Anspruch 19, wobei der genannte Analysator ein Einsteck-Modul der genannten Instant-Messaging-Anwendung ist.

21. System nach einem der vorherigen Ansprüche, wobei das genannte Computernetz, an das eine oder mehrere Workstation(s) angeschlossen werden kann/können, ein öffentliches Computernetz ist, und wobei die genannten ein oder mehreren Workstations zusammen ein privates Computernetz bilden.

22. System nach einem der vorherigen Ansprüche, das ferner eine Supervisor-Workstation umfasst, wobei die genannte Supervisor-Workstation auf die genannten Richtliniendaten zugreifen kann, so dass ein Benutzer der genannten Supervisor-Workstation die genannten Richtliniendaten bearbeiten kann.

23. Verfahren zum Verwalten von Informationen, das die folgenden Schritte beinhaltet:
Bereitstellen von einer oder mehreren Workstation(s) für den Anschluss an ein Computernetz (**10**), wobei jede Workstation einen Speicher hat;
Bereitstellen einer in dem genannten Speicher jeder Workstation gespeicherten Anwendung zum Senden von abgehenden Daten zu dem genannten Netzwerk und zum Empfangen von eingehenden Daten von dem genannten Netzwerk;
Analysieren, mittels eines Analysators, der in die Anwendung integriert ist, der genannten abgehenden Daten, um beim Einleiten des Sendens der abgehenden Daten und
gemäß Richtliniendatenregeln eine geeignete Verschlüsselungsstärke für die abgehenden Daten zu ermitteln; und
Steuern des Sendens der genannten abgehenden Daten von der genannten Anwendung gemäß der Ermittlung einer geeigneten Verschlüsselungsstärke in dem genannten Analyseschritt;
wobei die Richtliniendaten zentral definiert werden und Regeln enthalten, die eine geeignete Verschlüsselungsstärke für abgehende Daten vorgeben, wobei die Verschlüsselungsstärke vom Inhalt der Daten abhängig ist.

24. Verfahren nach Anspruch 23, wobei die genannten Regeln in den genannten Richtliniendaten vertrauliche Daten definieren, die nicht gesendet werden dürfen, und wobei in dem genannten Steuerschritt das Senden der genannten vertraulichen Daten verhindert wird.

25. Verfahren nach Anspruch 23 oder 24, wobei der genannte Analyseschritt ferner den Schritt des Ermittelns der aktuellen Verschlüsselungsstärke beim Gebrauch zum Senden der genannten abgehenden Daten umfasst; und wobei in dem genannten Steuerschritt das Senden der genannten abgehenden Daten von der genannten Anwendung sowohl von der Ermittlung einer geeigneten Verschlüsselungsstärke als auch von der Ermittlung der aktuellen Verschlüsselungsstärke beim Gebrauch abhängig ist.

26. Verfahren nach Anspruch 25, wobei dann, wenn ermittelt wird, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden der abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, in dem genannten Steuerschritt das Senden der genannten abgehenden Daten von der genannten Anwendung verhindert wird.

27. Verfahren nach Anspruch 25, wobei dann, wenn in dem genannten Analyseschritt ermittelt wird, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, in dem genannten Steuerschritt eine Verschlüsselungsstärke, die zum Senden der genannten abgehenden Daten geeignet ist, vor dem Senden negoziiert wird.

28. Verfahren nach Anspruch 25, wobei dann, wenn in dem genannten Analyseschritt ermittelt wird, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, in dem genannten Steuerschritt die abgehenden Daten so modifiziert werden, dass die aktuelle Verschlüsselungsstärke eine geeignete Verschlüsselungsstärke ist.

29. Verfahren nach Anspruch 25, wobei in dem genannten Analyseschritt, wenn ermittelt wird, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, in dem genannten Steuerschritt ein Benutzer der genannten Anwendung avisiert wird, dass die Verschlüsselungsstärke beim Gebrauch nicht ausreicht.

30. Verfahren nach einem der Ansprüche 23 bis 29, wobei der genannte Analyseschritt das Identifizieren von Kreditkartennummern in den genannten abgehenden Daten beinhaltet.

31. Verfahren nach Anspruch 30, wobei der genannte Analyseschritt das Unterscheiden eines vorbestimmten Satzes von einer oder mehreren Kreditkartennummern von anderen Kreditkartennummern beinhaltet, und wobei die genannten Regeln der genannten Richtliniendaten eine andere geeignete Verschlüsselungsstärke für abgehende Daten, die Kreditkartennummern enthalten, in diesem vorbestimmten Satz definiert als für andere Kreditkartennummern.

32. Verfahren nach Anspruch 31, wobei die genannten Regeln der genannten Richtliniendaten vorgeben, dass es keine geeignete Verschlüsselungs-

stärke für den genannten vorbestimmten Satz von einer oder mehreren Kreditkartennummern gibt.

33. Verfahren nach einem der Ansprüche 23 bis 32, wobei der genannte Analyseschritt das Identifizieren von ein oder mehreren Kreditkartennummern, Kontocodes, Benutzernamen, Passwörtern, Namen und Adressen und/oder anderen vorbestimmten Schlüsselwörtern im Inhalt der genannten abgehenden Daten beinhaltet.

34. Verfahren nach einem der Ansprüche 23 bis 33, wobei die genannten Regeln in den genannten Richtliniendaten eine geeignete Verschlüsselungsstärke für die genannten abgehenden Daten vorgeben, die von der Adresse abhängig ist, zu der die genannten abgehenden Daten gesendet werden sollen.

35. Verfahren nach einem der Ansprüche 23 bis 34, wobei die genannte Anwendung ein Web-Browser ist.

36. Verfahren nach Anspruch 35, wobei der genannte Analyseschritt durch ein Einsteck-Modul (**70**, **72**) des genannten Web-Browsers ausgeführt wird.

37. Verfahren nach Anspruch 36, wobei der genannte Web-Browser der Microsoft Internet Explorer ist und das genannte Einsteck-Modul ein Browser Helper Object ist.

38. Verfahren nach einem der Ansprüche 23 bis 34, wobei die genannte Anwendung ein Email-Client ist.

39. Verfahren nach Anspruch 38, wobei der genannte Analyseschritt durch ein Einsteck-Modul (**74**) des genannten Email-Client ausgeführt wird.

40. Verfahren nach Anspruch 39, wobei der genannte Email-Client der Microsoft Gutlook Email-Client ist und das genannte Einsteck-Modul eine Microsoft Exchange Client-Erweiterung ist.

41. Verfahren nach einem der Ansprüche 23 bis 34, wobei die genannte Anwendung eine Instant-Messaging-Anwendung ist.

42. Verfahren nach Anspruch 41, wobei der genannte Analysator ein Einsteck-Modul der genannten Instant-Messaging-Anwendung ist.

43. Verfahren nach einem der Ansprüche 23 bis 42, wobei das genannte Computernetz, an das die genannten ein oder mehreren Workstations angeschlossen werden können, ein öffentliches Computernetz ist, und wobei die genannten ein oder mehreren Workstations zusammen ein privates Computernetz bilden.

44. Verfahren nach einem der Ansprüche 23 bis 43, das ferner den Schritt des Bereitstellens einer Supervisor-Workstation beinhaltet, wobei die genannte Supervisor-Workstation auf die genannten Richtliniendaten zugreifen kann, so dass ein Benutzer der genannten Supervisor-Workstation die genannten Richtliniendaten bearbeiten kann.

45. Computerprogrammprodukt zum Steuern eines Computers, der an ein öffentliches Netzwerk zum Verwalten von Informationen angeschlossen ist, wobei der Computer Zugang zu zentral definierten Richtliniendaten hat, die Regeln enthalten, die eine geeignete Verschlüsselungsstärke für zu dem öffentlichen Netzwerk gesendete abgehende Daten vorgeben, wobei die Verschlüsselungsstärke vom Inhalt der Daten abhängig ist, umfassend:
ein vom Computer lesbares Aufzeichnungsmedium mit darauf aufgezeichnetem Programmcode, der bei Ausführung auf dem genannten Computer den genannten Computer so konfiguriert, dass er Folgendes tut:
Ermitteln, beim Einleiten des Sendens von abgehenden Daten von einer auf dem Computer laufenden Anwendung mit der Aufgabe, wenigstens abgehende Daten zu dem genannten öffentlichen Netzwerk (**10**) zu senden, mittels eines in die Anwendung integrierten Analysators und mit Bezug auf die genannten Regeln in den genannten Richtliniendaten einer geeigneten Verschlüsselungsstärke für die abgehenden Daten; und
Steuern des Sendens der genannten abgehenden Daten durch die genannte Anwendung in Abhängigkeit von der Ermittlung einer geeigneten Verschlüsselungsstärke.

46. Computerprogrammprodukt nach Anspruch 45, wobei die genannten Regeln in den genannten Richtliniendaten vertrauliche Daten definieren, die nicht gesendet werden können, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer die Aufgabe hat, das Senden der genannten vertraulichen Daten von der genannten Anwendung zu verhindern.

47. Computerprogrammprodukt nach Anspruch 45 oder 46, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ferner die Aufgabe hat, die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden der genannten abgehenden Daten zu ermitteln; und das Senden der genannten abgehenden Daten von der genannten Anwendung in Abhängigkeit sowohl von der Ermittlung einer geeigneten Verschlüsselungsstärke als auch von der Ermittlung der aktuellen Verschlüsselungsstärke beim Gebrauch zu steuern.

48. Computerprogrammprodukt nach Anspruch 47, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ferner die Aufga-

be hat, wenn ermittelt wird, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, das Senden der genannten abgehenden Daten von der genannten Anwendung zu verhindern.

49. Computerprogrammprodukt nach Anspruch 47, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ferner die Aufgabe hat, wenn ermittelt wird, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Versch1üsselungsstärke, eine geeignete Verschlüsselungsstärke zum Senden der genannten abgehenden Daten vor dem Senden zu negoziieren.

50. Computerprogrammprodukt nach Anspruch 47, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ferner die Aufgabe hat, wenn ermittelt wird, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, die abgehenden Daten so zu modifizieren, dass die aktuelle Verschlüsselungsstärke eine geeignete Verschlüsselungsstärke ist.

51. Computerprogrammprodukt nach Anspruch 47, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ferner die Aufgabe hat, wenn ermittelt wird, dass die aktuelle Verschlüsselungsstärke beim Gebrauch zum Senden von abgehenden Daten geringer ist als die genannte geeignete Verschlüsselungsstärke, eine Avisierung zu geben, dass die Verschlüsselungsstärke beim Gebrauch nicht ausreicht.

52. Computerprogrammprodukt nach einem der Ansprüche 45 bis 51, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ferner die Aufgabe hat, Kreditkartennummern in den genannten abgehenden Daten zu identifizieren.

53. Computerprogrammprodukt nach Anspruch 52, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ferner die Aufgabe hat, einen vorbestimmten Satz von einer oder mehreren Kreditkartennummern von anderen Kreditkartennummern zu identifizieren, und wobei die genannten Regeln der genannten Richtliniendaten eine andere geeignete Verschlüsselungsstärke für abgehende Daten, die Kreditkartennummern enthalten, in diesem vorbestimmten Satz definieren als für andere Kreditkartennummern.

54. Computerprogrammprodukt nach Anspruch 53, wobei die genannten Regeln der genannten Richtliniendaten vorgeben, dass es keine geeignete Verschlüsselungsstärke für den genannten vorbestimmten Satz von einer oder mehreren Kreditkartennummern gibt.

55. Computerprogrammprodukt nach einem der Ansprüche 45 bis 54, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ferner die Aufgabe hat, eine oder mehrere Kreditkartennummern, Kontocodes, Benutzernamen, Passwörtern, Namen und Adressen und/oder anderen vorbestimmten Schlüsselwörtern im Inhalt der genannten abgehenden Daten zu identifizieren.

56. Computerprogrammprodukt nach einem der Ansprüche 45 bis 55, wobei die genannten Regeln in den genannten Richtliniendaten eine geeignete Verschlüsselungsstärke für die genannten abgehenden Daten vorgeben, die von der Adresse abhängig ist, zu der die genannten abgehenden Daten gesendet werden sollen.

57. Computerprogrammprodukt nach einem der Ansprüche 45 bis 56, wobei die genannte Anwendung ein Web-Browser ist.

58. Computerprogrammprodukt nach Anspruch 57, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ein Einsteck-Modul (**70**, **72**) des genannten Web-Browsers ist.

59. Computerprogrammprodukt nach Anspruch 58, wobei der genannte Web-Browser der Microsoft Internet Explorer ist und das genannte Einsteck-Modul ein Browser Helper Object ist.

60. Computerprogrammprodukt nach einem der Ansprüche 45 bis 56, wobei die genannte Anwendung ein Email-Client ist.

61. Computerprogrammprodukt nach Anspruch 60, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ein Einsteck-Modul (**74**) des genannten Email-Client ist.

62. Computerprogrammprodukt nach Anspruch 61, wobei der genannte Email-Client der Microsoft Gutlook E-Mail-Client ist und das genannte Einsteck-Modul eine Microsoft Exchange Client-Erweiterung ist.

63. Computersoftwareprodukt nach einem der Ansprüche 45 bis 56, wobei die genannte Anwendung eine Instant-Messaging-Anwendung ist.

64. Computersoftwareprodukt nach Anspruch 63, wobei der genannte Programmcode bei Ausführung auf dem genannten Computer ein Einsteck-Modul der genannten Instant-Messaging-Anwendung ist.

Es folgen 25 Blatt Zeichnungen

Anhängende Zeichnungen

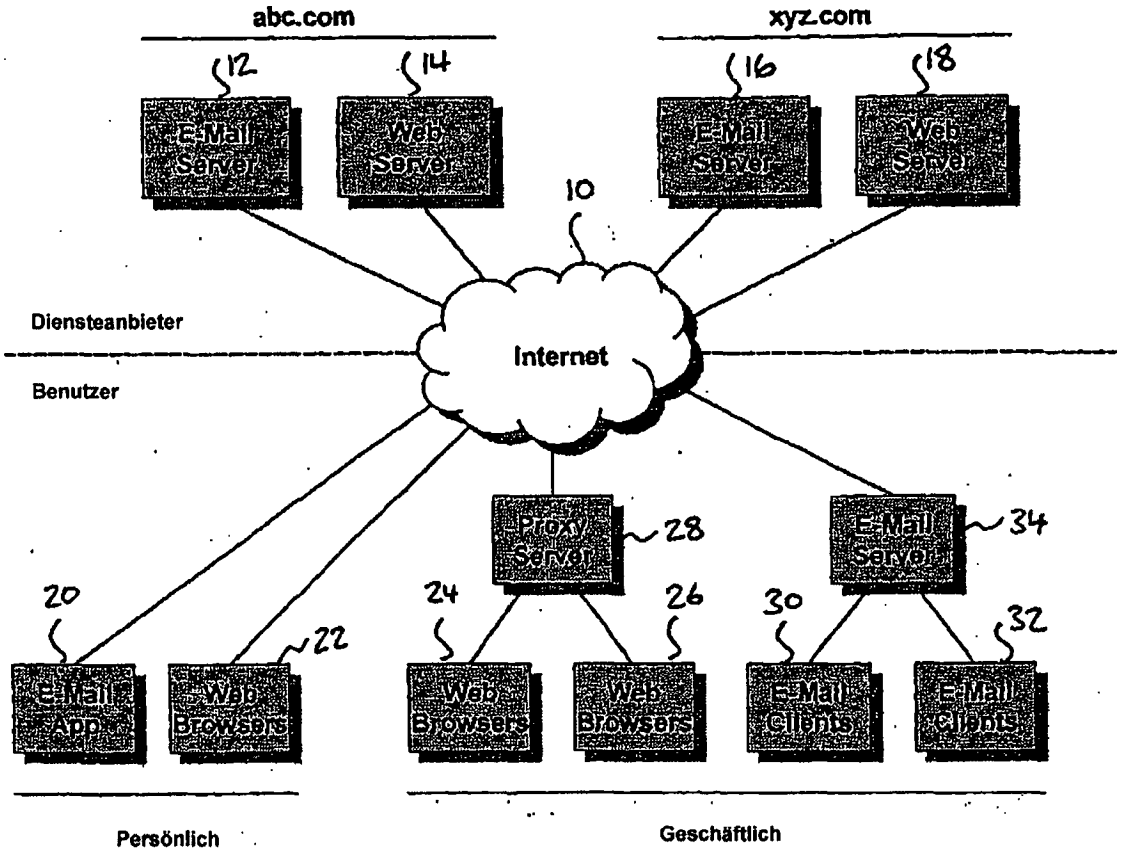
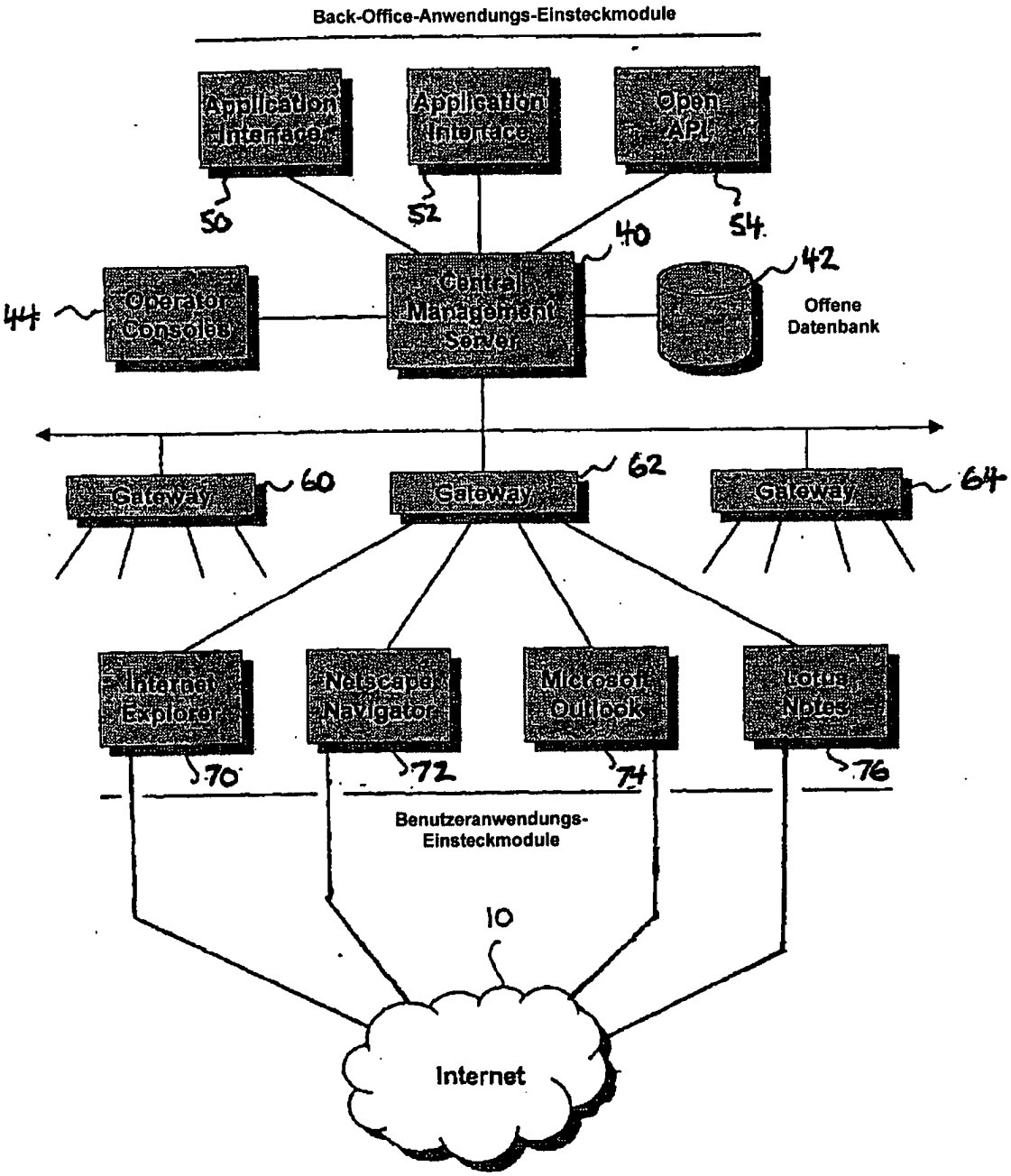


Fig. 1

Fig. 2


Back-Office-Anwendungs-Einsteckmodule
Application Interface
Application Interface
Open API
50
52
54
40
42
44
Operator Consoles
Central Management Server
Offene Datenbank
Gateway
60
Gateway
62
Gateway
64
Internet Explorer
Netscape Navigator
Microsoft Outlook
Lotus Notes
70
72
74
76
Benutzeranwendungs-Einsteckmodule
10
Internet

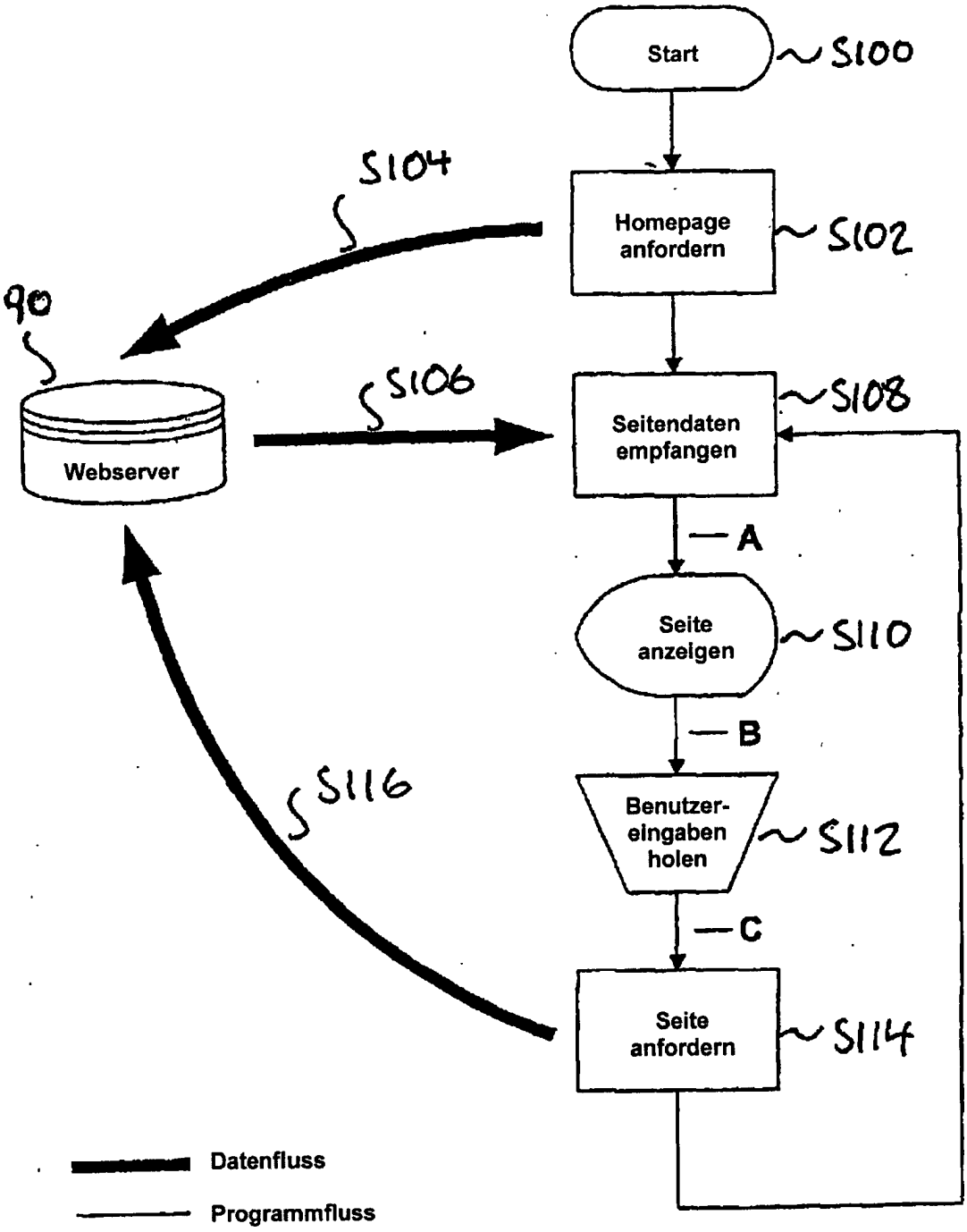

Start
S100
Homepage anfordern
S102
S104
90
Webserver
S106
Seitendaten empfangen
S108
A
Seite anzeigen
S110
B
Benutzer-eingaben holen
S112
S116
C
Seite anfordern
S114
Datenfluss
Programmfluss

Fig. 3

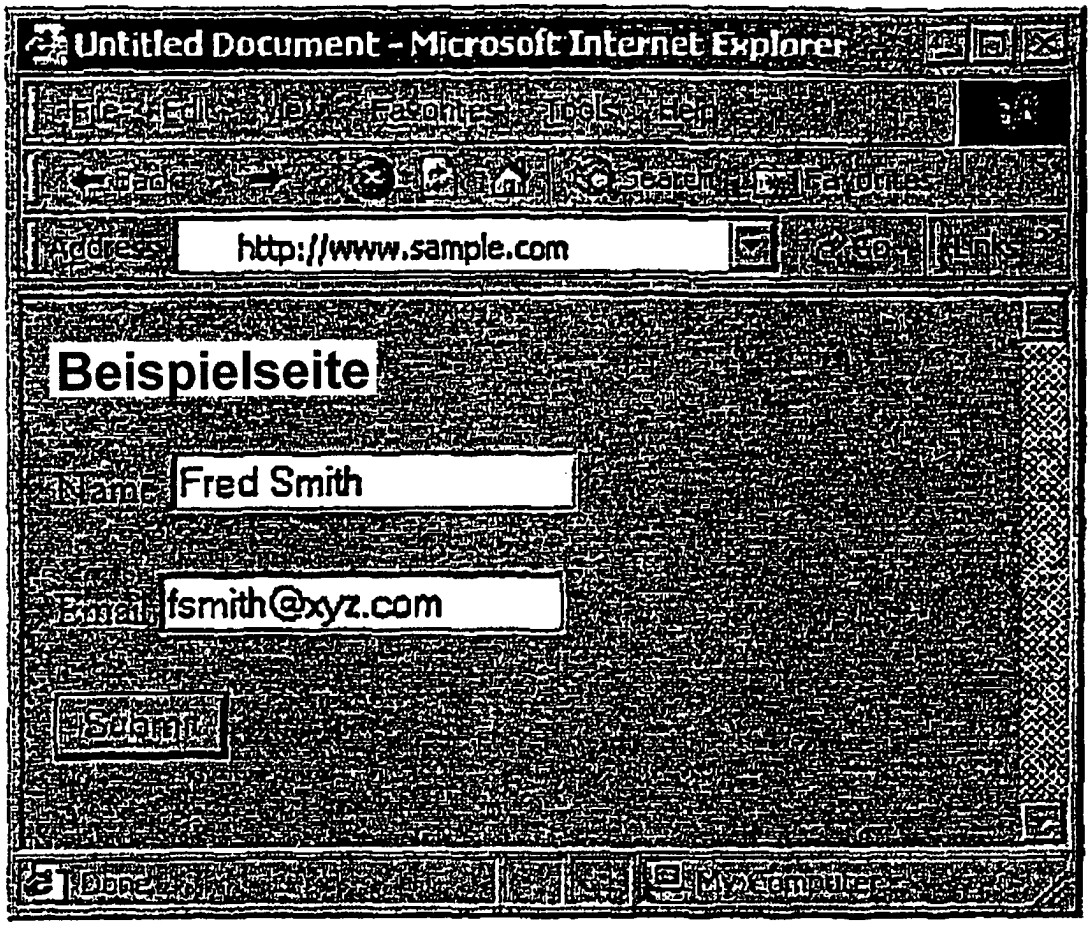

Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.sample.com
Links
Beispielseite
Name Fred Smith
Email fsmith@xyz.com
Submit
Done
My Computer

Fig. 4

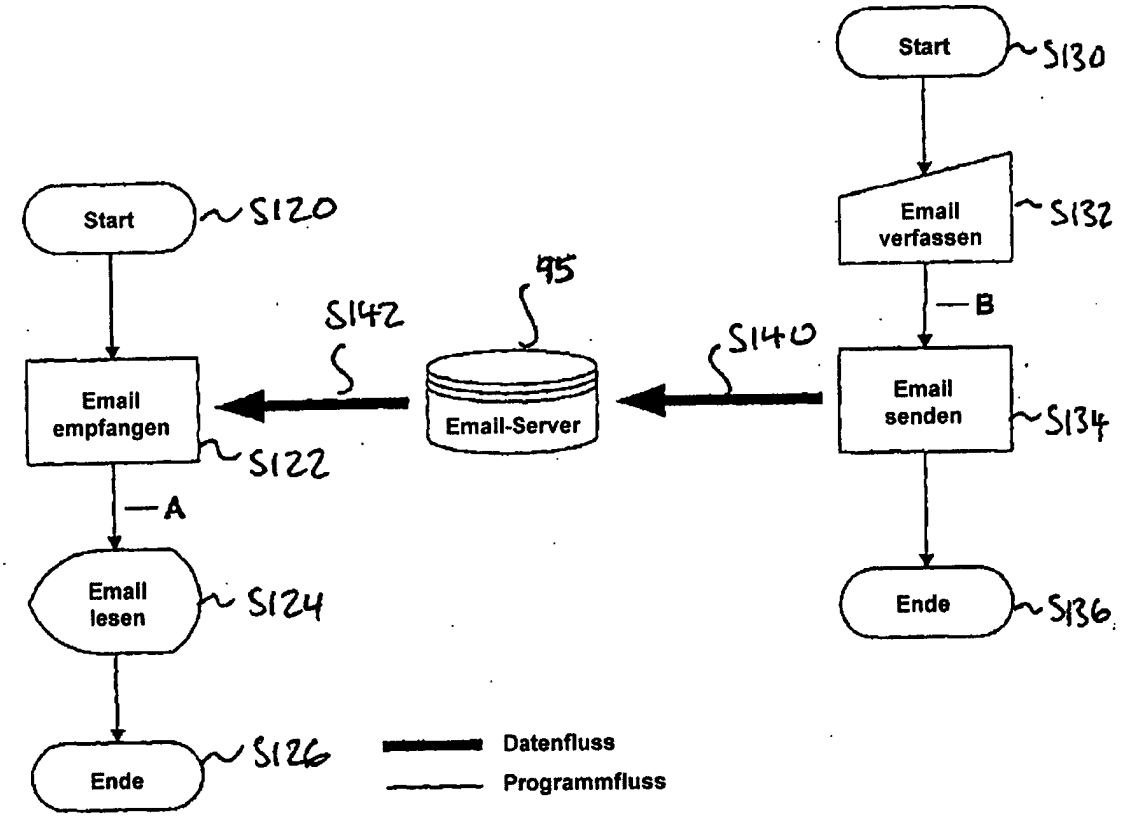

Start
S130
Email verfassen
S132
B
S140
Email senden
S134
Ende
S136
95
S142
Email-Server
Start
S120
Email empfangen
S122
A
Email lesen
S124
Ende
S126
Datenfluss
Programmfluss

Fig. 5

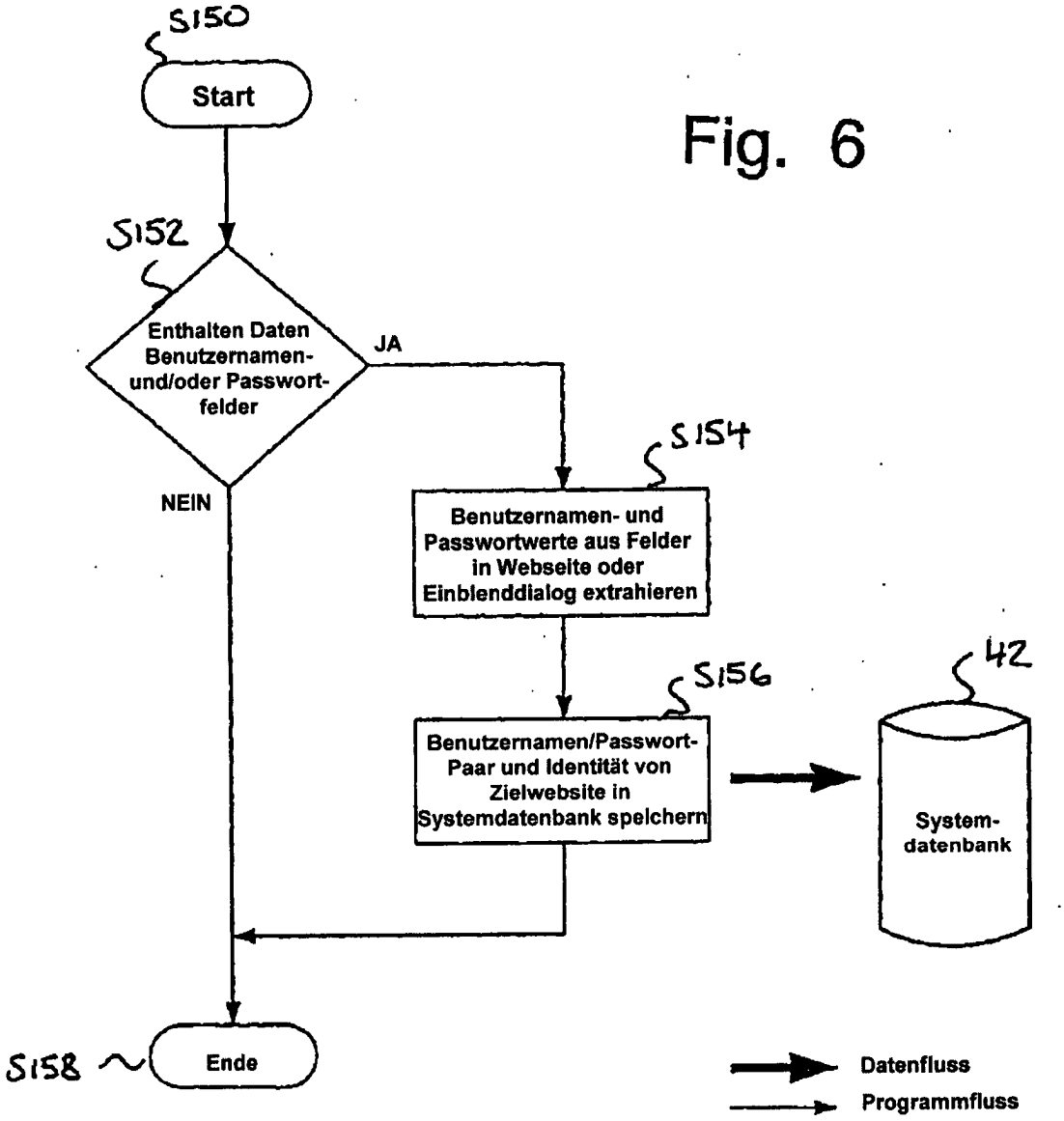

S150
Start
S152
Enthalten Daten Benutzernamen- und/oder Passwort-felder
JA
NEIN
S154
Benutzernamen- und Passwortwerte aus Felder in Webseite oder Einblenddialog extrahieren
S156
Benutzernamen/Passwort-Paar und Identität von Zielwebsite in Systemdatenbank speichern
42
System-datenbank
S158
Ende
Datenfluss
Programmfluss

Fig. 6

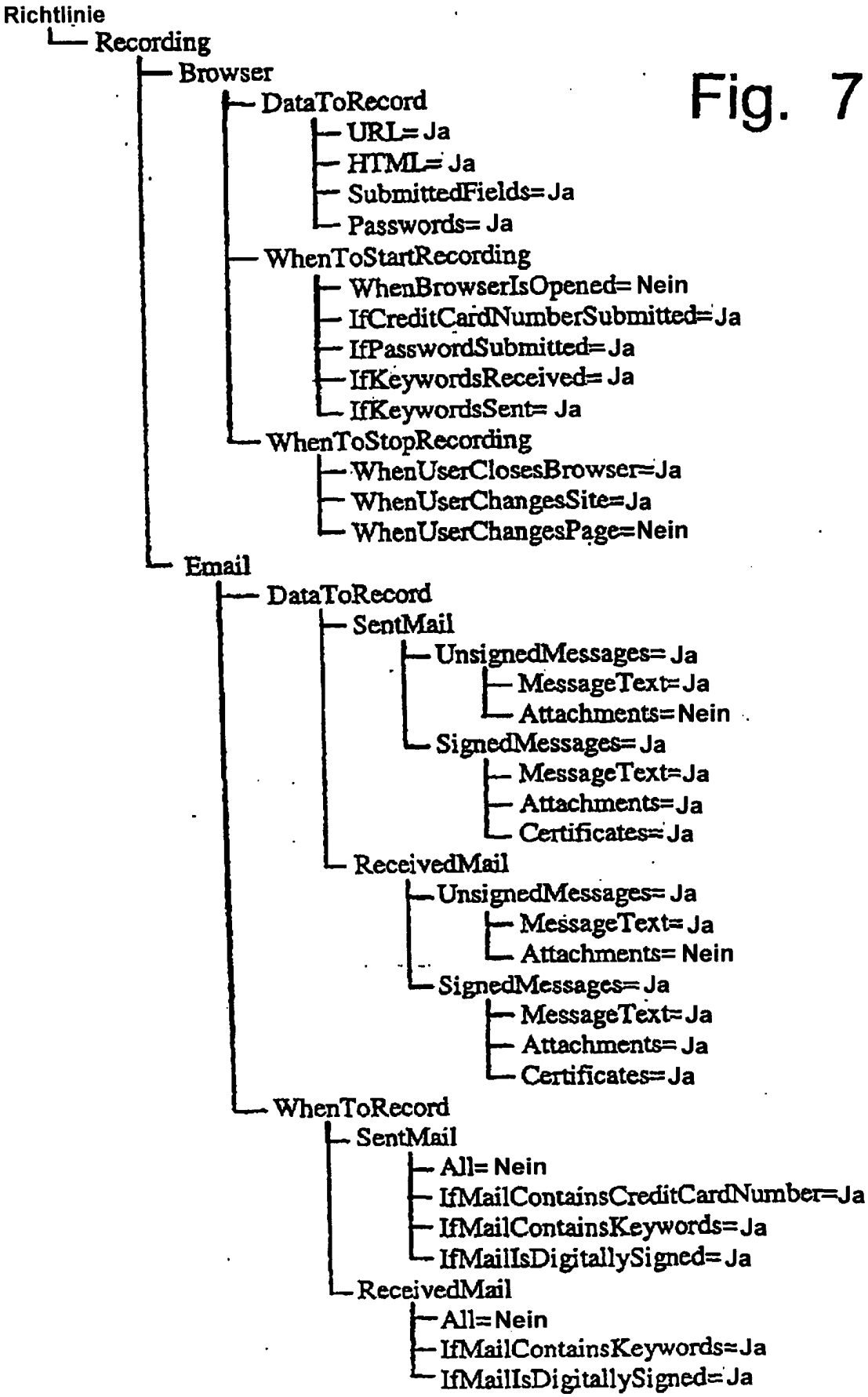

Richtlinie
Recording
Browser
DataToRecord
URL= Ja
HTML= Ja
SubmittedFields=Ja
Passwords= Ja
WhenToStartRecording
WhenBrowserIsOpened= Nein
IfCreditCardNumberSubmitted=Ja
IfPasswordSubmitted=Ja
IfKeywordsReceived= Ja
IfKeywordsSent= Ja
WhenToStopRecording
WhenUserClosesBrowser=Ja
WhenUserChangesSite=Ja
WhenUserChangesPage=Nein
Email
DataToRecord
SentMail
UnsignedMessages= Ja
MessageText=Ja
Attachments=Nein
SignedMessages= Ja
MessageText=Ja
Attachments=Ja
Certificates=Ja
ReceivedMail
UnsignedMessages= Ja
MessageText= Ja
Attachments= Nein
SignedMessages= Ja
MessageText=Ja
Attachments= Ja
Certificates=Ja
WhenToRecord
SentMail
All= Nein
IfMailContainsCreditCardNumber=Ja
IfMailContainsKeywords=Ja
IfMailIsDigitallySigned=Ja
ReceivedMail
All=Nein
IfMailContainsKeywords=Ja
IfMailIsDigitallySigned=Ja

Fig. 7

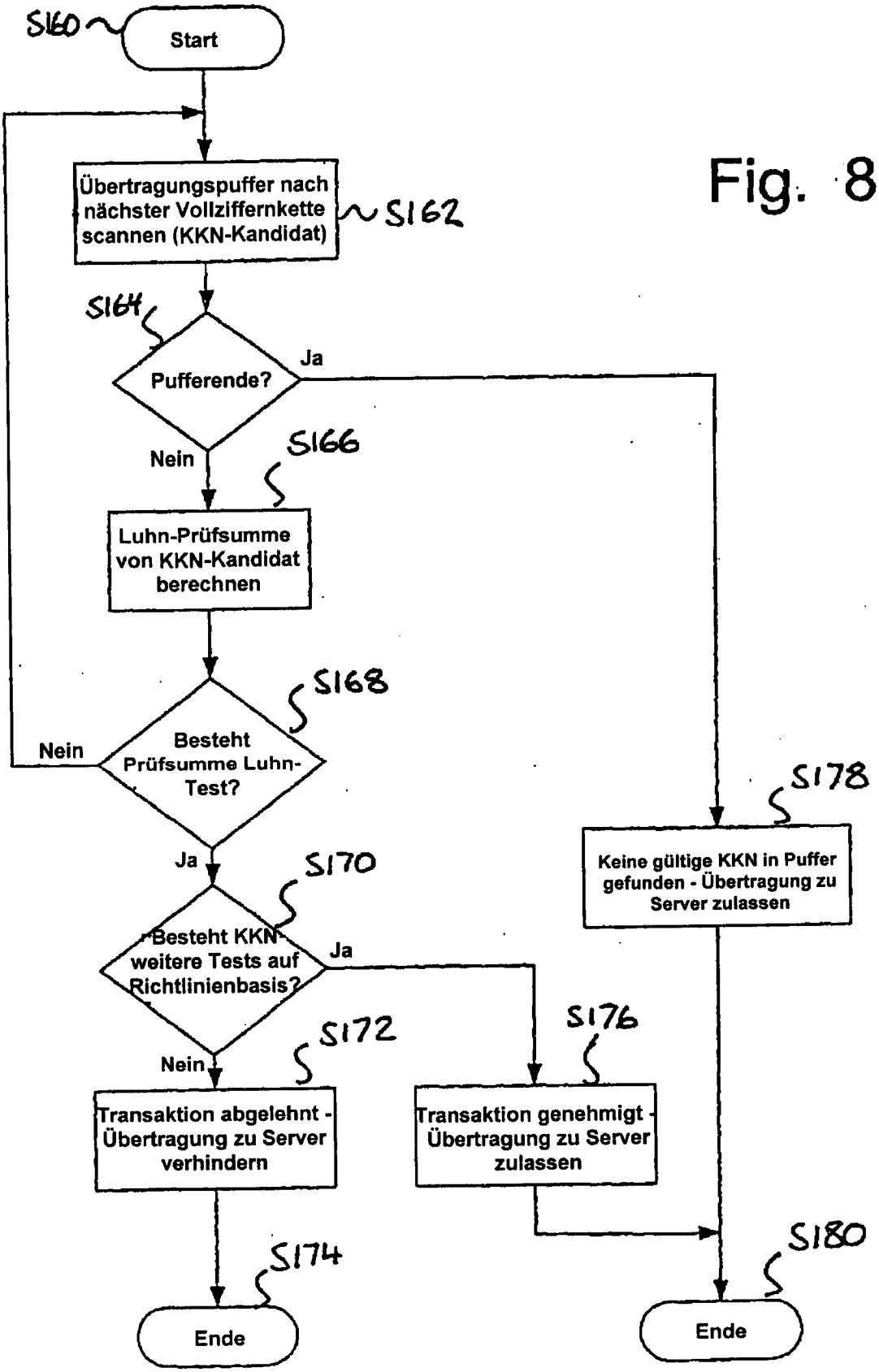

S160
Start
Übertragungspuffer nach nächster Vollziffernkette scannen (KKN-Kandidat)
S162
S164
Pufferende?
Ja
Nein
S166
Luhn-Prüfsumme von KKN-Kandidat berechnen
S168
Besteht Prüfsumme Luhn-Test?
Nein
Ja
S170
Besteht KKN weitere Tests auf Richtlinienbasis?
Ja
Nein
S172
Transaktion abgelehnt - Übertragung zu Server verhindern
S174
Ende
S176
Transaktion genehmigt - Übertragung zu Server zulassen
S178
Keine gültige KKN in Puffer gefunden - Übertragung zu Server zulassen
S180
Ende

Fig. 8

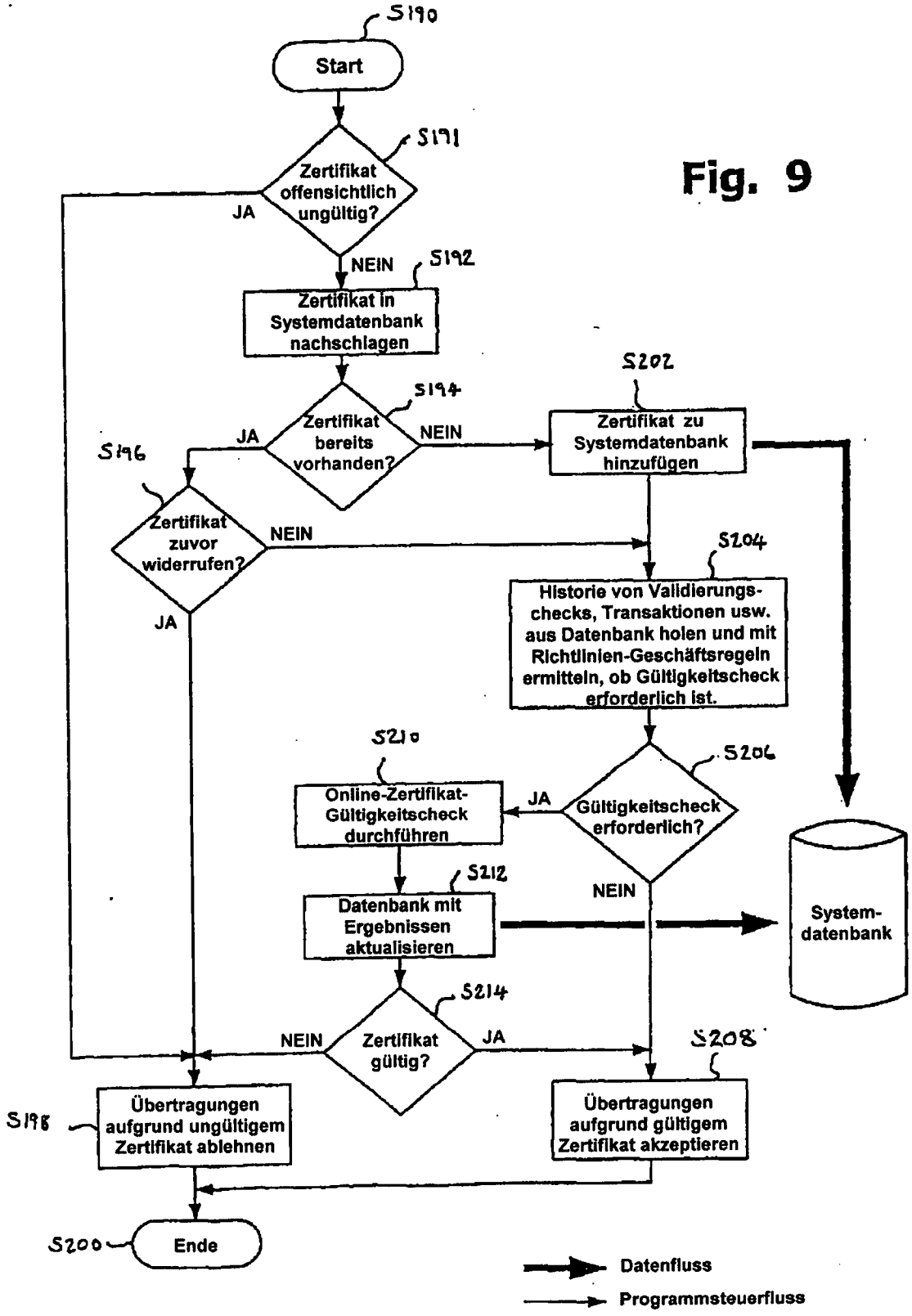

S190
Start
S191
Zertifikat offensichtlich ungültig?
JA
NEIN
S192
Zertifikat in Systemdatenbank nachschlagen
S194
Zertifikat bereits vorhanden?
JA
NEIN
S196
Zertifikat zuvor widerrufen?
NEIN
JA
S202
Zertifikat zu Systemdatenbank hinzufügen
S204
Historie von Validierungs-checks, Transaktionen usw. aus Datenbank holen und mit Richtlinien-Geschäftsregeln ermitteln, ob Gültigkeitscheck erforderlich ist.
S206
Gültigkeitscheck erforderlich?
JA
NEIN
S210
Online-Zertifikat-Gültigkeitscheck durchführen
S212
Datenbank mit Ergebnissen aktualisieren
System-datenbank
S214
Zertifikat gültig?
NEIN
JA
S208
Übertragungen aufgrund gültigem Zertifikat akzeptieren
S198
Übertragungen aufgrund ungültigem Zertifikat ablehnen
S200
Ende
Datenfluss
Programmsteuerfluss

Fig. 9

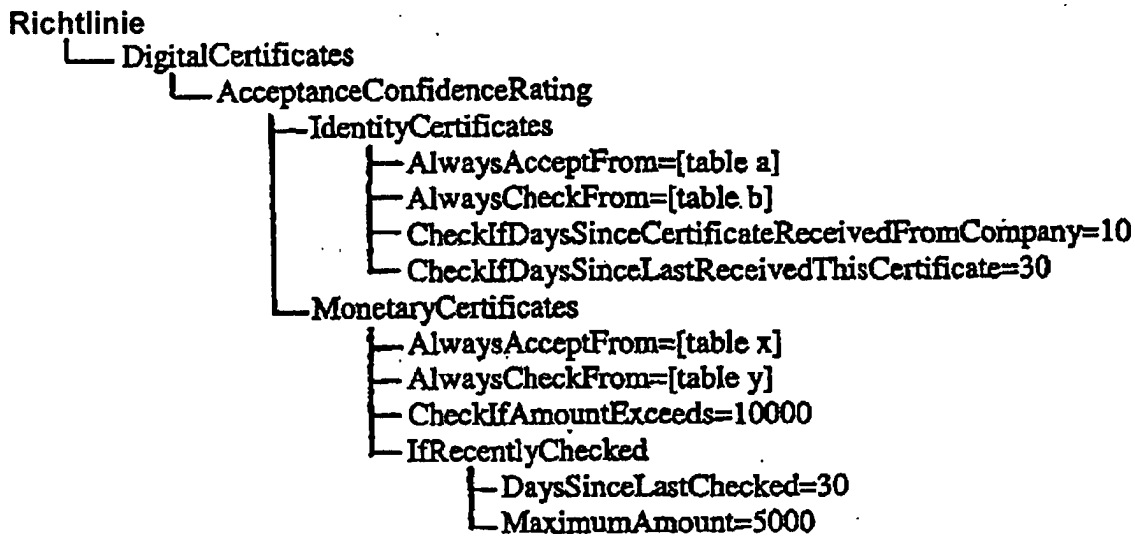
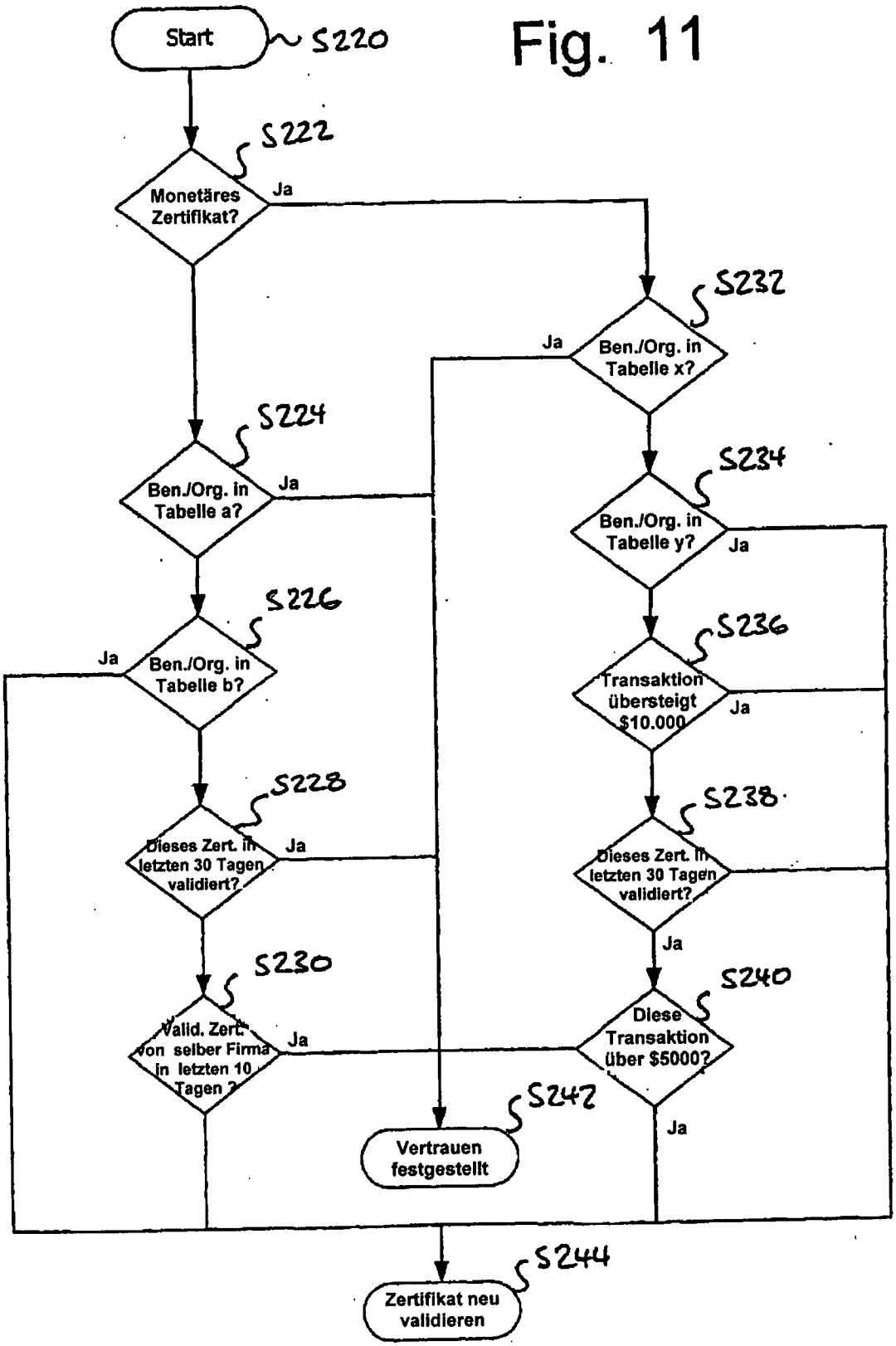

Richtlinie
DigitalCertificates
AcceptanceConfidenceRating
IdentityCertificates
AlwaysAcceptFrom=[table a]
AlwaysCheckFrom=[table b]
CheckIfDaysSinceCertificateReceivedFromCompany=10
CheckIfDaysSinceLastReceivedThisCertificate=30
MonetaryCertificates
AlwaysAcceptFrom=[table x]
AlwaysCheckFrom=[table y]
CheckIfAmountExceeds=10000
IfRecentlyChecked
DaysSinceLastChecked=30
MaximumAmount=5000

Fig. 10

Fig. 11


Start
S220
S222
Monetäres Zertifikat?
Ja
S224
Ben./Org. in Tabelle a?
Ja
S226
Ben./Org. in Tabelle b?
Ja
S228
Dieses Zert. in letzten 30 Tagen validiert?
Ja
S230
Valid. Zert. von selber Firma in letzten 10 Tagen ?
Ja
S232
Ben./Org. in Tabelle x?
Ja
S234
Ben./Org. in Tabelle y?
Ja
S236
Transaktion übersteigt $10.000
Ja
S238
Dieses Zert. in letzten 30 Tagen validiert?
Ja
S240
Diese Transaktion über $5000?
Ja
S242
Vertrauen festgestellt
S244
Zertifikat neu validieren

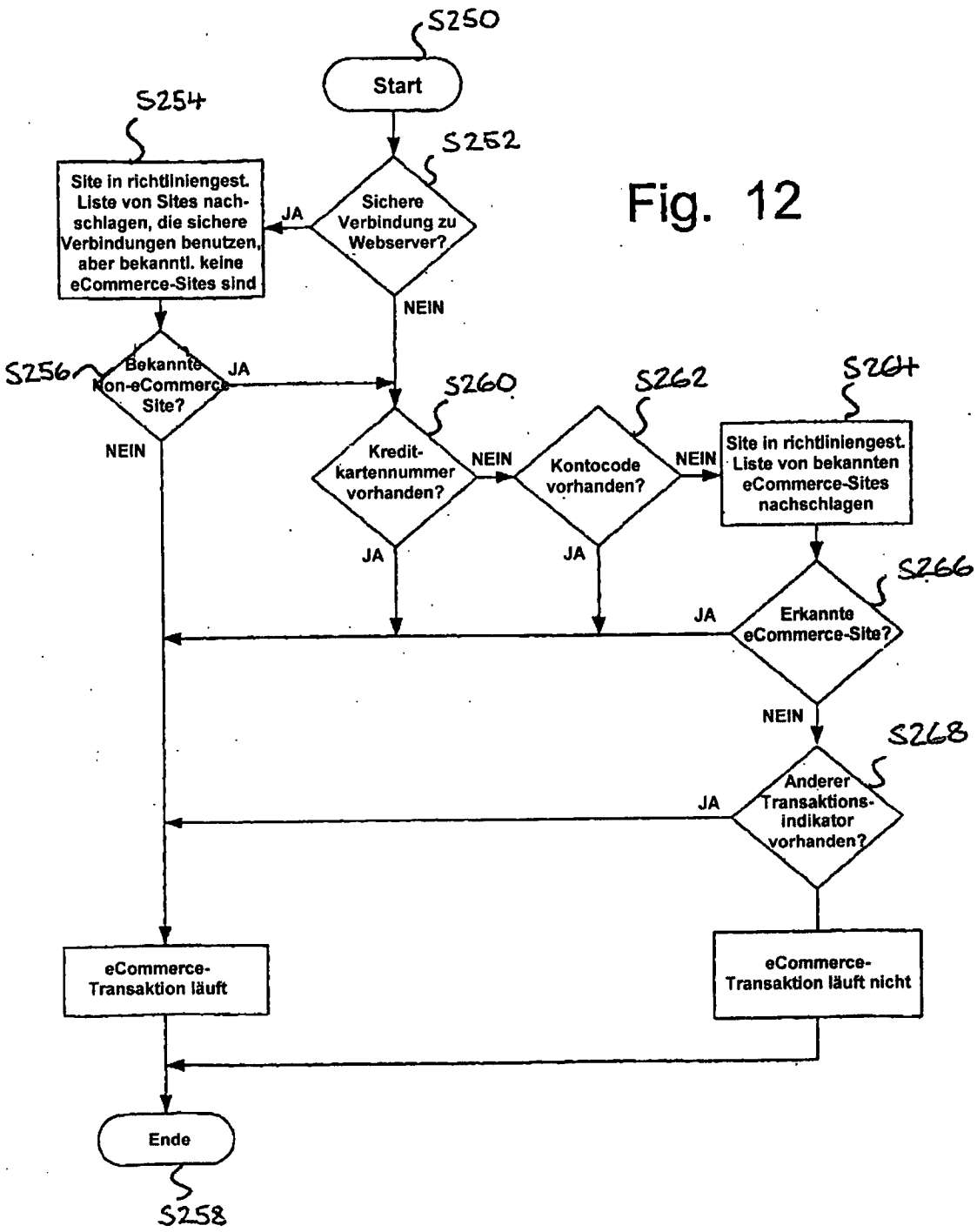

S250
Start
S252
Sichere Verbindung zu Webserver?
JA
S254
Site in richtliniengest. Liste von Sites nachschlagen, die sichere Verbindungen benutzen, aber bekanntl. keine eCommerce-Sites sind
NEIN
S256
Bekannte Non-eCommerce Site?
JA
NEIN
S260
Kredit-kartennummer vorhanden?
NEIN
JA
S262
Kontocode vorhanden?
NEIN
JA
S264
Site in richtliniengest. Liste von bekannten eCommerce-Sites nachschlagen
S266
Erkannte eCommerce-Site?
JA
NEIN
S268
Anderer Transaktions-indikator vorhanden?
JA
eCommerce-Transaktion läuft
eCommerce-Transaktion läuft nicht
Ende
S258

Fig. 12

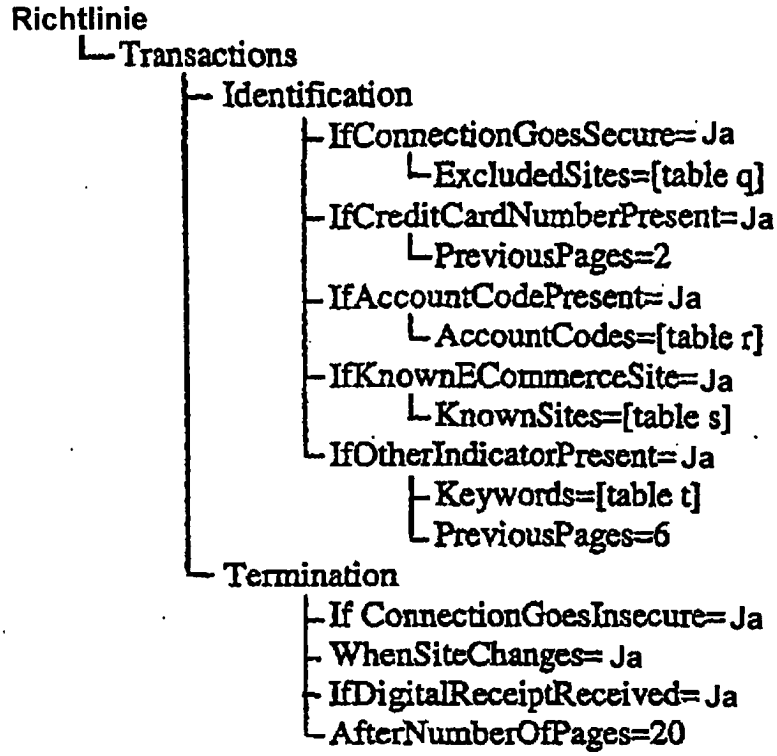


Tabelle q - Ausgeschlossene Sites
www.hotmail.com
www.passport.com
ibankon.barclays.co.uk
www.nwolb.co.uk

Tabelle r - Kontocodes	
Konto-code	Aufzuzeichnende vorherige Seiten
21321234	2
ORCH01	6
58734	1
PETER304	0

Tabelle s - Bekannte eCommerce-Sites
ecomm.us.dell.com/dellstore
buy.supersaver.co.uk
www.booksforall.com/basket

Tabelle t - Schlüsselwörter
"Quittung"
"Vielen Dank für Ihren Auftrag"
"Auftragsbestätigung"

Fig. 13

Fig. 14

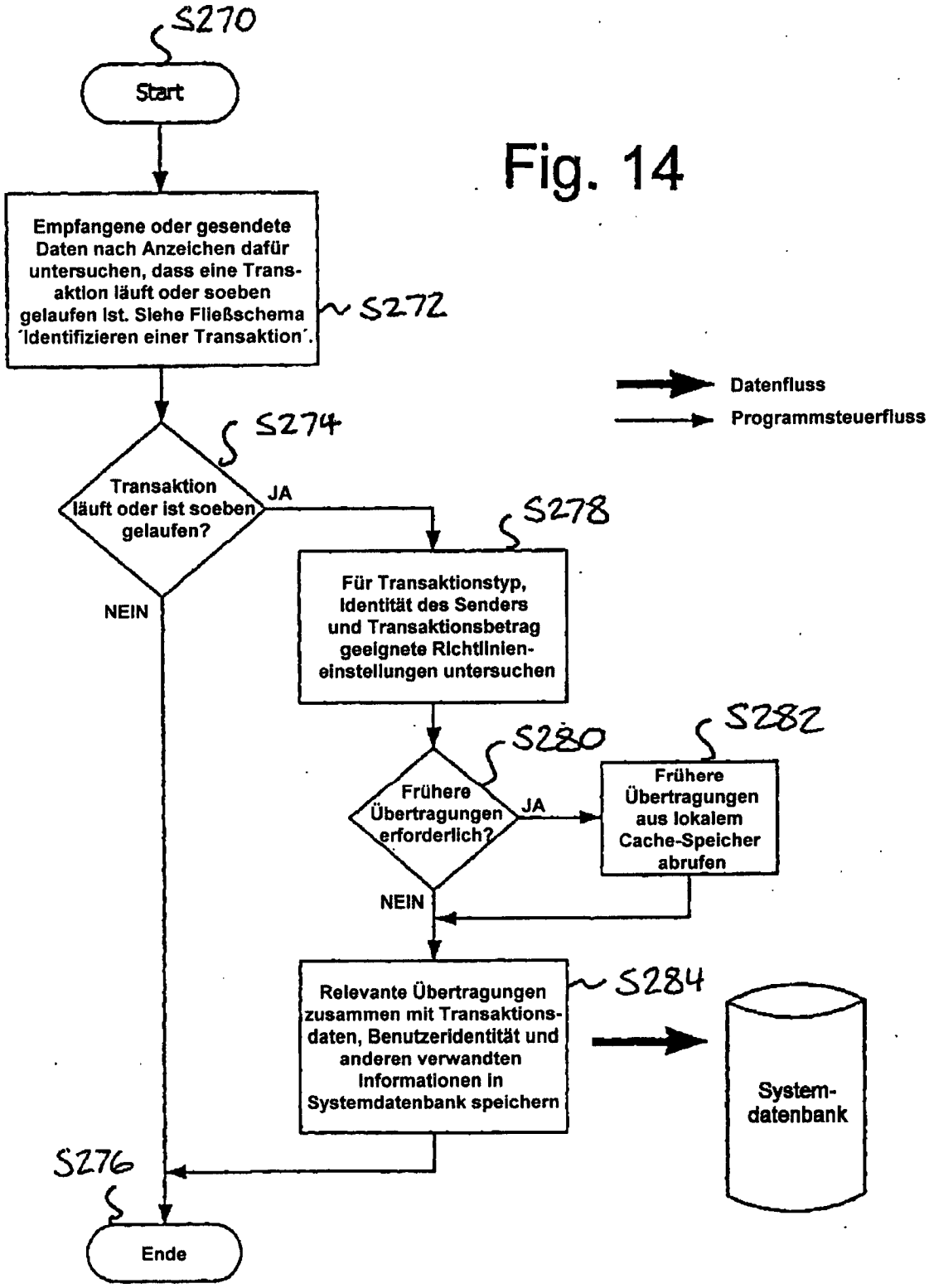
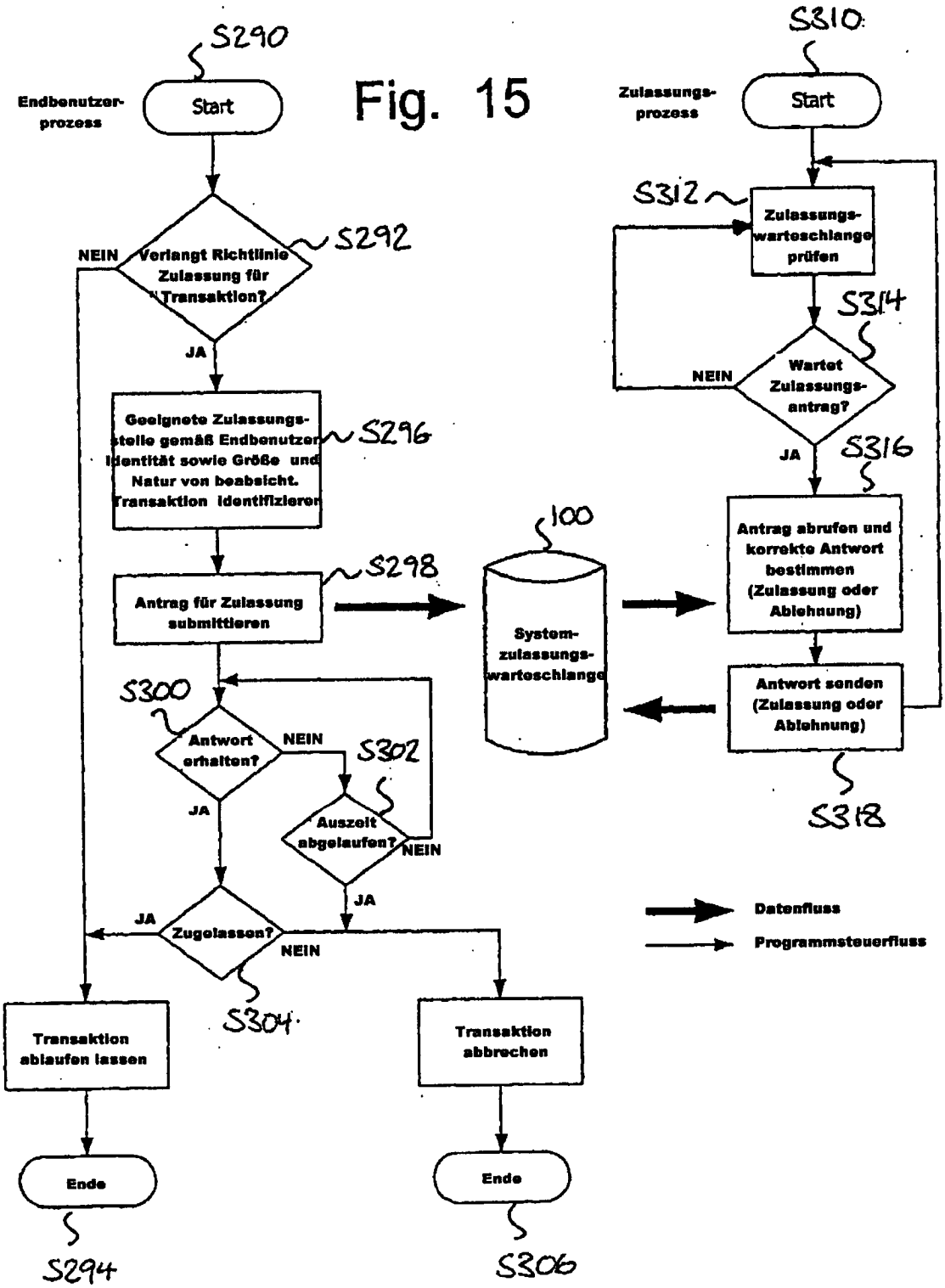

S270
Start
Empfangene oder gesendete Daten nach Anzeichen dafür untersuchen, dass eine Transaktion läuft oder soeben gelaufen ist. Siehe Fließschema 'Identifizieren einer Transaktion'.
S272
Datenfluss
Programmsteuerfluss
S274
Transaktion läuft oder ist soeben gelaufen?
JA
NEIN
S278
Für Transaktionstyp, Identität des Senders und Transaktionsbetrag geeignete Richtlinieneinstellungen untersuchen
S280
Frühere Übertragungen erforderlich?
JA
NEIN
S282
Frühere Übertragungen aus lokalem Cache-Speicher abrufen
Relevante Übertragungen zusammen mit Transaktionsdaten, Benutzeridentität und anderen verwandten Informationen in Systemdatenbank speichern
S284
Systemdatenbank
S276
Ende

Fig. 15


S290
Endbenutzer-prozess
Start
S292
Verlangt Richtlinie Zulassung für Transaktion?
NEIN
JA
S296
Geeignete Zulassungs-stelle gemäß Endbenutzer-Identität sowie Größe und Natur von beabsicht. Transaktion identifizieren
S298
Antrag für Zulassung submittieren
S300
Antwort erhalten?
NEIN
JA
S302
Auszeit abgelaufen?
NEIN
JA
Zugelassen?
JA
NEIN
S304
Transaktion ablaufen lassen
Ende
S294
Transaktion abbrechen
Ende
S306
100
System-zulassungs-warteschlange
S310
Zulassungs-prozess
Start
S312
Zulassungs-warteschlange prüfen
S314
Wartet Zulassungs-antrag?
NEIN
JA
S316
Antrag abrufen und korrekte Antwort bestimmen (Zulassung oder Ablehnung)
Antwort senden (Zulassung oder Ablehnung)
S318
Datenfluss
Programmsteuerfluss

Richtlinie
- TransactionApproval
  - MaximumUnapprovedTransactionAmount=500
  - MaximumUnapprovedMonthlyAmount=2500
  - ExcludedSites=[table e]
  - Approvers=[table f]

Tabelle f - Zulassungsstellen		
Benutzername	**Grenze**	**Ausgeschlossene Sites**
F Smith	$500	www.dell.com
R Jones	$1000	www.dell.com; www.officemax.com
F Healy	**Unbegrenzt**	**Keine**

Fig. 16

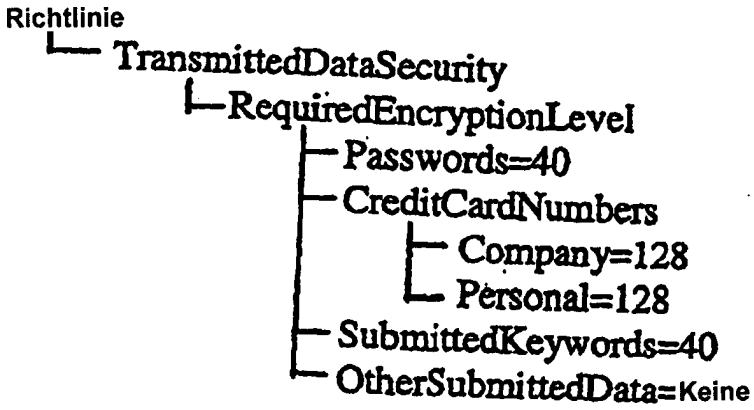
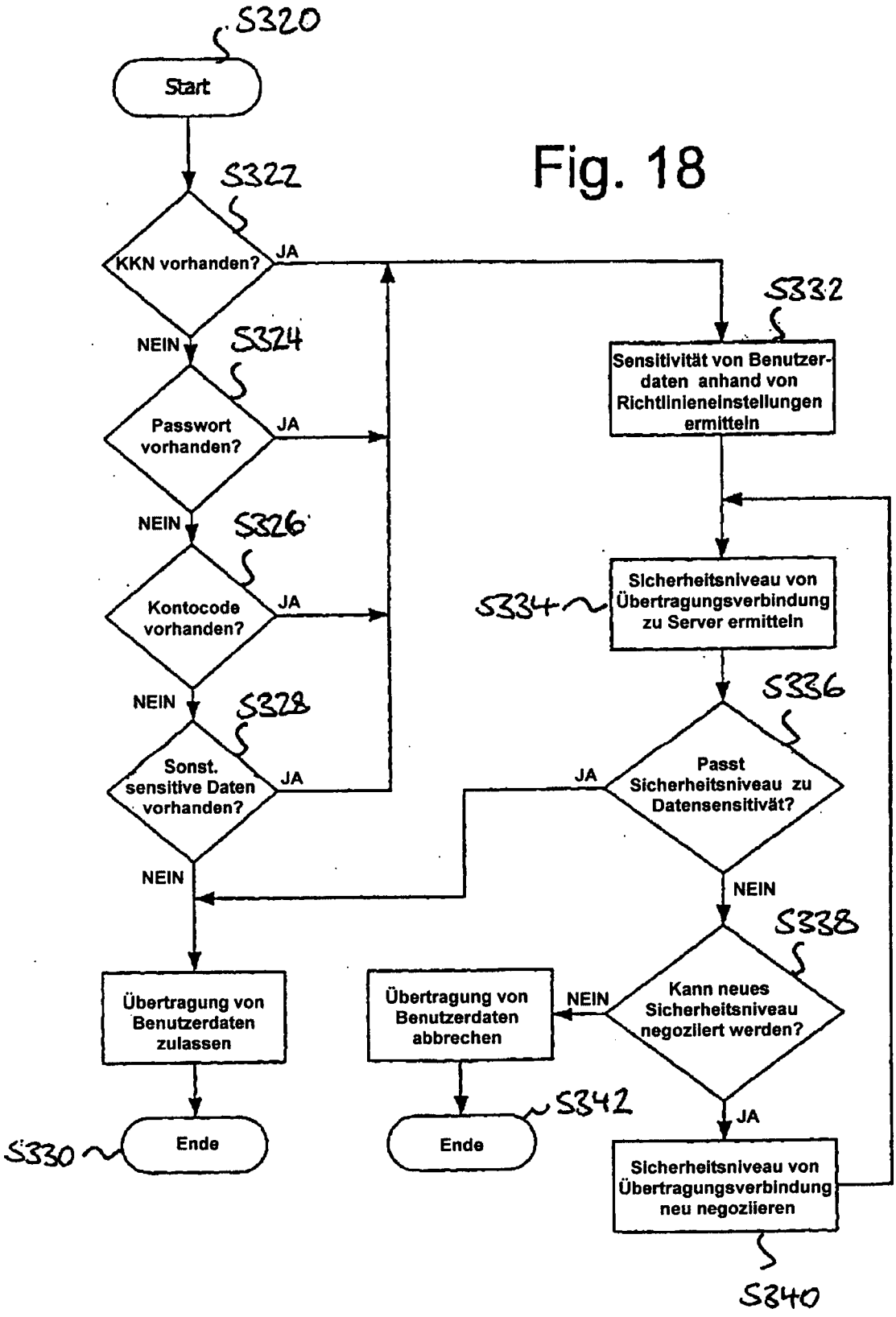
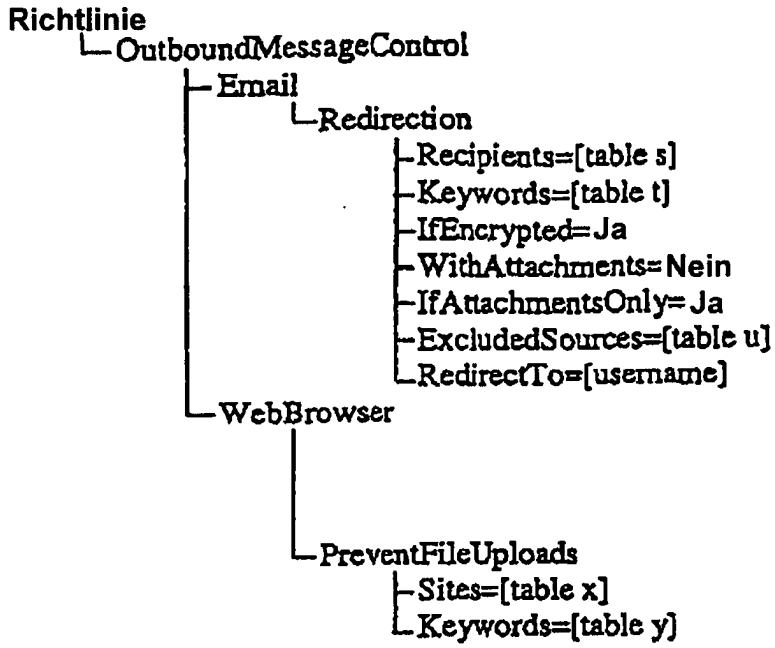

Richtlinie
TransmittedDataSecurity
RequiredEncryptionLevel
Passwords=40
CreditCardNumbers
Company=128
Personal=128
SubmittedKeywords=40
OtherSubmittedData=Keine

Fig. 17

Fig. 18


S320
Start
S322
KKN vorhanden?
JA
NEIN
S324
Passwort vorhanden?
JA
NEIN
S326
Kontocode vorhanden?
JA
NEIN
S328
Sonst. sensitive Daten vorhanden?
JA
NEIN
Übertragung von Benutzerdaten zulassen
S330
Ende
S332
Sensitivität von Benutzerdaten anhand von Richtlinieneinstellungen ermitteln
S334
Sicherheitsniveau von Übertragungsverbindung zu Server ermitteln
S336
Passt Sicherheitsniveau zu Datensensitivät?
JA
NEIN
S338
Kann neues Sicherheitsniveau negoziert werden?
NEIN
JA
Übertragung von Benutzerdaten abbrechen
S342
Ende
Sicherheitsniveau von Übertragungsverbindung neu negoziieren
S340



Beispiel für Tabelle s
*@microsoft.com
fred.smith@xyz.com
jjones@hotmail.com

Beispiel für Tabelle x
* @ hotmail.com
*@ aol.com
username

Beispiel für Tabelle t, y
vertraulich
geheim
Vertrag
Angebot
Auftrag
Projekt x

Beispiel für Tabelle u
A.N. Authoriseduser
T.H.E. Boss

Fig. 19

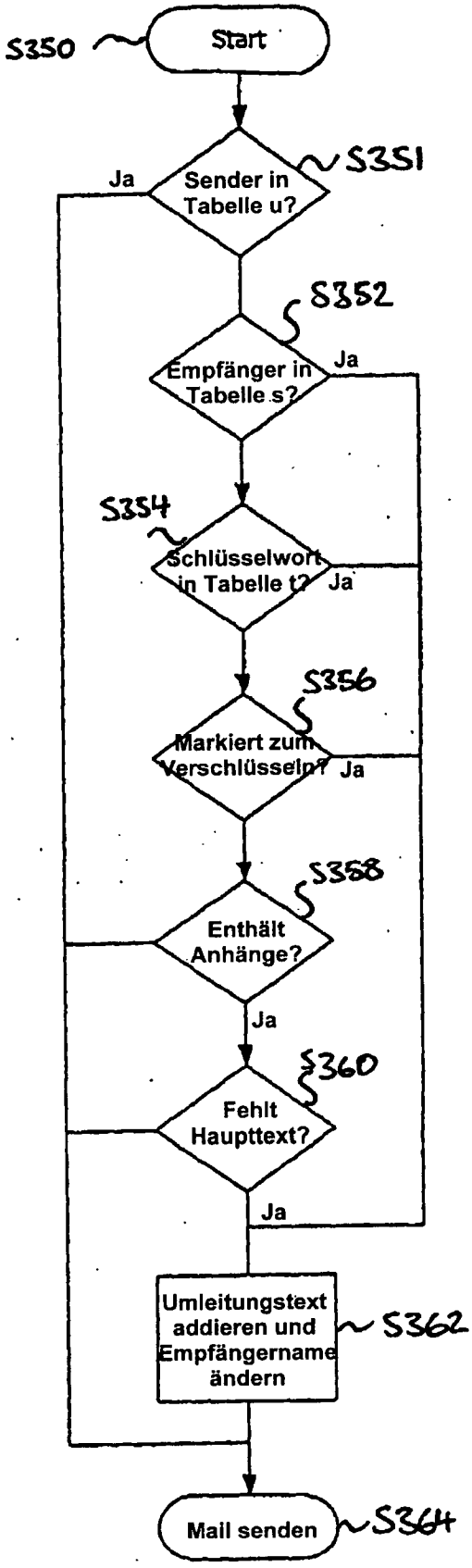

S350
Start
S351
Sender in Tabelle u?
Ja
S352
Empfänger in Tabelle s?
Ja
S354
Schlüsselwort in Tabelle t?
Ja
S356
Markiert zum Verschlüsseln?
Ja
S358
Enthält Anhänge?
Ja
S360
Fehlt Haupttext?
Ja
Umleitungstext addieren und Empfängername ändern
S362
Mail senden
S364

Fig. 20

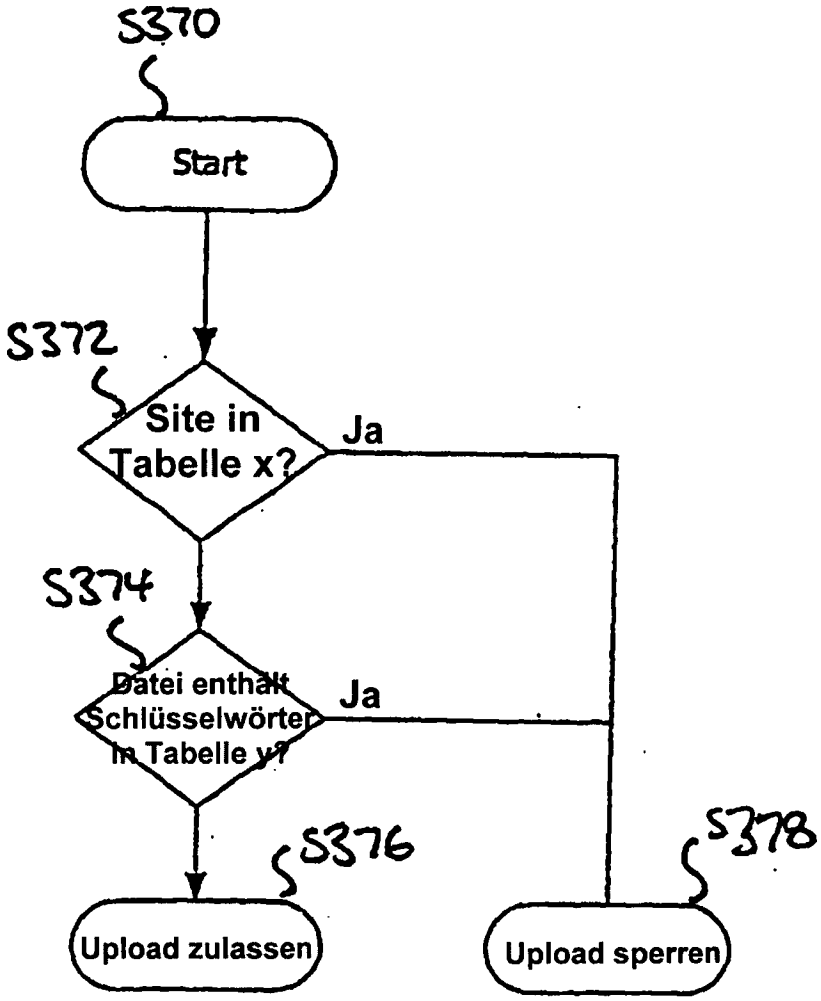
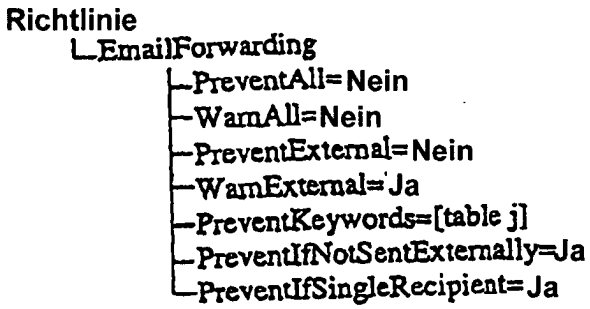

S370
Start
S372
Site in Tabelle x?
Ja
S374
Datei enthält Schlüsselwörter in Tabelle y?
Ja
S376
Upload zulassen
S378
Upload sperren

Fig. 21



Beispiel für Tabelle j
vertraulich
geheim
Vertrag
Angebot
Auftrag
Projekt x

Fig. 22

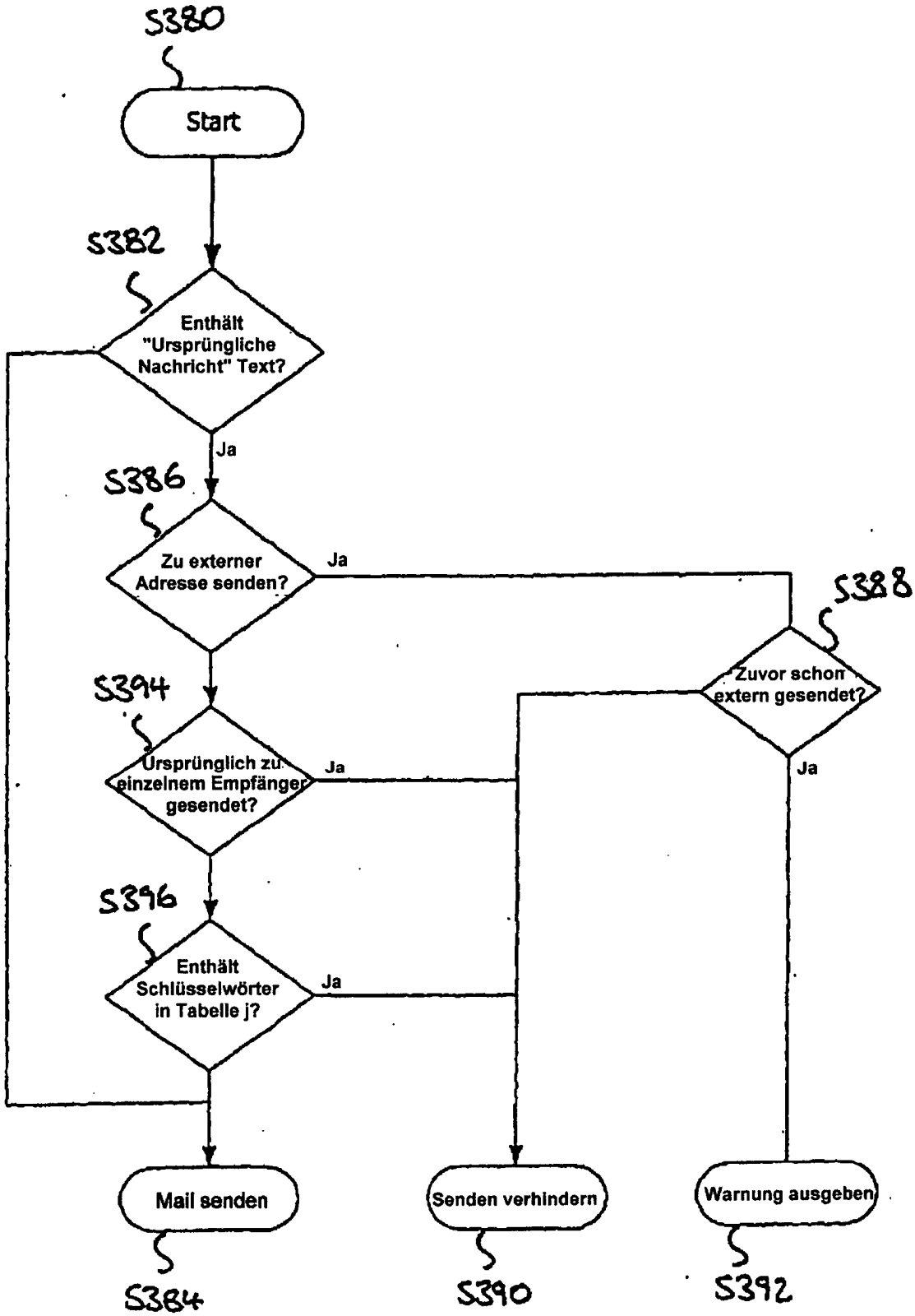
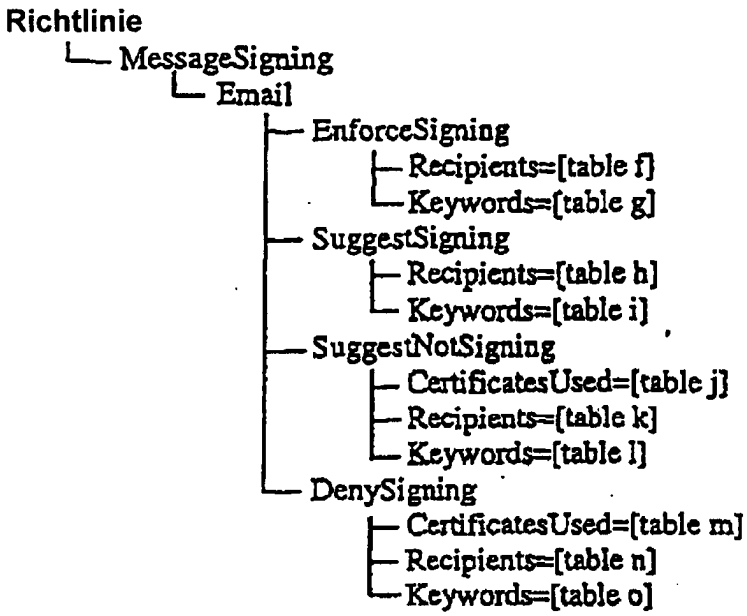

S380
Start
S382
Enthält "Ursprüngliche Nachricht" Text?
Ja
S386
Zu externer Adresse senden?
Ja
S388
Zuvor schon extern gesendet?
Ja
S394
Ursprünglich zu einzelnem Empfänger gesendet?
Ja
S396
Enthält Schlüsselwörter in Tabelle j?
Ja
Mail senden
S384
Senden verhindern
S390
Warnung ausgeben
S392

Fig. 23



Beispiel für Tabellen f, h, k, n
*@microsoft.com
fred.smith@xyz.com
jjones@hotmail.com

Beispiel für Tabellen j, m
Aussteller = "Identrus", Typ = Garantie
Aussteller= "MeineFirma", Typ = Beliebig
Key=1234567890

Beispiel für Tabellen g, i, l, o
vertraulich
geheim
Vertrag
Angebot
Auftrag
Projekt x

Fig. 24

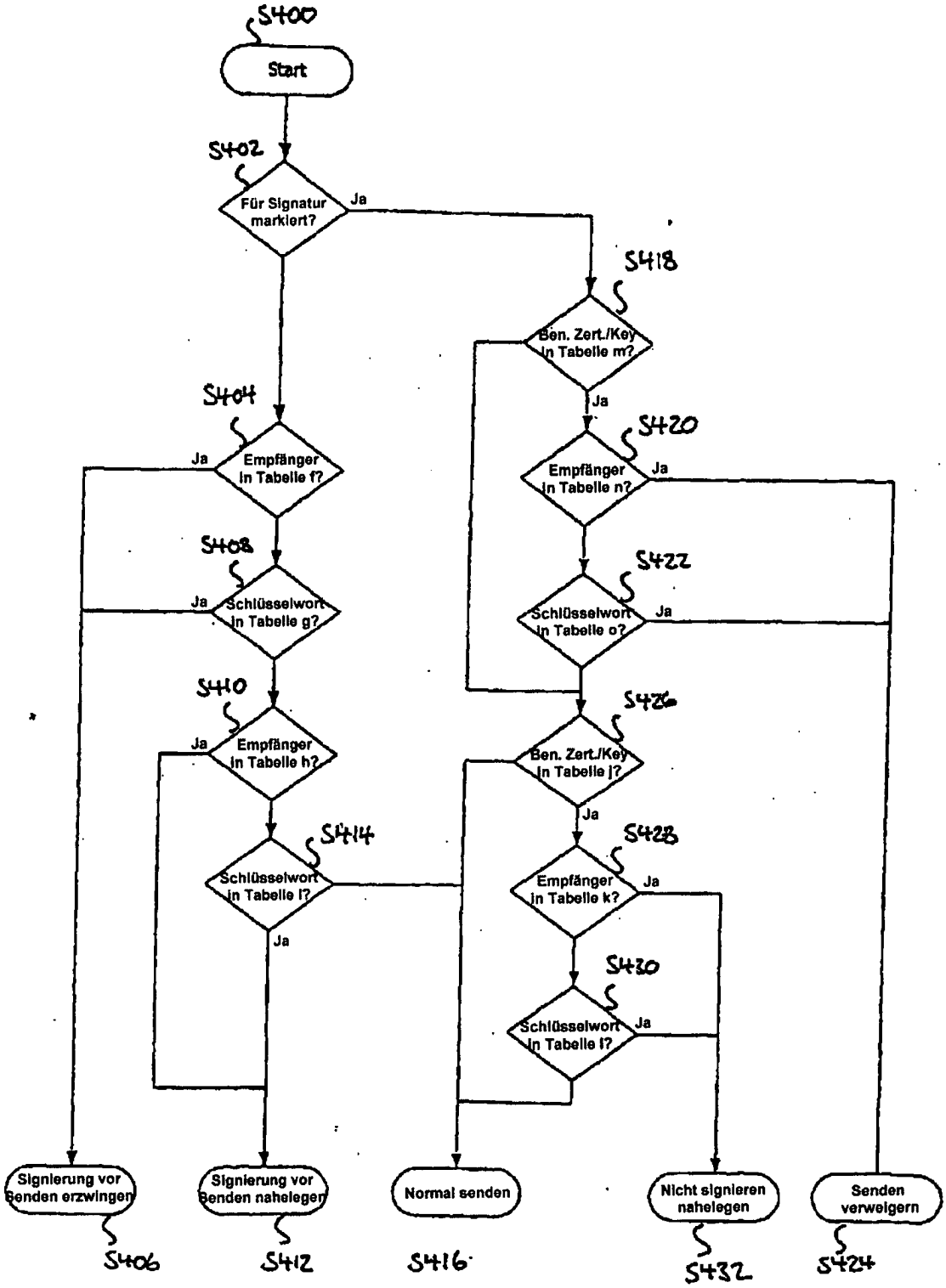

S400
Start
S402
Für Signatur markiert?
Ja
S418
Ben. Zert./Key in Tabelle m?
Ja
S420
Empfänger in Tabelle n?
Ja
S422
Schlüsselwort in Tabelle o?
Ja
S426
Ben. Zert./Key in Tabelle j?
Ja
S428
Empfänger in Tabelle k?
Ja
S430
Schlüsselwort in Tabelle l?
Ja
S404
Ja
Empfänger in Tabelle f?
S408
Ja
Schlüsselwort in Tabelle g?
S410
Ja
Empfänger in Tabelle h?
S414
Schlüsselwort in Tabelle i?
Ja
Signierung vor Senden erzwingen
S406
Signierung vor Senden nahelegen
S412
Normal senden
S416
Nicht signieren nahelegen
S432
Senden verweigern
S424

Fig. 25