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

(10) **DE 697 36 310 T2** 2007.07.05

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 798 892 B1**
(21) Deutsches Aktenzeichen: **697 36 310.4**
(96) Europäisches Aktenzeichen: **97 301 307.1**
(96) Europäischer Anmeldetag: **27.02.1997**
(97) Erstveröffentlichung durch das EPA: **01.10.1997**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **12.07.2006**
(47) Veröffentlichungstag im Patentblatt: **05.07.2007**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)
H04L 9/08 (2006.01)
G07F 7/10 (2006.01)

(30) Unionspriorität:
625475 **29.03.1996** **US**

(84) Benannte Vertragsstaaten:
DE, GB

(73) Patentinhaber:
International Business Machines Corp., Armonk, N.Y., US

(74) Vertreter:
Duscher, R., Dipl.-Phys. Dr.rer.nat., Pat.-Ass., 71034 Böblingen

(72) Erfinder:
Auerbach, Joshua Seth, Ridgefield, Connecticut 06877, US; Chow, Chee-Seng, Cupertino, California 95014, US; Kaplan, Marc Adam, Katonah, New York 10536, US; Crigler, Jeffrey Charles, McLean, Virginia, US

(54) Bezeichnung: **Erzeugung und Verteilung digitaler Dokumente**

Beschreibung

[0001] Diese Erfindung betrifft ein verfahren zur Erzeugung und Verteilung von digitalen Dokumenten, wobei insbesondere die Verfahren und Techniken von sicheren kryptographischen Umschlägen zum Einsatz kommen. Die Erfindung betrifft auch ein Verfahren für den Verkauf und den gesteuerten Zugriff auf digitale Dokumente unter Verwendung derselben Methoden und Techniken.

[0002] Digitale Dokumente haben zahlreiche Vorteile gegenüber papierbasierten analogen Dokumenten. Sie sind einfacher zu erstellen, zu verteilen und zu vervielfältigen. Diese Vorteile machen es jedoch auch schwierig, die mit ihnen verbundenen Rechte an geistigem Eigentum vor Verletzungen zu schützen. Nichtsdestotrotz werden digitale Dokumente papierbasierte Dokumente als Medium für die Verteilung und den Verkauf von Informationen in der Zukunft ersetzen.

[0003] Die US-Patentschrift 5 319 705 beschreibt ein Verfahren und ein System zur sicheren Verteilung einer Vielzahl von Software-Dateien von einem Software-Verteilungsserver an einen Benutzer-Client, während dem Benutzer-Client selektiv ermöglicht wird, eine Teilmenge einer kleineren Vielzahl der Software-Dateien zu nutzen. Ein wichtiger Unterschied zwischen unserer Arbeit und dem Literaturverweis [2] besteht darin, dass der Teil-Verschlüsselungsschlüssel in unserer Offenlegung in dem kryptographischen Umschlag mitgeführt und mit einem öffentlichen Schlüssel verschlüsselt wird. Beim Literaturverweis [2] hingegen enthalten die verteilten Daten nur eine Kennung des Verschlüsselungsschlüssels. Der Verschlüsselungsschlüssel ist auf einem Server gespeichert und wird nach Vorlage der Schlüsselkennung abgerufen. Daher muss beim Literaturverweis [2] eine Schlüsseldatenbank auf dem Server verwaltet werden, die ein gewisses Maß an Vertrauen zwischen einem Kaufserver und einem Dokumentenserver voraussetzt.

[0004] Pretty Good Privacy (PGP) ist ein auf einem öffentlichen Schlüssel beruhendes System zum Versenden von sicheren eMails. Der Hauptteil der eMail wird mit Hilfe eines IDEA-Algorithmus (siehe beispielsweise Literaturverweis [1]) verschlüsselt, und der Verschlüsselungsschlüssel wird mit dem öffentlichen Schlüssel des vorgesehenen Empfängers verschlüsselt. Sowohl der verschlüsselte eMail-Text als auch der verschlüsselte Verschlüsselungsschlüssel werden gesendet. Der Empfänger verwendet seinen privaten Schlüssel, um den Verschlüsselungsschlüssel wiederherzustellen, mit dem dann der unverschlüsselte Text wiederhergestellt wird.

[0005] Ein Verfahren zur Erzeugung, zur Verteilung und zum Verkauf von digitalen Informationen unter Verwendung der Verfahren und Techniken von sicheren kryptographischen Umschlägen wird beschrieben. Kryptographische Umschläge verwenden moderne kryptographische Techniken (wie zum Beispiel Verschlüsselung und die Prüfung der Echtheit beziehungsweise Identität), um Teile von Dokumenten davor zu schützen, dass sie von Unbefugten gelesen und manipuliert werden.

[0006] Der in dieser Offenlegung beschriebene Prozess ermöglicht es einem Benutzer, Teile eines kryptographischen Umschlags zu kaufen und deren Informationsgehalt sicher und kontrolliert freizugeben. Eine zusätzliche Verarbeitung der Teile wird eingeführt, um vor unerlaubter Vervielfältigung abzuschrecken. Außerdem macht der Einsatz der auf einem öffentlichen Schlüssel beruhenden Technologie das Verfahren mit dem kryptographischen Umschlag zu einem praktischen, sicheren und kompakten Mittel zur Verteilung digitaler Informationen.

Superverteilung

[0007] Das grundlegende Modell zur Verteilung von Informationen, das hier angenommen wird, ist die Superverteilung. (Siehe Literaturverweis [5] bezüglich einer eingehenden Erörterung dieses Themas). Die grundlegende Idee besteht darin, dass digitale Dokumente (oder Teile davon) über das Internet, über Funk- oder Fernsehsignale, Kabel, Satellit, lokale Netzwerke, Disketten, CD-ROMs und BBS frei verteilt werden können, solange jedes Dokument verschlüsselt wird. Unter der Annahme, dass der Prozess der Verschlüsselung ausreichend sicher ist, besteht die einzige Möglichkeit für einen Benutzer, Zugriff auf den Inhalt zu erlangen, im Erwerb der notwendigen Teil-Verschlüsselungsschlüssel (part encryption keys, PEKs), die gewöhnlich um viele Größenordnungen kompakter als die Dokumente sind, die sie entschlüsseln.

[0008] Superverteilung ist ein leistungsfähiges Konzept, da es das Problem der Verteilung von Informationen in

(1) die Verteilung von Massendaten; und
(2) die kontrollierte Freigabe von Inhalten durch die Freigabe von PEKs

trennt.

[0009] Diese Erfindung baut auf diesem grundlegenden Konzept auf und führt die Verfahren der kryptographischen Umschläge zur Verteilung und zum Verkauf von Inhalten ein. Außerdem werden die Konzepte und die Verfahren für den Umgang mit beliebigen Bedingungen für den Zugriff auf und die Verwendung von digitalen Dokumenten verallgemeinert. Durch die Verallgemeinerung kann der kryptographische Umschlag als Grundlage für die Gestaltung und die Realisierung der Steuerung des verteilten Zugriffs

auf digitale Dokumente genutzt werden.

[0010] Diese Erfindung macht die Verwaltung einer solchen Schlüsseldatenbank auf dem Server überflüssig und gestattet darüber hinaus eine sauberere Trennung der Vertrauensstellungen zwischen dem Dokumentenserver (dem Ort, an dem Inhalte verschlüsselt werden) und dem Kaufserver (dem Ort, an dem die Verschlüsselungsschlüssel für Dokumente abgerufen werden können).

[0011] Gemäß einem Aspekt der Erfindung wird ein Verfahren zur Bereitstellung des Zugangs zu Inhaltsdaten in einem kryptographischen Umschlag bereitgestellt, wobei das Verfahren Folgendes umfasst: a) Senden einer Anforderung von einem Client-Server, wobei die Anforderung eine Anforderung für den Zugriff auf einen Teil des kryptographischen Umschlags ist, wobei die Anforderung mindestens einen verschlüsselten Teil-Verschlüsselungsschlüssel umfasst, bei dem es sich um eine Verschlüsselung eines Schlüssels mit einem öffentlichen Schlüssel handelt, der zur Verschlüsselung des Teils verwendet wird; b) als Reaktion auf die Anforderung Senden einer Antwort von dem Server an den Client, wobei die Antwort eine Umwandlung des verschlüsselten Teil-Verschlüsselungsschlüssels ist, wobei die Umwandlung gekennzeichnet ist durch: Entschlüsseln des verschlüsselten Teil-Verschlüsselungsschlüssels mit einem geheimen Schlüssel, der zu dem öffentlichen Schlüssel gehört, und Verschlüsseln des Teil-Verschlüsselungsschlüssels mit einem zweiten öffentlichen Schlüssel in dem Server; und Entschlüsseln des umgewandelten Schlüssels in dem Client mit einem zweiten geheimen Schlüssel, der zu dem zweiten öffentlichen Schlüssel gehört, in den Teil-Verschlüsselungsschlüssel, wobei der ausgewählte Teil mit dem Teil-Verschlüsselungsschlüssel in unverschlüsselten Text entschlüsselt wird, wodurch dem Client der Zugriff ermöglicht wird.

[0012] Gemäß einem zweiten Aspekt der Erfindung wird ein Verfahren zur Erzeugung eines kryptographischen Umschlags bereitgestellt, der in beliebiger Weise an eine Vielzahl von Benutzern verteilt werden kann, wobei der Umschlag ein digitales Dokument ist, bei dem es sich um eine Zusammenstellung von Informationsteilen handelt, wobei das Verfahren Folgendes umfasst: a) Verschlüsseln von einem der Informationsteile mit einem Teil-Verschlüsselungsschlüssel, um einen verschlüsselten Teil zu erzeugen, der in den Umschlag aufgenommen wird; b) Verschlüsseln des Teil-Verschlüsselungsschlüssels mit einem ersten öffentlichen Schlüssel, um einen verschlüsselten Teil-Verschlüsselungsschlüssel zu erzeugen, der in den Umschlag aufgenommen wird, wobei der erste öffentliche Schlüssel einen ersten geheimen Schlüssel hat, c) Erstellen einer Liste mit Teilen, die in den Umschlag aufgenommen werden, wobei jeder Eintrag in der Liste einen Teilenamen und einen sicheren Hash-Wert des benannten Teils umfasst, wobei die Liste ebenfalls in den Umschlag aufgenommen wird; und gekennzeichnet ist durch d) Signieren der Liste mit einem zweiten geheimen Schlüssel, um eine Signatur zu erzeugen, die in den Umschlag aufgenommen wird; wobei die Unverfälschtheit der Liste mit einem zweiten öffentlichen Schlüssel geprüft werden kann, der zu dem zweiten geheimen Schlüssel gehört, um die Echtheit der Signatur zu prüfen, und wobei die Unverfälschtheit von einem beliebigen Teil des Umschlags geprüft werden kann, indem ein zweiter sicherer Hash-Wert von dem einen Teil berechnet und der zweite Hash-Wert mit seinem entsprechenden Hash-Wert in der Liste verglichen wird, und wobei der Informationsgehalt des verschlüsselten Teils vor Offenlegung geschützt wird und nur mit dem Teil-Verschlüsselungsschlüssel wiederhergestellt werden kann, und wobei der Teil-Verschlüsselungsschlüssel wiederhergestellt werden kann, indem der verschlüsselte Teil-Verschlüsselungsschlüssel mit dem ersten geheimen Schlüssel, der dem ersten öffentlichen Schlüssel entspricht, entschlüsselt wird.

[0013] Folglich wird ein Verfahren zur Erzeugung eines kryptographischen Umschlags bereitgestellt, der in beliebiger Weise an beliebig viele Benutzer verteilt werden kann, wobei nur berechtigte Benutzer Zugriff auf den Inhalt der sicheren Informationsteile in Form des unverschlüsselten Texts haben. Bei dieser Erfindung wird jeder der Informationsteile mit einem entsprechenden Teil-Verschlüsselungsschlüssel verschlüsselt, um einen verschlüsselten Informationsteil zu erzeugen. Jeder Teil-Verschlüsselungsschlüssel wird dann mit einem öffentlichen Schlüssel verschlüsselt. Eine Liste der Teile, die in den Umschlag aufgenommen werden, wird ebenfalls erstellt, und jeder Eintrag in der Liste hat einen Teilenamen und eine sicheren Hash-Wert des benannten Teils. Der Umschlag enthält dann die verschlüsselten Informationsteile, die nichtverschlüsselten Informationsteile, die verschlüsselten Teil-Verschlüsselungsschlüssel und die Liste der Teile. Abschließend wird die Liste der Teile mit einem geheimen Schlüssel signiert, um eine Signatur zu erzeugen, und diese Signatur wird ebenfalls in den Umschlag aufgenommen. Die Unverfälschtheit der Liste kann mit einem zweiten öffentlichen Schlüssel geprüft werden, der zu dem geheimen Schlüssel gehört, mit dem die Liste signiert wurde. Die Unverfälschtheit von einem beliebigen Informationsteil kann geprüft werden, indem ein zweiter Hash-Wert von dem Teil berechnet und der zweite Hash-Wert mit dem entsprechenden Hash-Wert für den Teil in der Liste verglichen wird. Schließlich wird der Informationsgehalt des verschlüsselten Teils vor Offenlegung geschützt und kann nur mit einem Teil-Verschlüsselungsschlüssel wiederhergestellt werden, und die Kenntnis eines Geheimnisses, das einem öffentlichen Schlüssel entspricht, ist notwendig, um einen unverschlüsselten Teil-Verschlüsse-

lungsschlüssel abzurufen. Letzterer unverschlüsselte Schlüssel wird dann verwendet, um unverschlüsselten Text aus dem Informationsteil zu erzeugen.

[0014] Damit sich dieser und andere Aspekte der vorliegenden Erfindung besser verstehen lassen, wird nun lediglich anhand eines Beispiels und mit Bezug auf die beigefügten Zeichnungen eine Ausführungsform beschrieben, bei denen:

[0015] Fig. 1 einen Überblick über die fünf Schritte des Prozesses der Erzeugung eines kryptographischen Umschlags gibt. Die an dem Prozess beteiligten Hauptinstanzen sind der Dokumentenserver (DS) **100**, der Kaufserver (BS) **102**, das Entschlüsselungs-Fingerabdruck- und Wasserzeichenmarkierungsmodul (DFWM) **103** und der Personal Computer eines Benutzers (UPC) **101**;

[0016] Fig. 2 die Struktur eines typischen kryptographischen Umschlags zeigt. Die Mindestelemente sind ein verschlüsselter Teil **203** und sein zugehöriger verschlüsselter Teil-Verschlüsselungsschlüssel (PEK) **202**, eine Liste der Teile **209** und die Signatur der Liste der Teile **208**;

[0017] Fig. 3 die Struktur einer Stückliste (bill of materials, BOM) zeigt, die eine Teileliste **209** hat. Jeder Tabelleneintrag enthält den Teilenamen **302**, zum Beispiel "Zusammenfassung" ("Abstract"), und die MessageDigest5 (MD5), das heißt, einen sicheren Hash-Wert des benannten Teils **301**, zum Beispiel "13ADBF77F...". Der MD5 der Liste wird berechnet, und der sich ergebende Hash-Wert wird mit dem geheimen Schlüssel des DS signiert, um eine digitale Signatur **208** zu erzeugen. Die Liste **209** und die Signatur **208** bilden die BOM;

[0018] Fig. 4 eine typische Preismatrix zeigt. Die Spalten zeigen den Nachlassfaktor für verschiedene Mitgliedschaftskategorien (**402**, **403**, **404**, **405**), und die Zeilen zeigen den Mengennachlass (**406**, **407**, **408**, **409**). Eine beispielhafte Formel zur Berechnung des Preises des n-ten Exemplars und des Gesamtpreises von n Exemplaren ist bei **401** gezeigt;

[0019] Fig. 5 eine Kaufanforderungsnachricht (Buy Request Message, BRM) **500** zeigt. In der BRM sind die verschlüsselten PEKs (**202**, **211**), die verschlüsselten Fingerabdruck- und Wasserzeichenmarkierungsbefehle **205**, die Bedingungen **206** und die BOM **207** enthalten. Die Elemente **202**, **205**, **206**, **207** und **211** werden aus dem kryptographischen Umschlag **200** (siehe Fig. 2) kopiert. Die anderen Teile der BRM (**501** bis **505**) werden am UPC erzeugt; und

[0020] Fig. 6 eine Antwort des Kaufservers (Buy Server Response, BSR) **600** zeigt. Der Kaufserver (BS) setzt die PEKs um, um umgesetzte PEKs (**602**, **603**) zu erzeugen, die nur das DFWM **103** entschlüsseln kann. Die Fingerabdruck- und Wasserzeichenmarkierungsbefehle werden entschlüsselt, individuell angepasst und wieder verschlüsselt, und das Ergebnis **604** kann nur vom DFWM entschlüsselt werden. Die Bedingungen in der BRM (**500**, Fig. 5) werden ebenfalls ausgewertet und können aktualisierte oder umgewandelte Bedingungen **605** erzeugen. Der tatsächliche Kaufpreis **601** wird berechnet, indem die entsprechenden Nachlässe auf den Basispreis angewendet werden.

[0021] Bezug nehmend auf Fig. 1 besteht einer der Hauptvorteile des Prozesses der Erzeugung eines kryptographischen Umschlags in der Sicherheit. Es wird davon ausgegangen, dass der Kaufserver (BS) **102** und der Dokumentenserver (DS) **100** sicher sind. Sie gehören zum Beispiel den jeweiligen Geschäftspartnern des Unternehmens und werden von diesen verwaltet und von vertrauenswürdigem Personal in einem Glashaus bedient.

[0022] Es wird auch davon ausgegangen, dass es am Personal Computer des Benutzers (UPC) **101** mit Ausnahme eines verhältnismäßig kleinen und sicheren Entschlüsselungs-Fingerabdruck- und Wasserzeichenmarkierungsmoduls (DFWM) **103**, bei dem die Sicherheit in Software oder durch eine gegen Missbrauch geschützte Hardware bereitgestellt wird, keine besonderen Sicherheitsvorkehrungen gibt, da er dem Benutzer gehört.

Überblick über die Schritte

[0023] Nachstehend wird ein Überblick über die Verarbeitungsschritte gegeben (siehe Fig. 1).

[0024] Schritt 1 Erzeugung eines kryptographischen Umschlags

[0025] Schritt 2 Verteilung des kryptographischen Umschlags

[0026] Schritt 3 Durch den Benutzer eingeleitete Kaufanforderung

[0027] Schritt 4 Antwort des Kaufservers

[0028] Schritt 5 Öffnung des kryptographischen Umschlags

Schritte zur Verarbeitung des kryptographischen Umschlags

[0029] Jeder dieser Verarbeitungsschritte wird ausführlicher beschrieben.

Schritt 1: Erzeugung eines kryptographischen Umschlags

[0030] Der erste Schritt ist die Erzeugung eines

kryptographischen Umschlags. Siehe **200** von Fig. 2. Der Vorgang der Erzeugung wird gewöhnlich im verbindungslosen Betriebszustand (offline) vom Inhalteanbieter aufgrund eines vorhergesehenen Bedarfs an einer Auswahl digitaler Dokumente zur Superverteilung durchgeführt.

[0031] Alternativ könnte er durch eine Benutzeranforderung ausgelöst werden. In diesem Fall würde der kryptographische Umschlag speziell für den Benutzer erzeugt werden, und er könnte bestimmte Informationen enthalten, die auf den Benutzer oder die Anforderung zugeschnitten sind. Wenn überdies zu erwarten ist, dass es zukünftig ähnliche Anforderungen von anderen Benutzern geben wird, könnten zusätzliche Informationen in den kryptographischen Umschlag aufgenommen werden, und der kryptographische Umschlag würde im Cachespeicher zwischengespeichert werden, damit zukünftige ähnliche Anforderungen schneller erfüllt werden könnten.

Teile eines kryptographischen Umschlags

[0032] Bei einem kryptographischen Umschlag handelt es sich um eine gruppenweise Zusammenstellung von Informationsteilen. Siehe **201** bis **211** von Fig. 2. Einige der Informationsteile werden verschlüsselt, während andere in Form von unverschlüsseltem Text erscheinen. Der Prozess der Erzeugung eines kryptographischen Umschlags ist mit einer Vielfalt von Gruppierungstechnologien (zum Beispiel zip, tar und die eher objektorientierten Vorgehensweisen von OpenDoc Bento und Microsoft OLE) vereinbar. Die Anforderungen an das Gruppierungsverfahren sind äußerst gering:

(1) Die Teile können zu einer Einheit zusammengestellt werden, die sich zur Verteilung eignet, und die Teile können später einzeln abgerufen werden; und

(2) es sollten Mittel vorhanden sein, mit denen sich verschiedene Teile zum Beispiel durch Namensgebung, Zeiger oder Indexe verknüpfen lassen.

[0033] Es gibt zwei Arten von Informationsteilen: Dokument (**201** und **203**) und Steuerung (**202**, **204** bis **211**). Die Dokumentteile stellen den "Inhalt" dar. Zu Beispielen von Dokumentteilen gehören Zusammenfassungen, Inhaltsverzeichnisse, Figuren, Tabellen und Texte. Sie könnten auch Teile eines ausführbaren Programms, eine Bibliothek mit Unterroutinen, Softwaremodule oder Objektkomponenten sein.

[0034] Bezug nehmend auf Fig. 2 können Dokumentteile verschlüsselt werden (**203**). Verschlüsselte Dokumentteile **203** sind oftmals der "wertvolle Inhalt", der vom Benutzer zu erwerben ist (zum Beispiel ein Teil eines Buches, ein hochauflösendes JPEG-Bild oder ein MPEG-Datentrom). Unverschlüsselte Teile sind die "Appetitmacher" (Teaser) **201** (zum Beispiel Rezensionen von Büchern durch Dritte, das Inhaltsverzeichnis, die Zusammenfassung oder ein JPEG-Bild mit niedriger Auflösung). Die unverschlüsselten Teile haben den Zweck, dem Benutzer die Möglichkeit zu geben, den Inhalt eines kryptographischen Umschlags vor dem tatsächlichen Erwerb "vorab einzusehen", "stichprobenweise zu lesen" oder "zu durchsuchen".

[0035] Eine gewisse Vorverarbeitung wie zum Beispiel die Kompression und das Einfügen von speziellen Zeichenfolgemustern kann auf Teile eines Dokuments angewendet werden. Durch Kompression wird der Speicherplatzbedarf verringert. Eine weitere Vorverarbeitungsoperation besteht in der Durchführung von Änderungen an Teilen eines Dokuments, um die Markierung von Dokumentteilen mit einem Fingerabdruck und einem Wasserzeichen durch das DFWM zu vereinfachen.

[0036] Steuerteile sind die Metadaten, die zur Unterstützung der Funktionen und des Prozessmodells eines kryptographischen Umschlags erforderlich sind. Es gibt zwei Hauptfunktionen: Echtheit und Vertraulichkeit. Die Funktionen des kryptographischen Umschlags werden nicht manipuliert. Diese Funktion zur Überprüfung der Echtheit wird durch Verwendung von digitalen Signaturen erreicht. Die Vertraulichkeitsfunktion wird durch Verschlüsselung (zum Beispiel durch Verwendung des DES- oder des IDEA-Algorithmus) erreicht. Die Grundlagen dieser Verschlüsselungs- und Echtheitsüberprüfungsverfahren sind in der Technik bekannt und finden sich in neueren Texten über Kryptographie (siehe zum Beispiel Literaturverweis [1]). Alle Steuerteile werden auf Echtheit überprüft, und einige können bei Bedarf verschlüsselt werden.

[0037] Beispiele für Steuerteile sind die Preismatrix (siehe die Bezugszahl **400** in Fig. 4) und die Fingerabdruck- und Wasserzeichenmarkierungsbefehle **205** für die Nachverarbeitung der Dokumentteile. Die Nachverarbeitung der Dokumentteile wird von dem DFWM durchgeführt, wenn der kryptographische Umschlag geöffnet ist. Die Markierung mit einem Fingerabdruck und mit einem Wasserzeichen sind Beispiele für die Nachverarbeitung, dabei werden Dokumentteile so markiert, dass eine unerlaubte Vervielfältigung verhindert werden soll.

[0038] Nehmen wir nun Bezug auf Fig. 4. Die Preismatrix **400** beschreibt die Preisbildungsstruktur für den Erwerb der Dokumentteile, zum Beispiel den Mengenrabatt beim Kauf von mehreren Exemplaren, den Nachlass für eine Club-Mitgliedschaft oder den Firmenrabatt. Die Formel **401** ist eine beispielhafte Formel zur Berechnung des Kaufpreises von n Exemplaren eines Dokuments. (Es sei angemerkt, dass der Preisnachlassfaktor auch zeitabhängig sein kann, wobei es sich bei den Spalten der Preismatrix

(**402** bis **405**) in diesem Fall um zeitbegrenzte Sonderangebote anstelle von Preisen aufgrund einer Club-Mitgliedschaft handelt.) Bezug nehmend auf Fig. 2 können die Bedingungen **206** hinsichtlich des Erwerbs und der Verwendung der Dokumentteile auch in den kryptographischen Umschlag aufgenommen werden. Sie können als Dokumentteile (in diesem Fall werden sie für den Benutzer sichtbar gemacht) oder als Steuerteile (in diesem Fall werden sie am Kaufserver (BS) **102** und möglicherweise erneut am Personal Computer des Benutzers (UPC) **101** ausgewertet) aufgenommen werden. Die Dokumentteile enthalten einige Textinformationen, und die Steuerteile können ein Programm (das zum Beispiel in einer Skriptsprache wie Perl (Literaturverweis [4]) geschrieben ist) enthalten, das die Bedingungen umsetzt. (Man beachte die Fingerabdruck- und Wasserzeichenmarkierungsbefehle sowie die Preismatrix. Wir führen sie ausdrücklich der Klarheit halber auf.)

Vertraulichkeit und Echtheit

[0039] Wir beschreiben nun ein Verfahren, bei dem Vertraulichkeit erreicht werden kann. Teile, die von Wert sind, werden mit Hilfe eines Data-Encryption-Standard-(DES-)Algorithmus (siehe zum Beispiel Literaturverweis [1]) verschlüsselt. Verschiedene Teile werden mit verschiedenen PEKs (Teil-Verschlüsselungsschlüssel) verschlüsselt. Diese Schlüssel werden zufällig und unabhängig gewählt.

[0040] Es gibt viele Möglichkeiten, einen zufälligen Verschlüsselungsschlüssel zu erzeugen. Eine Möglichkeit besteht darin, einen Zufallszahlengenerator oder einen Pseudozufallszahlengenerator zu verwenden, um eine zufällige Zahlenfolge zu erzeugen, die als Schlüssel verwendet wird. Weitere Einzelheiten zu diesem Schema finden sich in den Literaturverweisen [1] und [3].

[0041] Jeder PEK wird mit dem öffentlichen Schlüssel eines Kaufservers (BS) **102** verschlüsselt, und der sich daraus ergebende verschlüsselte PEK **202** (Fig. 2) wird ein Steuerteil in dem kryptographischen Umschlag. (Beachte: Ein PEK kann mit verschiedenen öffentlichen Schlüsseln eines BS verschlüsselt werden, und alle diese verschlüsselten PEKs werden in den kryptographischen Umschlag aufgenommen.)

[0042] Es gibt viele Möglichkeiten, die Echtheit eines kryptographischen Umschlags und seiner Teile sicherzustellen. Ein solches Verfahren wird nun von uns beschrieben. Jeder kryptographische Umschlag hat einen speziellen Steuerteil mit der Bezeichnung BOM (Bill of Materials (Stückliste)) **207**. Die BOM besteht aus zwei Teilen:

(1) einer Teileliste **209**; und
(2) einer digitalen Signatur **208**.

[0043] Wir wenden eine sichere Hash-Funktion, MessageDigest 5 (MD5) (siehe zum Beispiel Literaturverweis [1] bezüglich Einzelheiten), auf jeden in einem kryptographischen Umschlag enthaltenen Teil an und erstellen eine Liste. Bezug nehmend auf Fig. 3 enthält jeder Eintrag in der Liste den Namen des Teils oder den Verweis **302** und einen sicheren Hash-Wert **301** des Informationsteils, der dem Namen des Teils entspricht. (Im Falle einer dateibasierten gruppenweisen Zusammenstellung wäre die Teileliste zum Beispiel eine Datei, die die Dateinamen aller Dateien und ihre entsprechenden Hash-Ergebnisse enthielte).

[0044] Die Liste wird dann mit einem geheimen Schlüssel, der nur dem Dokumentenserver (DS) **100** bekannt ist, digital signiert. Es gibt viele Möglichkeiten, ein Dokument digital zu signieren (siehe zum Beispiel Literaturverweis [1]). Eine Möglichkeit besteht darin, den MD5 (oder irgendeinen anderen sicheren Hash-Wert) der Teileliste zu berechnen und den sich daraus ergebenden Hash-Wert mit dem geheimen Schlüssel **208** zu verschlüsseln (um eine Signatur zu erzeugen). Die Teileliste und die Signatur zusammen werden als die BOM **207** bezeichnet. Man beachte, dass nur der öffentliche Schlüssel des DS erforderlich ist, um die Echtheit der BOM zu prüfen.

[0045] Die Echtheit des kryptographischen Umschlags wird geprüft, indem die Signatur mit dem öffentlichen Schlüssel des DS entschlüsselt und mit dem MD5 der Teileliste verglichen wird. Wenn die beiden übereinstimmen, wurde die Teileliste nicht manipuliert. Die Echtheit von einzelnen Teilen kann auch geprüft werden, indem man den MD5 eines jeden Teils berechnet und das Ergebnis mit seinem entsprechenden Eintrag in der Liste vergleicht. Daher stellt die BOM **207** die Unverfälschtheit eines kryptographischen Umschlags und aller seiner Teile sicher.

Der kryptographische Umschlag ist eigenständig

[0046] Ein wichtiges Merkmal des kryptographischen Umschlags ist, dass er im folgenden Sinn eigenständig ist. Nur der öffentliche Schlüssel eines DS ist erforderlich, um die Echtheit des kryptographischen Umschlags zu prüfen. Da die verschlüsselten PEKs (**202**, **210**, **211**, siehe Fig. 2) in dem kryptographischen Umschlag enthalten sind, ist nur der geheime Schlüssel eines BS erforderlich, um den Inhalt wiederherzustellen. Überdies können verschiedene Dokumentenserver kryptographische Umschläge erzeugen, wobei sie nur den öffentlichen Schlüssel des BS zu verwenden brauchen; weitere Datenaustauschoperationen zwischen Kaufservern (BSs) und Dokumentenservern (DSs) sind nicht notwendig.

Schritte zur Erzeugung eines kryptographischen Umschlags

[0047] Wir fassen nun die Verarbeitungsschritte bei

der Erzeugung eines kryptographischen Umschlags zusammen. (Siehe Fig. 2).

1-a Stelle die Informationsteile zusammen, die in den kryptographischen Umschlag aufgenommen werden sollen.

1-b Wende optionale Verarbeitungsschritte (zum Beispiel Kompression, Vorabmarkierung mit einem Fingerabdruck und Vorabmarkierung mit einem Wasserzeichen) auf die Teile an. Bewahre ausreichend viele Zustandsinformationen über diese Verarbeitungsschritte auf, um die Operationen später rückgängig zu machen.

1-c Erzeuge zufällige PEKs (Teil-Verschlüsselungsschlüssel) **202**, einen für jeden zu verschlüsselnden Teil.

1-d Verschlüssele die Dokumententeile mit ihren jeweiligen PEKs, um die verschlüsselten Teile (**203**, **205**, **205**) zu bilden, die in den kryptographischen Umschlag aufgenommen werden.

1-e Die PEKs werden dann mit dem öffentlichen Schlüssel eines BS verschlüsselt, um verschlüsselte PEKs (**202**, **210**, **211**) zu bilden, die in den kryptographischen Umschlag aufgenommen werden. Verschlüsselte PEKs und ihre entsprechenden verschlüsselten Teile sind einander zugeordnet.

1-f Verschlüssele auch die Befehle und andere Zustandsinformationen vom Schritt 1-b mit Hilfe von ein paar zufälligen PEKs. Die PEKs werden mit einem öffentlichen Schlüssel des BS verschlüsselt. Sowohl die verschlüsselten Teile (**203**, **304**, **205**) als auch die verschlüsselten PEKs (**202**, **210**, **211**) werden in den kryptographischen Umschlag eingefügt.

1-g Nimm unverschlüsselte Textteile wie zum Beispiel "Appetitmacher", Zusammenfassungen und ein Inhaltsverzeichnis **201** in den kryptographischen Umschlag auf.

1-h Nimm Bedingungen wie zum Beispiel Fingerabdruck- und Wasserzeichenmarkierungsbefehle **205** und die Preisbildungsmatrix **206** auf. Verschlüssele erforderlichenfalls alle Teile oder Unterteile (und nimm ihre verschlüsselten PEKs auf). Ordne wie bereits zuvor die verschlüsselten Teile ihren verschlüsselten PEKs zu.

1-i Erstelle eine Liste **209** mit den Informationsteilen, und führe dabei alle zusammengestellten Teile auf und berechne einen sicheren Hash-Wert für jeden der aufgeführten Teile.

1-j Erzeuge eine Signatur **208** für die BOM **207**, indem die Liste digital signiert wird, zum Beispiel, indem der sichere Hash-Wert der Liste berechnet und mit dem geheimen Schlüssel des DS verschlüsselt wird. Die BOM **207** (Liste **209** und Signatur **208**) werden zu dem kryptographischen Umschlag hinzugefügt.

[0048] Siehe Fig. 2 bezüglich Einzelheiten über den möglichen Aufbau des kryptographischen Umschlags.

Schritt 2: Verteilung des kryptographischen Umschlags

[0049] Sobald ein kryptographischer Umschlag erzeugt worden ist, kann er über ein beliebiges Mittel verteilt werden, zum Beispiel kann er über das Internet, mittels Funk- oder Fernsehsignalen, über Kabel, Satellit, CD-ROMs und BBS gesendet werden. Eine sichere Verteilung ist nicht erforderlich. Kryptographische Umschläge können kopiert, vervielfältigt und unter Benutzern freigegeben werden. Tatsächlich gehen wir davon aus, dass eine Verteilung eines kryptographischen Umschlags zum Nutzer ("downstream") (d.h. das Kopieren eines kryptographischen Umschlags durch Freunde) eine sehr kostengünstige Möglichkeit darstellt, einen kryptographischen Umschlag zu verteilen. Schließlich kann der kryptographische Umschlag in irgendeinem Server gespeichert werden, ohne dass der Server Sicherheitsanforderungen erfüllen muss.

Schritt 3: Vom Benutzer eingeleitete Kaufanforderung

[0050] Diesem Schritt geht häufig voraus, dass ein Benutzer den als unverschlüsselten Text angezeigten Teil eines kryptographischen Umschlags, den "Appetitmacher" **201**, durchsucht. Ein Benutzer, der an dem Inhalt des kryptographischen Umschlags interessiert ist, müsste die erforderlichen PEKs von dem BS erwerben. (Siehe Fig. 1.)

Grafische Benutzeroberfläche

[0051] Das Durchsuchen des kryptographischen Umschlags wird mit Hilfe einer grafischen Benutzeroberfläche (GUI) wie zum Beispiel eines geänderten Webbrowsers durchgeführt, der die Struktur des kryptographischen Umschlags versteht. Zunächst muss der geänderte Browser in der Lage sein, die Unverfälschtheit des kryptographischen Umschlags zu prüfen. Durch die Prüfung der Unverfälschtheit wird der Benutzer über mögliche Manipulationen an den Teilen des kryptographischen Umschlags informiert. Als Nächstes sollte der Browser die unverschlüsselten Textteile in dem kryptographischen Umschlag anzeigen können, zum Beispiel sollte er die Zusammenfassungen und das Inhaltsverzeichnis anzeigen können. Bezug nehmend auf die Fig. 2 und Fig. 5 muss der Browser schließlich dem kryptographischen Umschlag **200** die Teile entnehmen können, die notwendig sind, um eine Kaufanforderungsnachricht (BRM) **500** zu erstellen.

vorherige Anmeldung

[0052] Wir gehen davon aus, dass der Benutzer den Schritt der vorherigen Anmeldung durchgeführt hat, so dass er von dem BS erkannt wird. Zum Beispiel könnte sich der Benutzer bei einer vertrauenswürdi-

gen dritten Partei anmelden.

[0053] Die Anmeldung könnte beispielsweise einen Telefonanruf des Benutzers bei einem Meldezentrum einschließen, das eine Kontonummer an den Benutzer ausgibt. Die Kontonummer wird dann an alle Kaufserver (BSs) weitergereicht. Alternativ dazu kann das Meldezentrum die Kontonummer digital signieren, wobei in diesem Fall keine Aktualisierung in dem BS erforderlich ist. Ein BS kann die Richtigkeit der Kontonummer einfach prüfen, indem er die Signatur prüft.

[0054] Nach der Anmeldung werden bestimmte Berechtigungsnachweise (credentials) an den Benutzer ausgegeben (zum Beispiel die Kontonummer und andere Informationen über Mitgliedschaften). Ein Berechtigungsnachweis ist ein von einer vertrauenswürdigen dritten Partei digital signiertes Dokument, das Informationen wie zum Beispiel eine Kontonummer, Mitgliedschaften oder Rechte, über die der Benutzer ebenfalls verfügt, enthält. Beispielsweise könnte die dritte Partei bestimmte Berechtigungsnachweise aufgrund einer Mitgliedschaft in einem "Buchclub" an den Benutzer ausgeben, die ihn zu Nachlässen auf den Listenpreis berechtigen würden.

Sicheres DFWM

[0055] Weitaus kennzeichnender für unsere Verfahren ist, dass wir als Folge der Anmeldung davon ausgehen, dass am UPC ein sicheres Entschlüsselungs-Fingerabdruck- und Wasserzeichenmarkierungsmodul (DFWM) (**103**, Fig. 1) realisiert wird.

[0056] Das DFWM ist für die Entschlüsselung der Teile und gleichzeitig für die Durchführung der Markierung mit einem Fingerabdruck und einem Wasserzeichen auf den entschlüsselten Teilen zuständig. Bei der Markierung mit einem Wasserzeichen werden sichtbare Markierungen so in das Dokument eingelassen, dass sie schwer zu entfernen sind und bei der Durchsicht des Dokuments keine Beeinträchtigungen entstehen. Fingerabdrücke sind "unsichtbare" Markierungen in dem Dokument und folglich schwer zu entfernen.

[0057] Weitere Informationen über Markierungsverfahren mit Fingerabdrücken und Wasserzeichen finden sich in der am 23. Juni 1995 eingereichten Anmeldung mit der Seriennummer 08/494 615, die auf denselben Rechtsnachfolger der vorliegenden Anmeldung übertragen wurde.

Realisierung des DFWM

[0058] Es gibt verschiedene Ausführungen eines sicheren DFWM. Die einfachste Ausführung beruht auf den Verfahren mit einem öffentlichen Schlüssel, bei denen das DFWM einen geheimen Schlüssel sicher erzeugt und ihn innerhalb der Sicherheitsgrenze des DFWM speichert. Das DFWM könnte zum Beispiel einen Pseudozufallszahlengenerator verwenden, um ein aus einem öffentlichen Schlüssel und einem geheimen Schlüssel bestehendes Schlüsselpaar zu erzeugen. Der geheime Schlüssel des DFWM wird im DFWM gespeichert, und der öffentliche Schlüssel ist der Außenwelt bekannt. Der Anmeldeprozess ermöglicht der vertrauenswürdigen dritten Partei die Bestätigung des öffentlichen Schlüssels des DFWM. (Siehe zum Beispiel Literaturverweis [1] über den Prozess der Bestätigung eines öffentlichen Schlüssels). Der geheime Schlüssel des DFWM ist die einzige geheime Information, die im DFWM-Modul hinterlegt wird.

Sicherheit des DFWM

[0059] Das DFWM könnte eine Softwarekomponente sein, die in einem physisch sicheren Modul (zum Beispiel in intelligenten Chipkarten) oder in der Umgebung des Personal Computers des Benutzers (die unsicher ist) ausgeführt wird. Im ersteren Fall wird die Sicherheit durch die physische Manipulationssicherheit der Verkapselung erreicht. Die derzeit angewandte Verkapselungstechnologie kann in der Praxis für ausreichend Sicherheit des DFWM sorgen.

[0060] Wir konzentrieren uns auf den letzteren Fall, in dem wir nicht davon ausgehen, dass das DFWM physisch sicher ist. Dies ist der interessantere Fall, da das Vorhandensein von physischer Sicherheit die Sicherheit des DFWM nur erhöht.

[0061] Ohne sichere Hardware kann die Sicherheit des DFWM nicht gewährleistet werden. In vielen praktischen Fällen können wir unter Anwendung von bekannten Software-Verfahren (zum Beispiel Code verschleiernde Techniken, die Virenschreibern wohlbekannt sind) ausreichend Sicherheit erzielen.

[0062] Einer der Hauptvorteile des in dieser Beschreibung dargelegten Prozesses besteht jedoch darin, dass selbst in dem Fall, in dem die Sicherheit des DFWM beeinträchtigt ist, die Offenlegung begrenzt ist. Der Benutzer kann einen Teil eines Dokuments, der nicht erworben wurde (weil der PEK nicht verfügbar ist), nicht freigeben. Die Kauftransaktion ist sicher, da sie über einen sicheren Kaufserver (BS) laufen muss.

[0063] Wenn die Sicherheit eines DFWM beeinträchtigt ist (der geheime Schlüssel des DFWM ist beispielsweise offen gelegt), besteht der einzige mögliche Nachteil darin, dass ein von einem Benutzer erworbenes Dokument nicht ordnungsgemäß mit einem Fingerabdruck und einem Wasserzeichen versehen ist. Die Möglichkeit, dass der Benutzer die Markierungen von dem Dokument entfernt, stellt jedoch ein nahezu gleiches Sicherheitsrisiko dar.

Kaufanforderungstransaktion

[0064] Wir beschreiben nun die Kaufanforderungtransaktion ausführlicher.

[0065] Über die grafische Benutzeroberfläche (GUI) wird dem Benutzer eine Liste mit Artikeln angezeigt, die in dem kryptographischen Umschlag enthalten sind. Der Benutzer kann die entsprechenden Zusammenfassungen nach weiteren Informationen durchsuchen. Der Benutzer kennt möglicherweise auch den Listenpreis der Artikel. Wenn er die Artikel dennoch kaufen möchte, leitet er eine Kaufanforderung über die grafische Benutzeroberfläche ein, was zur Folge hat, dass eine Kaufanforderungsnachricht (BRM) (siehe **500**, Fig. 5) an den BS 102 gesendet wird.

Prüfung der Identität des Benutzers

[0066] Bevor die Kaufanforderung fertig gestellt werden kann, möchte das System gegebenenfalls die Identität des Benutzers prüfen. Es gibt viele bekannte Verfahren zur Identitätsprüfung des Benutzers durch das System. Ein solches Verfahren (das ähnlich dem bei Pretty Good Privacy, Literaturverweis [3]) angewendeten Verfahren ist) besteht zum Beispiel darin, den privaten Schlüssel des Benutzers in verschlüsselter Form auf dem Festplattenlaufwerk seines Personal Computers zu speichern.

[0067] Der Benutzer wird zur Eingabe seines Passworts aufgefordert, mit dem der private Schlüssel entschlüsselt wird. Der private Schlüssel wird verwendet, um eine kaufbezogene Nachricht digital zu signieren oder zu bestätigen, und er wird am Ende einer jeden Sitzung gelöscht.

Umgebungsvariablen

[0068] Umgebungsvariablen sind Informationen über die Benutzerumgebung oder Informationen über den Personal Computer des Benutzers (zum Beispiel Standort, Uhrzeit, Rechnertyp, Bezeichnung des Betriebssystems usw.). Im Gegensatz dazu handelt es sich bei den Benutzer-Berechtigungsdaten um Informationen über den Benutzer.

[0069] Es gibt zwei Arten von Umgebungsvariablen: sichere und unsichere. Sichere Variablen werden bestätigt und digital signiert. Sie können entweder vom BS (während der Anmeldung) geprüft und signiert oder vom DFWM erzeugt und signiert werden.

[0070] Unsichere Variablen werden vom UPC erzeugt. Sie werden weder bestätigt noch signiert. Sie werden lediglich zu Informationszwecken aufgenommen. Im gesamten Dokument sind unter Umgebungsvariablen beide Arten zu verstehen.

Kaufanforderungsnachricbt

[0071] Bezug nehmend auf Fig. 5 enthält die BRM **500** die folgenden Informationen, die aus dem kryptographischen Umschlag (**200**, Fig. 2) kopiert oder diesem entnommen wurden:

3.1 BOM des kryptographischen Umschlags **207**
3.2 Liste der zum Erwerb vorgesehenen Artikel **501**
3.3 PEKs, die zu der Liste mit den Artikeln gehören, und andere Steuerteile (**202** und **211**)
3.4 Bedingungen (wie zum Beispiel die Preismatrix usw.) **206**; und die folgenden Informationen, die aus der Benutzerumgebung oder dem DFWM kopiert oder diesen entnommen wurden oder aber vom Benutzer kopiert oder entnommen wurden:
3.5 Liste der Benutzer-Berechtigungsdaten (zum Beispiel Mitglieds- und Rabattkarten) sowie Informationen **502** in Bezug auf die Prüfung der Identität des Benutzers;
3.6 Umgebungsvariablen (zum Beispiel Datum und Uhrzeit, Standort, DFWM oder Kennung der Rechner-Hardware) **503**;
3.7 der öffentliche Schlüssel **504** des DFWM.

[0072] Standardmäßige kryptographische Verfahren wie zum Beispiel Verschlüsselung und Echtheitsprüfung können auf die BRM angewendet werden. Eine Möglichkeit, die Echtheit der BRM zu prüfen, besteht darin, den MD5 der gesamten BRM zu berechnen und den sich ergebenden MD5 mit dem geheimen Schlüssel des DFWM zu verschlüsseln, um eine Signatur **505** zu erzeugen, die an das Ende der BRM angefügt wird.

[0073] Wir fassen nun die Schritte zusammen, die zur Erzeugung einer BRM führen:

3-a Durchsicht der unverschlüsselten Textteile des kryptographischen Umschlags über die grafische Benutzeroberfläche;
3-b Auswahl der Informationsteile des kryptographischen Umschlags, die erworben werden sollen;
3-c Ausdrückliche Zustimmung des Benutzers zu den Bedingungen **206** des Kaufs (zum Beispiel Listenpreis, Nichtweitergabeverpflichtung);
3-d Aufforderung des Benutzers zur Eingabe eines Passworts zur Identitätsprüfung. (In der Folge werden Informationen in Bezug auf die Identitätsprüfung des Benutzers erzeugt und in die BRM aufgenommen);
3-e Erzeugung der BRM **500** durch die grafische Benutzeroberfläche; und
3-f Senden der BRM an den BS.

[0074] Hinweis: Eine BRM kann als eine spezielle Art eines kryptographischen Umschlags betrachtet werden – nämlich als ein kryptographischer Umschlag in Form einer "Kaufanforderung".

Schritt 4: Antwort des Kaufservers

[0075] Nach dem Empfang einer BRM wird die Antwort des Kaufservers (BSR) gesendet. Wir beschreiben nun ausführlich die von einem Kaufserver (BS) vor dem Versenden einer BSR durchgeführten Maßnahmen.

Benutzerkonto

[0076] Wenn ein BS eine BRM empfängt, prüft er die BOM, um festzustellen, ob die Steuerteile echt sind. Er prüft auch die Echtheit des öffentlichen Schlüssels des DFWM, die Benutzer-Berechtigungsdaten und die Informationen in Bezug auf die Prüfung der Identität des Benutzers. Der Benutzer kann aufgrund des Schritts der vorherigen Anmeldung über ein Konto bei dem BS verfügen, wobei das Benutzerkonto in diesem Fall mit dem entsprechenden Betrag belastet wird (nachdem eventuelle Rabatte, zu denen der Benutzer berechtigt ist, berücksichtigt wurden).

Auswertung der Bedingungen

[0077] Die in dem kryptographischen Umschlag (und auch in der BRM) enthaltenen Bedingungen **206** dienen hauptsächlich zur Sicherstellung, dass der Benutzer die in den Bedingungen dargelegten Voraussetzungen erfüllt hat, die notwendig sind, um den Kauf durchzuführen. Der BS prüft, ob der Benutzer die Voraussetzungen erfüllt hat, indem er die Bedingungen auswertet (ausführt). Das Ergebnis der Auswertung bestimmt, ob der Kauf durchgeführt werden kann. Wenn das Ergebnis positiv ist, erfolgt die Fortsetzung mit den restlichen Schritten; andernfalls wird eine Fehlermeldung in die BSR aufgenommen. Bei einem positiven Ergebnis wird auch der tatsächliche Kaufpreis berechnet, wobei die bei der Preismatrix (**400**) angegebene Formel **401** zur Anwendung kommt.

Schlüsselumsetzung

[0078] Eine der vom BS an einer BRM durchgeführte Maßnahme ist die Schlüsselumsetzung. Wie in Schritt 1 erwähnt wurde, werden Teil-Verschlüsselungsschlüssel (PEKs) mit dem öffentlichen Schlüssel eines BS verschlüsselt. Der BS entschlüsselt die verschlüsselten PEKs mit seinem geheimen Schlüssel. Nach der Entschlüsselung der verschlüsselten PEKs verschlüsselt der BS die PEKs erneut mit dem öffentlichen Schlüssel des DFWM, so dass nur das DFWM PEKs abrufen kann. Dies ist der Schritt der Schlüsselumsetzung.

Individuell angepasste Markierung mit einem Fingerabdruck und einem Wasserzeichen

[0079] Eine weitere Reihe von Maßnahmen, die von dem BS durchgeführt werden, besteht in der individuellen Anpassung der Fingerabdruck- und Wasserzeichenmarkierungsbefehle. Wie im Schritt 1 erwähnt wurde, werden diese Befehle mit dem öffentlichen Schlüssel des BS verschlüsselt und in dem kryptographischen Umschlag als Steuerteile mitgeführt. Der BS würde zuerst die Befehle entschlüsseln und dann Informationen über den Benutzer (zum Beispiel den Benutzernamen, die Mitgliedsnummer) und Informationen über die Transaktion (zum Beispiel das Kaufdatum, Lizenzbeschränkungen, die Transaktionskennung) in die Befehle aufnehmen. Diese Befehle werden dann mit dem öffentlichen Schlüssel des DFWM verschlüsselt. (Das DFWM prüft, ob diese verschlüsselten Fingerabdruck- und Wasserzeichenmarkierungsbefehle vorhanden sind, bevor es das Dokument entschlüsselt.)

Umwandlung der Bedingungen

[0080] Andere Aspekte in Bezug auf die Einschränkungen hinsichtlich der Verwendung des Inhalts sind in der Antwort des Kaufservers (BSR) enthalten. Die in der BRM enthaltenen Bedingungen können erweitert oder modifiziert werden (zum Beispiel können sich die Bedingungen seit der Erzeugung des kryptographischen Umschlags geändert haben). Die sich daraus ergebenden Bedingungen könnten ein paar einfache unverschlüsselte Texte sein, die die Einschränkungen sowie die allgemeinen Bedingungen hinsichtlich der Verwendung der Dokumente angeben. Oder sie könnten ausführbare Befehle, Objekte und Agenten sein, die die Bedingungen durchsetzen. All diese sind in der BSR enthalten.

Schritte bei der Kaufantwort

[0081] Bezug nehmend auf Fig. 6 fassen wir nun die vom BS durchgeführten Schritte vom Empfang einer BRM bis zum Versenden einer BSR zusammen.

4-a Empfang einer BRM

4-b Prüfe die Echtheit der BRM (durch Prüfung der BOM), prüfe die Benutzer-Berechtigungsdaten, prüfe die Informationen in Bezug auf die Identitätsprüfung des Benutzers, prüfe den öffentlichen Schlüssel des DFWM, prüfe Umgebungsvariablen.

4-c Werte die Bedingungen aus, und verwende dabei als Eingaben (von der BRM) die Benutzer-Berechtigungsdaten, die Preismatrix und Umgebungsvariablen und (vom BS) Benutzerinformationen in der Datenbank und weitere Umgebungsvariablen. Die Ausgaben von der Auswertung der Bedingungen sind:

(a) ob dem Benutzer der Zugriff auf die Teile gestattet ist; und

(b) der tatsächliche Preis für den Kauf der Teile **601**.

4-d Prüfe, ob dem Benutzer der Zugriff gestattet ist und ob das Guthaben des Benutzers ausreichend beziehungsweise der Benutzer kreditwür-

dig ist. Wenn nicht, brich ab und sende eine Fehler-BSR.

4-e Setze die PEKs um. (Entschlüssele die PEKs mit dem privaten Schlüssel des BS und verschlüssele die PEKs erneut mit dem öffentlichen Schlüssel des DFWM.) Nimm sie in die BSR (**602**, **603**) auf.

4-f Pass die Fingerabdruck- und Wasserzeichenmarkierungsbefehle individuell an. (Entschlüssele Befehle, nimm benutzerspezifische und transaktionsbezogene Informationen in die Befehle auf. Verschlüssele geänderte Befehle mit dem öffentlichen Schlüssel des DFWM). Nimm sie in die BSR **604** auf.

4-g Nimm die umgewandelten Bedingungen und andere Einschränkungen bezüglich der Verwendung der Dokumente in die BSR **605** auf.

4-h Sende die BSR an den Benutzer.

[0082] Eine BSR kann als eine spezielle Art eines kryptographischen Umschlags betrachtet werden – nämlich als einen "kryptographischen Umschlag in Form von einer Lizenz". Es können wieder standardmäßige kryptographische Verfahren wie zum Beispiel Verschlüsselung und Identitätsprüfung angewendet werden, um die Vertraulichkeit und die Echtheit einer BSR **606** zu schützen. (Siehe zum Beispiel Literaturverweis [1]).

Schritt 5: Öffnen eines kryptographischen Umschlags

[0083] Dies ist der letzte Schritt. Eine Voraussetzung für diesen Schritt ist der Empfang einer BSR vom BS. Nach dem Empfang einer BSR kann der Benutzer den kryptographischen Umschlag zu einem ihm genehmen Zeitpunkt öffnen.

[0084] Die BSR ist der "Schlüssel" zur Freigabe des kryptographischen Umschlags. Der Inhalt der BSR kann nur von dem jeweiligen DFWM verwendet werden, da alle PEKs mit dem öffentlichen Schlüssel des DFWM verschlüsselt werden. Bezug nehmend auf Fig. 6 sind die beim Öffnen eines kryptographischen Umschlags durchzuführenden Schritte wie folgt:

5-a Das DFWM nimmt eine Prüfung vor, um die Echtheit der BSR **606** sicherzustellen. Die Öffnung des kryptographischen Umschlags wird nur fortgesetzt, wenn die Prüfung der BSR auf Echtheit erfolgreich verläuft.

5-b Dem Benutzer können optional die aktualisierten Lizenzbestimmungen **605** in der BSR angezeigt werden. Das Öffnen des kryptographischen Umschlags wird nur fortgesetzt, wenn der Benutzer den Lizenzbestimmungen zustimmt.

5-c Das DFWM prüft die umgesetzten PEKs (**602**, **603**) und die individuell angepassten Fingerabdruck- und Wasserzeichenmarkierungsbefehle (**604**) auf Echtheit und entschlüsselt sie. Die Öffnung des kryptographischen Umschlags wird nur fortgesetzt, wenn die Prüfung auf Echtheit erfolgreich verläuft.

5-d Unter Verwendung der entschlüsselten PEKs entschlüsselt das DFWM die entsprechenden verschlüsselten Teile des kryptographischen Umschlags (**203**, **205**).

5-e Das DFWM wendet die entsprechenden Fingerabdruck- und Wasserzeichenmarkierungsbefehle **604** auf die entschlüsselten Dokumente an. (Die Markierung mit einem Fingerabdruck und einem Wasserzeichen wird individuell auf den Benutzer angepasst, was eine zusätzliche Abschreckung vor unbefugter Verteilung darstellt).

5-f Die sich daraus ergebenden entschlüsselten Dokumente werden außerhalb der Sicherheitsgrenze des DFWM für den Benutzer freigegeben.

[0085] Der Prozess des Erzeugens eines kryptographischen Umschlags kann auch zur Realisierung einer wirksamen, sicheren, verteilten Zugriffssteuerung für äußerst kritische Daten (wie zum Beispiel Krankenakten von Patienten) oder von Datenbanken im Allgemeinen angewendet werden.

[0086] Zusammenfassend kann gesagt werden, dass ein Verfahren und eine Vorrichtung zur Erzeugung, zur Verteilung, zum Verkauf von digitalen Dokumenten und zur Steuerung des Zugriffs auf digitale Dokumente unter Verwendung von sicheren kryptographischen Umschlägen beschrieben wurde. Ein Umschlag ist eine Zusammenfassung von Informationsteilen, wobei jeder der zu schützenden Teile mit einem entsprechenden Teil-Verschlüsselungsschlüssel verschlüsselt wird. Diese verschlüsselten Informationsteile werden zusammen mit den anderen Informationsteilen ein Teil des Umschlags. Jeder Teil-Verschlüsselungsschlüssel wird auch mit einem öffentlichen Schlüssel verschlüsselt, und diese verschlüsselten Teil-Verschlüsselungsschlüssel werden ebenfalls in den Umschlag aufgenommen. Der Umschlag enthält auch eine Liste der Teile, wobei jeder Eintrag in der Liste einen Teilenamen und einen sicheren Hash-Wert des benannten Teils hat. Die Liste wird dann mit einem geheimen Schlüssel signiert, um eine Signatur zu erzeugen, die ebenfalls in den Umschlag aufgenommen wird. Die Echtheit der Signatur kann mit einem zweiten öffentlichen Schlüssel, der zu dem ersten geheimen Schlüssel gehört, geprüft werden, und die Unverfälschtheit eines beliebigen Informationsteils in dem Umschlag kann geprüft werden, indem ein zweiter Hash-Wert berechnet und dieser mit dem entsprechenden Hash-Wert in der Teileliste verglichen wird. Auch kann der Informationsgehalt eines beliebigen verschlüsselten Teils nur in Kenntnis eines zweiten geheimen Schlüssels wiederhergestellt werden, der dem öffentlichen Schlüssel entspricht, welcher zur Verschlüsselung der Teil-Verschlüsselungsschlüssel verwendet wurde.

Literaturangaben

[1] B. Schneier, Applied Cryptography, 2. Auflage Addison Wesley, 1996.
[2] IBM CD-Showcase Patent (US-PATENT Nr 5 319 705, erteilt an B. Halter u.a. am 7. Juni 1994).
[3] S. Garfinkel, Pretty Good Privacy, O'Reilly & Associates, 10 Inc., 1994.
[4] L.W. Wall und R.L. Schwartz, Programming Perl, O'Reilly & W Associates, Inc., 1991.
[5] B. Cox, Superdistribution and Electronic Objects, Dr. Dobb's Journal, Band 17, Nr. 10, Okt. 1992.
[6] US-Patentanmeldung, Seriennummer 08/494,615, A METHOD TO DETER DOCUMENT AND INTELLECTUAL PROPERTY PRIVACY THROUGH INDIVIDUALIZATION, eingereicht am 23. Juni 1995 und auf den Rechtsnachfolger der vorliegenden Anmeldung übertragen.

Patentansprüche

1. Verfahren zur Bereitstellung des Zugangs zu Inhaltsdaten in einem kryptographischen Umschlag, wobei das Verfahren Folgendes umfasst:
a) Senden einer Anforderung von einem Client (**101**) an einen Server (**100**), wobei die Anforderung eine Anforderung für den Zugriff auf einen Teil (**203**) des kryptographischen Umschlags (**200**) ist, wobei die Anforderung mindestens einen verschlüsselten Teil-Verschlüsselungsschlüssel (**202**) umfasst, bei dem es sich um eine Verschlüsselung eines Schlüssels mit einem öffentlichen Schlüssel handelt, der zur Verschlüsselung des Teils verwendet wird;
b) als Reaktion auf die Anforderung Senden einer Antwort von dem Server (**102**) an den Client (**101**), wobei die Antwort eine Umwandlung des verschlüsselten Teil-Verschlüsselungsschlüssels (**202**) ist, wobei die Umwandlung gekennzeichnet ist durch:
Entschlüsseln des verschlüsselten Teil-Verschlüsselungsschlüssels (**202**) mit einem geheimen Schlüssel, der zu dem öffentlichen Schlüssel gehört, und
Verschlüsseln des Teil-Verschlüsselungsschlüssels mit einem zweiten öffentlichen Schlüssel in dem Server (**102**); und
Entschlüsseln des umgewandelten Schlüssels in dem Client (**101**) mit einem zweiten geheimen Schlüssel, der zu dem zweiten öffentlichen Schlüssel gehört, in den Teil-Verschlüsselungsschlüssel, wobei der ausgewählte Teil mit dem Teil-Verschlüsselungsschlüssel in unverschlüsselten Text entschlüsselt wird, wodurch dem Client (**101**) der Zugriff ermöglicht wird.

2. Verfahren zur Erzeugung eines kryptographischen Umschlags (**200**), der in beliebiger Weise an eine Vielzahl von Benutzern verteilt werden kann, wobei der Umschlag ein digitales Dokument ist, bei dem es sich um eine Zusammenfassung von Informationsteilen handelt, wobei das Verfahren Folgendes umfasst:
a) Verschlüsseln von einem der Informationsteile (**203**) mit einem Teil-Verschlüsselungsschlüssel, um einen verschlüsselten Teil zu erzeugen, der in den Umschlag aufgenommen wird;
b) Verschlüsseln des Teil-Verschlüsselungsschlüssels mit einem ersten öffentlichen Schlüssel, um einen verschlüsselten Teil-Verschlüsselungsschlüssel (**202**) zu erzeugen, der in den Umschlag aufgenommen wird, wobei der erste öffentliche Schlüssel einen ersten geheimen Schlüssel hat,
c) Erstellen einer Liste mit Teilen (**209**), die in den Umschlag (**200**) aufgenommen werden, wobei jeder Eintrag in der Liste einen Teilenamen und einen sicheren Hash-Wert des benannten Teils umfasst, wobei die Liste ebenfalls in den Umschlag (**200**) aufgenommen wird; und gekennzeichnet durch
d) Signieren der Liste (**209**) mit einem zweiten geheimen Schlüssel, um eine Signatur (**209**) zu erzeugen, die in den Umschlag (**200**) aufgenommen wird;
wobei die Unverfälschtheit der Liste (**209**) mit einem zweiten öffentlichen Schlüssel geprüft werden kann, der zu dem zweiten geheimen Schlüssel gehört, um die Echtheit der Signatur zu prüfen, und wobei die Unverfälschtheit von einem beliebigen Teil des Umschlags (**200**) geprüft werden kann, indem ein zweiter sicherer Hash-Wert von dem einen Teil berechnet und der zweite Hash-Wert mit seinem entsprechenden Hash-Wert in der Liste verglichen wird, und wobei der Informationsgehalt des verschlüsselten Teils vor Offenlegung geschützt wird und nur mit dem Teil-Verschlüsselungsschlüssel wiederhergestellt werden kann, und wobei der Teil-Verschlüsselungsschlüssel wiederhergestellt werden kann, indem der verschlüsselte Teil-Verschlüsselungsschlüssel mit dem ersten geheimen Schlüssel, der dem ersten öffentlichen Schlüssel entspricht, entschlüsselt wird.

3. Verfahren nach Anspruch 2, das des Weiteren den Schritt des Änderns von jeweils ausgewählten Teilen der Dokumentteile durch Einfügungen, Löschungen oder Änderungen von ausgewählten Wörtern oder Bits in den ausgewählten Teilen und des Aufbewahrens von Zustandsinformationen umfasst, die jeden geänderten Dokumentteil mit seinen Änderungen verknüpfen, um ein entsprechendes nichtgeändertes Dokument wiederherzustellen.

4. Verfahren nach Anspruch 3, wobei die Änderungen auf die jeweils ausgewählten der Teile angewendet werden, bevor der Teil verschlüsselt wird, wobei die Zustandsinformationen mit einem dritten Teil-Verschlüsselungsschlüssel (**211**) verschlüsselt werden, der mit einem dritten öffentlichen Schlüssel verschlüsselt wird,

5. Verfahren nach Anspruch 2, 3 oder 4, wobei der kryptographische Umschlag (**200**) ein Rechnerprogramm enthält, das auf einem Server ausgeführt werden soll, und wobei das Ergebnis der Ausführung nachfolgende Operationen durch den Server be-

stimmt.

6. Verfahren nach Anspruch 5, wobei das Programm die Bedingungen bezüglich des Zugriffs auf die Informationsteile in dem kryptographischen Umschlag (**200**) beschreibt und wobei die Ausführung festlegt, ob der Zugriff auf die Informationsteile gestattet wird.

7. Verfahren nach Anspruch 5, wobei das Programm Befehle zur Änderung eines jeden Dokumentteils umfasst, wobei jeder Teil durch Einfügungen, Löschungen oder Änderungen von ausgewählten Wörtern oder Bits in jedem Teil geändert wird, und wobei Zustandsinformationen, die jeden geänderten Dokumentteil mit seinen Änderungen verknüpfen, aufbewahrt werden, um ein entsprechendes nichtgeändertes Dokument wiederherzustellen.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

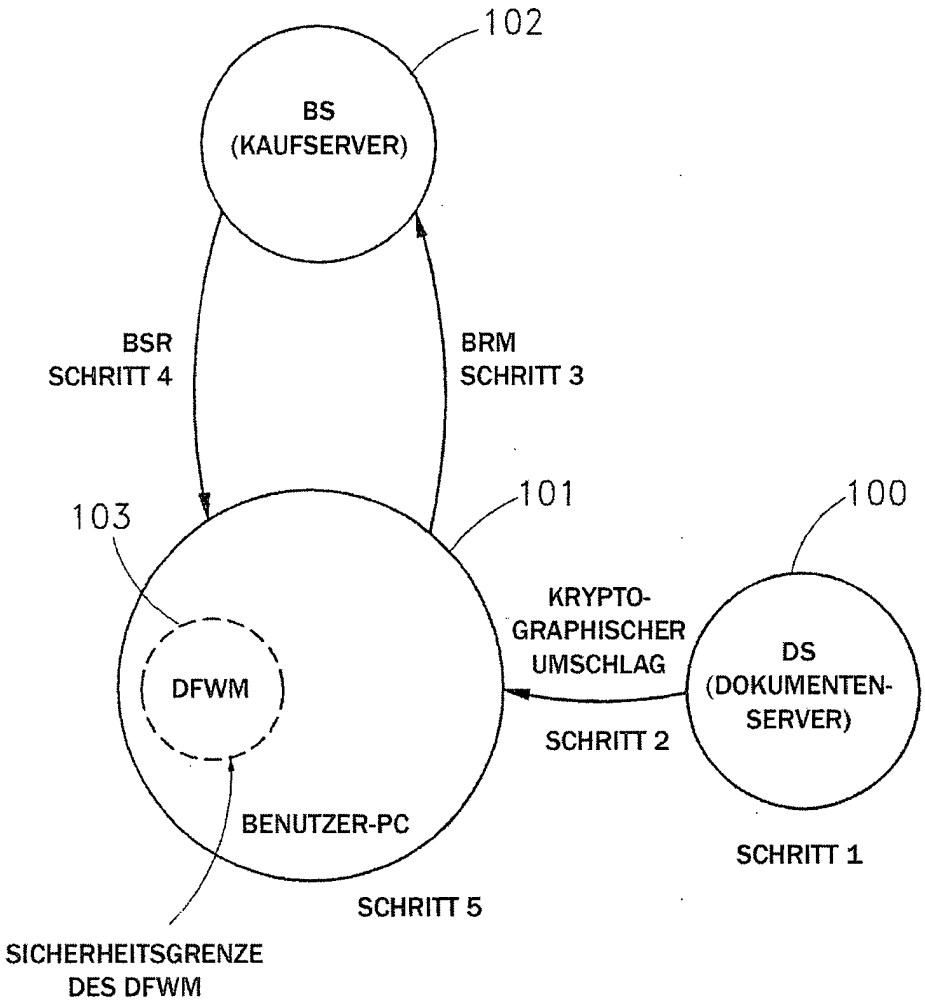

FIG.1

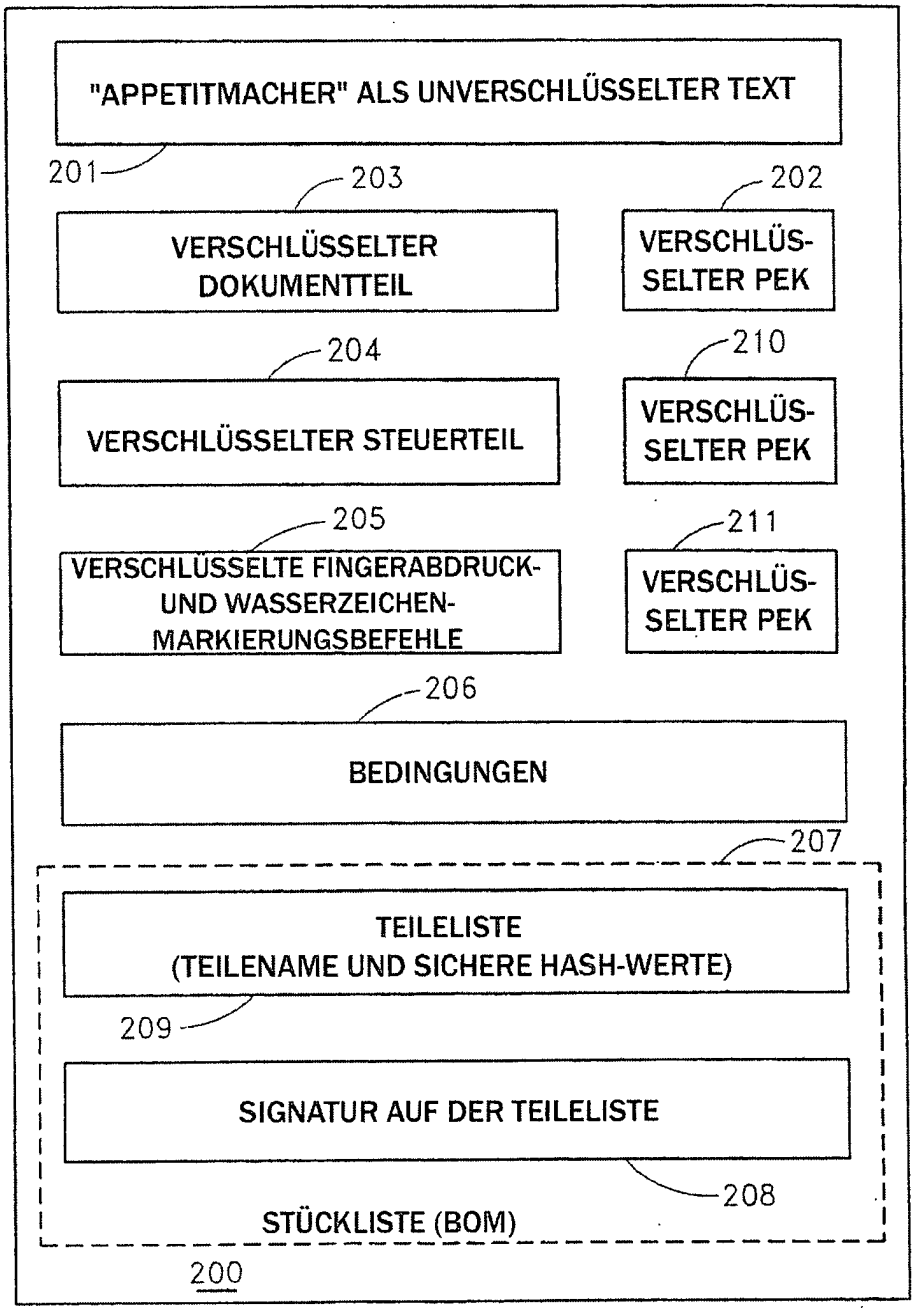
"APPETITMACHER" ALS UNVERSCHLÜSSELTER TEXT
201
203
VERSCHLÜSSELTER DOKUMENTTEIL
202
VERSCHLÜS-SELTER PEK
204
VERSCHLÜSSELTER STEUERTEIL
210
VERSCHLÜS-SELTER PEK
205
VERSCHLÜSSELTE FINGERABDRUCK- UND WASSERZEICHEN-MARKIERUNGSBEFEHLE
211
VERSCHLÜS-SELTER PEK
206
BEDINGUNGEN
207
TEILELISTE (TEILENAME UND SICHERE HASH-WERTE)
209
SIGNATUR AUF DER TEILELISTE
208
STÜCKLISTE (BOM)
200

FIG.2

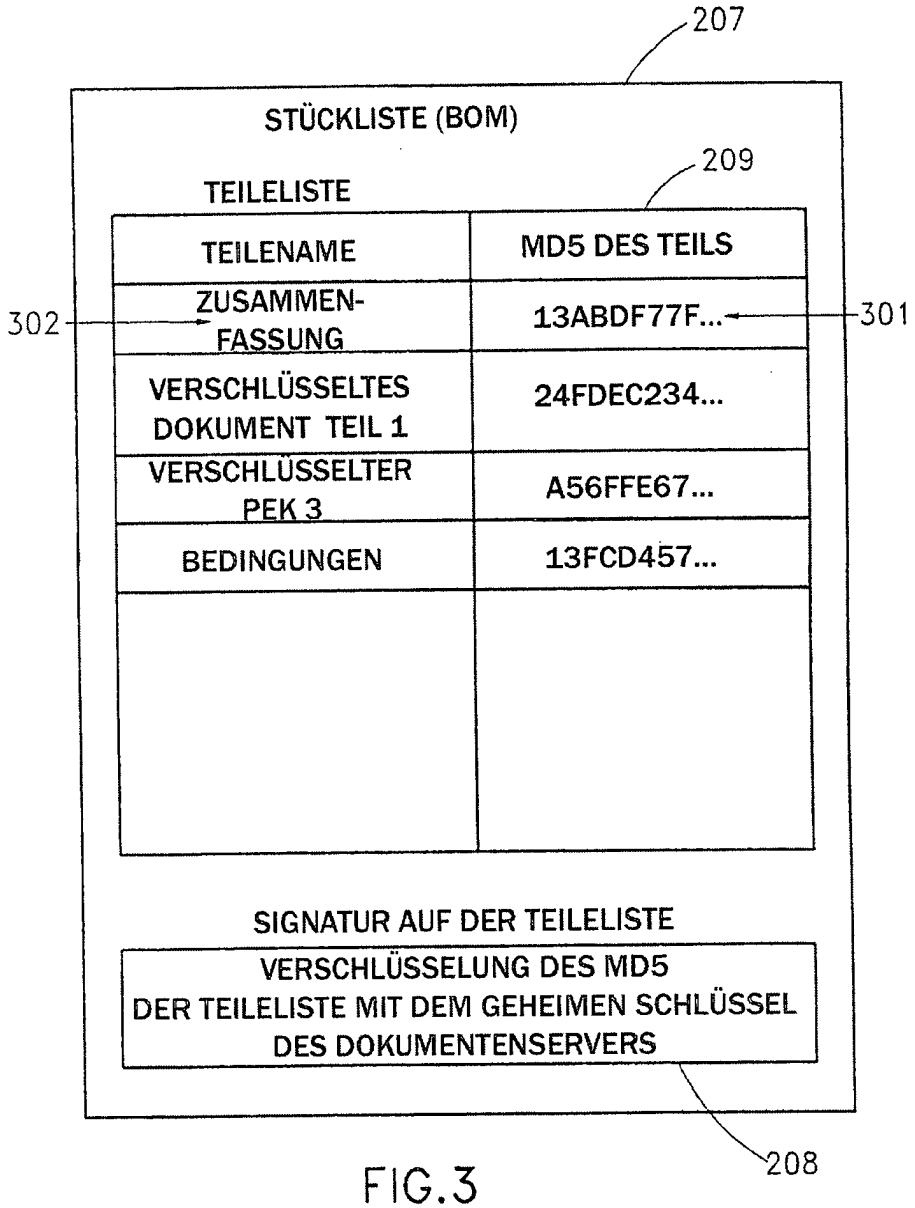
207
STÜCKLISTE (BOM)
209
TEILELISTE
TEILENAME
MD5 DES TEILS
302
ZUSAMMEN-
FASSUNG
13ABDF77F...
301
VERSCHLÜSSELTES
DOKUMENT TEIL 1
24FDEC234...
VERSCHLÜSSELTER
PEK 3
A56FFE67...
BEDINGUNGEN
13FCD457...
SIGNATUR AUF DER TEILELISTE
VERSCHLÜSSELUNG DES MD5
DER TEILELISTE MIT DEM GEHEIMEN SCHLÜSSEL
DES DOKUMENTENSERVERS
208

FIG.3

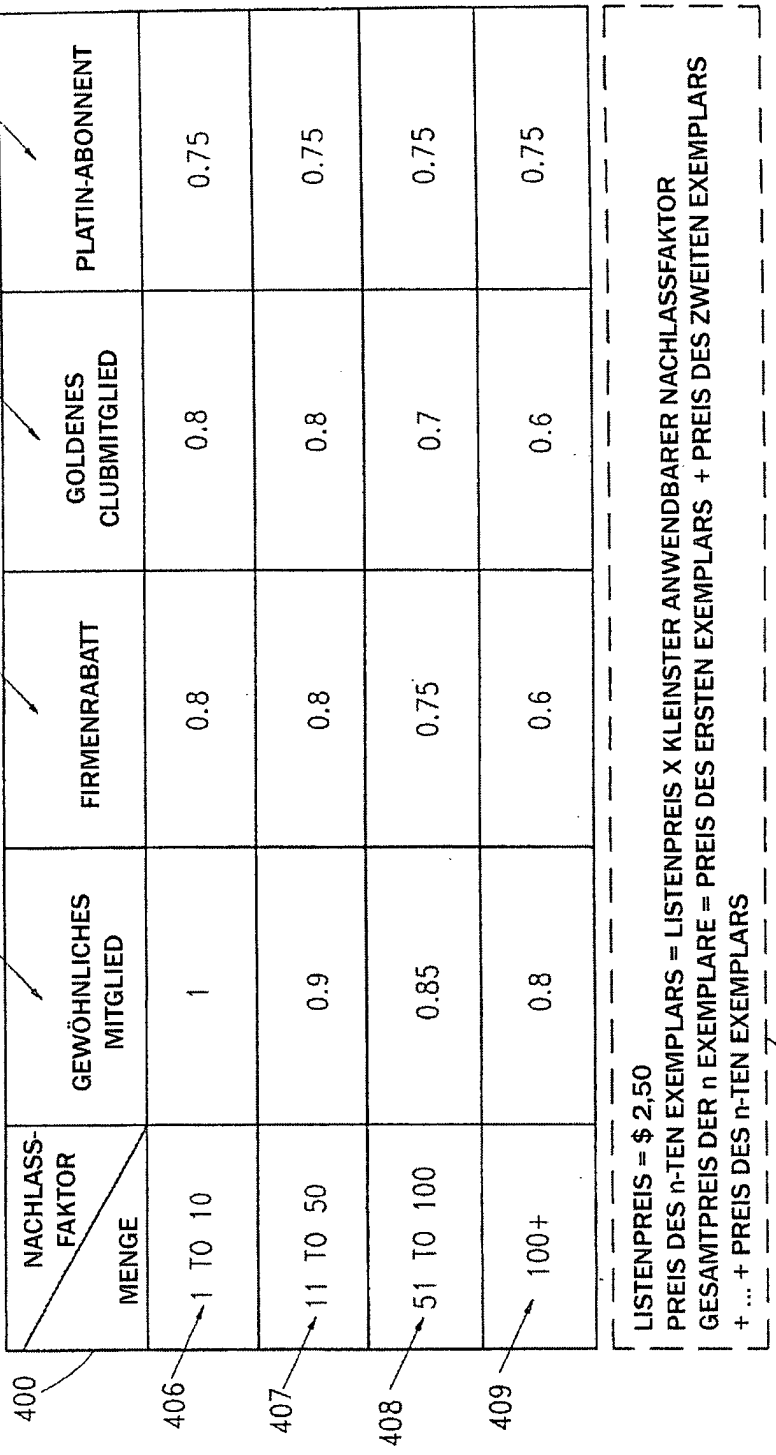
400
NACHLASS-FAKTOR
MENGE
402
GEWÖHNLICHES MITGLIED
403
FIRMENRABATT
404
GOLDENES CLUBMITGLIED
405
PLATIN-ABONNENT
406
1 TO 10
1
0.8
0.8
0.75
407
11 TO 50
0.9
0.8
0.8
0.75
408
51 TO 100
0.85
0.75
0.7
0.75
409
100+
0.8
0.6
0.6
0.75
401
LISTENPREIS = $ 2,50
PREIS DES n-TEN EXEMPLARS = LISTENPREIS X KLEINSTER ANWENDBARER NACHLASSFAKTOR
GESAMTPREIS DER n EXEMPLARE = PREIS DES ERSTEN EXEMPLARS + PREIS DES ZWEITEN EXEMPLARS
+ ... + PREIS DES n-TEN EXEMPLARS

FIG. 4

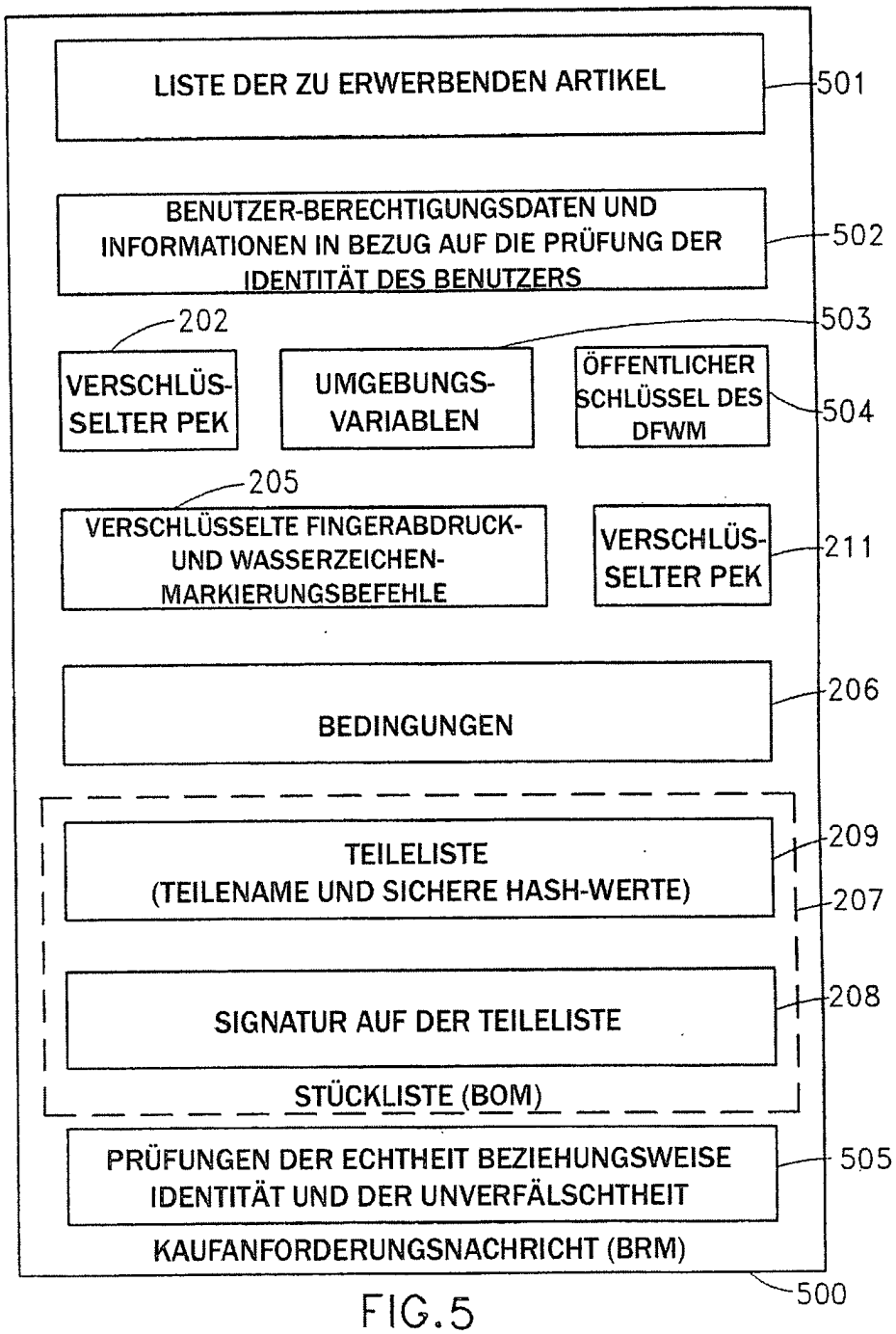
LISTE DER ZU ERWERBENDEN ARTIKEL
501
BENUTZER-BERECHTIGUNGSDATEN UND INFORMATIONEN IN BEZUG AUF DIE PRÜFUNG DER IDENTITÄT DES BENUTZERS
502
202
503
VERSCHLÜS-SELTER PEK
UMGEBUNGS-VARIABLEN
ÖFFENTLICHER SCHLÜSSEL DES DFWM
504
205
VERSCHLÜSSELTE FINGERABDRUCK- UND WASSERZEICHEN-MARKIERUNGSBEFEHLE
VERSCHLÜS-SELTER PEK
211
BEDINGUNGEN
206
TEILELISTE (TEILENAME UND SICHERE HASH-WERTE)
209
207
SIGNATUR AUF DER TEILELISTE
208
STÜCKLISTE (BOM)
PRÜFUNGEN DER ECHTHEIT BEZIEHUNGSWEISE IDENTITÄT UND DER UNVERFÄLSCHTHEIT
505
KAUFANFORDERUNGSNACHRICHT (BRM)
500

FIG.5

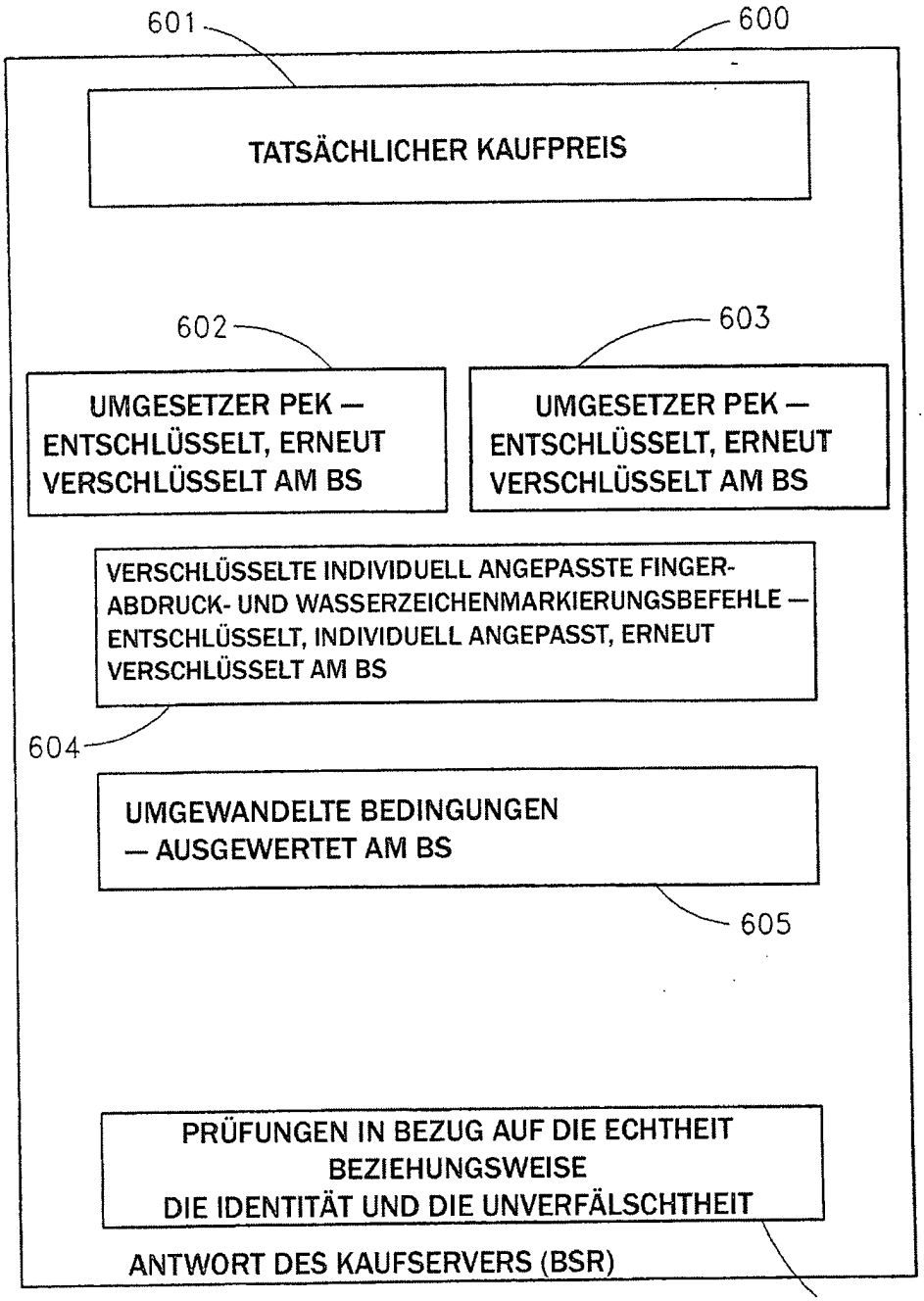
601
600
TATSÄCHLICHER KAUFPREIS
602
603
UMGESETZER PEK — ENTSCHLÜSSELT, ERNEUT VERSCHLÜSSELT AM BS
UMGESETZER PEK — ENTSCHLÜSSELT, ERNEUT VERSCHLÜSSELT AM BS
VERSCHLÜSSELTE INDIVIDUELL ANGEPASSTE FINGER-ABDRUCK- UND WASSERZEICHENMARKIERUNGSBEFEHLE — ENTSCHLÜSSELT, INDIVIDUELL ANGEPASST, ERNEUT VERSCHLÜSSELT AM BS
604
UMGEWANDELTE BEDINGUNGEN — AUSGEWERTET AM BS
605
PRÜFUNGEN IN BEZUG AUF DIE ECHTHEIT BEZIEHUNGSWEISE DIE IDENTITÄT UND DIE UNVERFÄLSCHTHEIT
ANTWORT DES KAUFSERVERS (BSR)
606

FIG.6