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

(10) **DE 602 00 616 T2** 2004.11.04

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 225 500 B1**
(21) Deutsches Aktenzeichen: **602 00 616.3**
(96) Europäisches Aktenzeichen: **02 250 236.3**
(96) Europäischer Anmeldetag: **14.01.2002**
(97) Erstveröffentlichung durch das EPA: **24.07.2002**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **16.06.2004**
(47) Veröffentlichungstag im Patentblatt: **04.11.2004**

(51) Int Cl.[7]: **G06F 1/00**

(30) Unionspriorität:
766142 **19.01.2001** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB, IT

(73) Patentinhaber:
Xerox Corp., Rochester, N.Y., US

(72) Erfinder:
Evans, William D, Cupertino, California 95014, US

(74) Vertreter:
Grünecker, Kinkeldey, Stockmair & Schwanhäusser, 80538 München

(54) Bezeichnung: **Gesicherte Inhaltsobjekte**

Beschreibung

[0001] Die vorliegende Erfindung betrifft im Allgemeinen die Sicherheit elektronischer Dokumente und im Besonderen Systeme und Verfahren zum sicheren Speichern und Verwalten elektronischer Dokumente sowie zum gesteuerten Zugriff auf selbige. Ein anderer Aspekt der Erfindung betrifft die Steuerung des Zugriffs auf Zusatzinformationen, z. B. zu den elektronischen Dokumenten gehörende Anmerkungen (Annotationen).

[0002] Elektronische Dokumente sind der De-facto-Standard für die Informationserstellung, -übertragung und -speicherung geworden. Ein elektronisches Dokument (bzw. eine elektronische Datei oder ein elektronisches Objekt) weisen im typischen Fall Inhaltsinformationen (wie beispielsweise Text, Grafiken, Gleichungen, Tabellen, Tabellenkalkulationen, Bilder, Ton, Bewegtbilder und andere Multimedia-Inhalte, usw.) sowie Formatierungsinformationen auf, die angeben, wie der Inhalt anzuzeigen ist. Verschiedene Arten von Inhaltsinformationen werden leichter verstanden, wenn sie in einer bestimmten Art und Weise formatiert sind. Tabellenkalkulationen lassen sich beispielsweise leichter verstehen, wenn sie in interaktiven Tabellen formatiert sind. Es sind viele verschiedene Anwendungsprogramme bzw. Sprachen entwickelt worden, um Inhaltsinformationen auf spezielle Art und Weise anzuzeigen oder zu formatieren. Jede Sprache, wie beispielsweise Microsoft Word, Adobe Acrobat, HTML usw., definiert einen Satz von Formatierungsregeln, der festlegt, wie die Inhaltsinformationen (z. B. ein Brief, Artikel, Verkaufsinformationen usw.) einem Benutzer angezeigt werden.

[0003] Viele Benutzer haben ein Interesse daran, die Inhaltsinformationen zu schützen, vor allem wenn sich das Dokument nicht in Gebrauch befindet. Das von den Benutzern gewünschte Schutzniveau hängt vom Wert der Inhaltsinformationen ab. Je wertvoller die Inhaltsinformationen sind, desto stringenter sind die von den Benutzern gewünschten Schutzvorkehrungen. Unter Berücksichtigung dessen enthalten viele Anwendungsprogramme Verfahren zum Schutz des Inhalts. Microsoft Word ermöglicht es beispielsweise den Benutzern, Dokumente durch Zuweisen eines Passwortes zu schützen. Das Word-Dokument ist in Klarschrift gespeichert, so dass ein einfallsreicher Hacker das Passwort entfernen und den Dokumentinhalt sehen könnte.

[0004] Das von Adobe Acrobat erzeugte „Portable Document Format", PDF, präsentiert Inhaltsinformationen in einem Format, welches das von dem Autor gewünschte Erscheinungsbild bewahrt und plattformunabhängig ist, wodurch es für die Verwendung über das Internet attraktiv wird. Durch die Acrobat-Software wird ein gewisser Dokument-„Schutz" geschaffen. Ein PDF-Dokument kann zum Schutz von dessen Inhalt verschlüsselt werden. Die Verschlüsselung erfolgt bei allen Zeichenketten und Datenströmen in der PDF-Datei, jedoch nicht bei anderen zum Übertragen von Informationen über die Dokumentstruktur verwendeten Objekten, die nicht zum Inhalt gehören. Der Zugriff auf das „geschützte" PDF-Dokument erfolgt über ein Benutzerpasswort. Während der Inhalt über die Verschlüsselung geschützt ist, gewährleistet das PDF jedoch keine „sichere" Übertragung, d. h. eine Übertragung, bei der die Struktur und/oder andere Informationen über das Dokument nicht sichtbar sind. Selbst wenn ein teilweise verschlüsselter Inhalt vorliegt, kann viel über ein Dokument in Erfahrung gebracht werden, indem das Verhältnis des formatierten Inhalts beobachtet wird oder indem eine Version eines digitalen Dokuments mit einer anderen verglichen wird. Weiterhin ermöglicht das PDF-Format keine durch den Benutzer auszuwählenden Verschlüsselungsebenen und auch keinen Schutz von vorbereitenden Informationen (die häufig die Struktur des Dokuments offen legen), die dem Benutzer zum Eingeben des Passwortes angezeigt werden und die jeder Benutzer vor dem Öffnen der geschützten Teile lesen kann.

[0005] Viele Anwendungsprogramme und Sprachen ermöglichen das Einfügen von Kommentaren, Fußnoten und anderen Arten von Anmerkungen in ein vorhandenes Dokument. Häufig werden Anmerkungen von Personen gemacht, bei denen es sich nicht um den bzw. die Autor(en) des Originaldokuments handelt. Ob eine Person, die nicht der Autor ist, eine Anmerkung zu dem Dokument eines anderen Benutzers machen darf, hängt von dem konkreten Anwendungsprogramm ab und davon, ob dieser Person die Berechtigung erteilt worden ist, Anmerkungen abzugeben. In einem Microsoft Word-Dokument kann beispielsweise jeder beliebige Benutzer, der Zugriff auf ein Dokument hat, Anmerkungen einfügen. Bei Adobe Acrobat bestimmt die Benutzerversion der Adobe Acrobat-Software, ob der Benutzer Anmerkungen machen darf oder nicht. Wenn die Benutzerversion Anmerkungen zulässt, dann wird im Normalfall der Benutzer Änderungen an den Anmerkungen speichern, was dazu führt, dass die Adobe Acrobat-Software die neue Anmerkung und/oder Änderungen an vorhandenen Anmerkungen in einer neuen Version der vorhandenen PDF-Datei einschließt.

[0006] Derartige Anmerkungen können jedoch von sämtlichen Benutzern gelesen werden, die zum Öffnen des Dokuments berechtigt sind (ungeachtet dessen, ob es ein Word-Dokument oder ein PDF- oder ein Dokument eines anderen Typs ist). Es gibt keine Möglichkeit der Begrenzung dahingehend, wer die von einem Benutzer zu der Datei hinzugefügten Anmerkungen lesen oder bearbeiten kann, wenn die neue Version an andere Benutzer mit Zugriff auf eine Software-Anwendung verteilt wird, die Anmerkungen

anzeigt/bearbeitet. So kann beispielsweise der Schutz von Dokumenten, bei denen ein Sicherheitsmechanismus lediglich gewährleistet, dass der Zugriff auf jene begrenzt ist, die das Passwort für das Dokument kennen, nicht als eine allgemeine Lösung betrachtet werden.

[0007] US-A-5953419, US-A-5787175 und US-A-6011847 legen Verfahren zum Erkennen eines elektronischen Dokuments offen, welche umfassen:
Verschlüsseln des elektronischen Dokuments unter Verwendung eines Dokumenten-Verschlüsselungscodes;
Erzeugen einer Mehrfachcode-Verschlüsselungstabelle zur Verwendung in einem Mehrfachcode-Verschlüsselungsverfahren, wobei die Tabelle wenigstens eine Mehrfachcode-Komponente umfasst;
Erzeugen eines verschlüsselten Headers, der Informationen umfasst, die das elektronische Dokument betreffen;
Verknüpfen einer Benutzerschnittstellen-Vorrichtung mit dem verschlüsselten Header, der Mehrfachcode-Verschlüsselungstabelle und dem verschlüsselten elektronischen Dokument, wobei die Benutzerschnittstellen-Vorrichtung unverschlüsselte Informationen zum Identifizieren des elektronischen Dokuments und ein interaktives Element umfasst, das den Benutzer befähigt, eine Benutzer-Berechtigung zum Zugriff auf wenigstens einen Teil des verschlüsselten elektronischen Dokuments einzugeben;
Kombinieren der Benutzer-Berechtigung mit jeder der gespeicherten Mehrfachcode-Komponenten in der Mehrfachcode-Verschlüsselungscodetabelle, um den verschlüsselten Header zu entschlüsseln; und
bei einer gültigen Entschlüsselung des verschlüsselten Headers Entschlüsseln des Abschnitts des verschlüsselten elektronischen Dokuments.

[0008] Nach einem ersten Aspekt der vorliegenden Erfindung ist ein Verfahren zum Schutz eines elektronischen Dokuments dadurch gekennzeichnet, dass der verschlüsselte Header oder das verschlüsselte Dokument eine Verschlüsselungs-Markierung enthält, die eine willkürliche Zahlenfolge umfasst, auf die eine herleitbare Abwandlung dieser willkürlichen Zahlenfolge folgt, wobei eine gültige Entschlüsselung der Verschlüsselungs-Markierung anzeigt, dass der Dokumenten-Verschlüsselungscode gefunden worden ist.

[0009] Nach einem zweiten Aspekt der Erfindung umfasst ein Objekt mit sicherem Inhalt:
ein verschlüsseltes elektronisches Dokument, das mit einem Dokumenten-Verschlüsselungscode verschlüsselt worden ist;
einen verschlüsselten Header, der Informationen umfasst, die das elektronische Dokument betreffen;
eine Mehrfachcode-Verschlüsselungstabelle zur Verwendung in einem Mehrfachcode-Verschlüsselungsverfahren, wobei die Tabelle wenigstens eine Mehrfachcode-Komponente umfasst;
eine Benutzerschnittstellen-Vorrichtung, die unverschlüsselte Informationen zum Identifizieren des elektronischen Dokuments und ein interaktives Element umfasst, das einen Benutzer befähigt, eine Benutzer-Berechtigung zum Zugriff auf wenigstens einen Teil des verschlüsselten elektronischen Dokuments einzugeben, zum Eingeben der Benutzer-Berechtigung in eine Entschlüsselungs-Maschine, die das Mehrfachcode-Verschlüsselungsverfahren verwendet, um die Benutzer-Berechtigung mit jeder der Mehrfachcode-Komponenten in der Mehrfachcode-Verschlüsselungscodetabelle zu kombinieren und den verschlüsselten Header zu entschlüsseln, und
zum Ermöglichen der Entschlüsselung des Teils des verschlüsselten elektronischen Dokuments bei einer gültigen Entschlüsselung des verschlüsselten Headers, dadurch gekennzeichnet, dass der verschlüsselte Header oder das verschlüsselte Dokument eine Verschlüsselungs-Markierung enthält, die eine willkürliche Zahlenfolge umfasst, auf die eine herleitbare Abwandlung dieser willkürlichen Zahlenfolge folgt, wobei eine gültige Entschlüsselung der Verschlüsselungs-Markierung anzeigt, dass der Dokumenten-Verschlüsselungscode gefunden worden ist.

[0010] Nach einem Beispiel der Erfindung enthält ein Objekt mit sicherem Inhalt ein verschlüsseltes elektronisches Dokument, einen verschlüsselten Header, eine Mehrfachcode-Verschlüsselungstabelle und eine Benutzerschnittstellen-Vorrichtung. Das elektronische Dokument und der Header werden mit einem Dokumenten-Verschlüsselungscode verschlüsselt, der zu einem Mehrfachcode-Verschlüsselungsverfahren gehört. Zur höheren Sicherheit können für das elektronische Dokument und den Header verschiedene Verschlüsselungscodes verwendet werden. Die Mehrfachcode-Verschlüsselungstabelle enthält wenigstens eine Mehrfachcode-Komponente (für jeden Verschlüsselungscode, falls verschiedene Codes zum Verschlüsseln des elektronischen Dokuments und des Headers verwendet werden). Für jeden autorisierten Benutzer wird eine gesonderte Komponente in der Tabelle gespeichert. Durch Kombination der Benutzerinformationen (nachstehend definiert) und der Mehrfachcode-Komponente des Benutzers entsteht der Dokumenten-Verschlüsselungscode. Der verschlüsselte Header enthält Informationen zu dem elektronischen Dokument. Die Informationen zu dem elektronischen Dokument können Angaben darüber enthalten, auf welche Teile des Dokuments ein bestimmter Benutzer Zugriff hat und welche Berechtigungen dem Benutzer zugewiesen sind. Wenn mehrere Benutzer Zugriff auf ein bestimmtes Dokument haben oder wenn ein Benutzer Zugriff auf mehrere Dokumente hat, so können diese Informationen in Form einer Benutzer-/Berechtigungstabelle in dem verschlüsselten Header gespeichert sein.

[0011] Der verschlüsselte Header enthält eine Verschlüsselungs-Markierung, die eine willkürliche Zahlenfolge umfasst, auf die eine herleitbare Abwandlung dieser willkürlichen Zahlenfolge folgt. Wenn die Verschlüsselungs-Markierung gültig entschlüsselt ist, ist der korrekte Code gefunden worden. Die Verschlüsselungs-Markierung verwendet eine willkürliche Zahlenfolge, die die Schwächen einer Verschlüsselungs-Markierung mit feststehendem Text umgeht. Eine Verschlüsselungs-Markierung kann ebenfalls am Anfang des verschlüsselten elektronischen Dokuments hinzugefügt werden. Die gültige Entschlüsselung der Verschlüsselungs-Markierung am Anfang des verschlüsselten elektronischen Dokuments bedeutet, dass auch das elektronische Dokument gültig entschlüsselt ist. Oft ist es schwierig, aus der Prüfung des entschlüsselten Dokuments festzustellen, ob die Entschlüsselung richtig ist, vor allem wenn das elektronische Dokument ein unbekanntes Format aufweist.

[0012] Die Benutzerschnittstelle enthält Informationen zum Identifizieren des elektronischen Dokuments und ein interaktives Element. Das interaktive Element ermöglicht es einem Benutzer, eine Benutzer-Berechtigung für den Zugriff zu dem gesamten elektronischen Dokument oder zu Teilen davon einzugeben. Das interaktive Element nimmt die Benutzer-Berechtigung und gibt sie in eine Entschlüsselungsmaschine ein, die Mehrfachcode-Verschlüsselungsverfahren zum Entschlüsseln des verschlüsselten Headers verwendet. Die Entschlüsselungsmaschine kombiniert die Benutzer-Berechtigung mit jeder Mehrfachcode-Komponente, die in der Mehrfachcode-Verschlüsselungstabelle gespeichert ist, und versucht, den verschlüsselten Header zu entschlüsseln. Wenn der verschlüsselte Header gültig entschlüsselt ist, ist der korrekte Code gefunden worden. Anschließend ermöglicht das interaktive Element der Entschlüsselungsmaschine, die autorisierten Teile des verschlüsselten elektronischen Dokuments zu entschlüsseln.

[0013] Wenngleich das Verschlüsselungsverfahren Mehrfachcode-Verschlüsselungsverfahren genannt wird, so können eine oder mehrere Mehrfachcode-Komponenten in der Mehrfachcode-Verschlüsselungstabelle gespeichert werden. Um die Sicherheit zu erhöhen und es schwieriger werden zu lassen, Informationen über die Berechtigung eines Benutzers zu ermitteln, können in der Tabelle zusätzliche Scheinkomponenten gespeichert werden. Weiterhin können die Mehrfachcode-Komponenten in der Tabelle bei jeder Anforderung eines Zugriffs auf ein elektronisches Dokument willkürlich vermischt werden.

[0014] Wenngleich die Mehrfachcode-Verschlüsselungstabelle normalerweise zusammen mit dem Objekt mit sicherem Inhalt gespeichert wird, so kann die Tabelle auch lokal auf dem Computer oder der Arbeitsstation eines Benutzers oder auf einem entfernten Server gespeichert werden.

[0015] Bei der Benutzer-Eingabeberechtigung kann es sich um eine beliebige Benutzer-Eingabeinformation handeln, beispielsweise um eine Benutzer-Kennung (ID) oder einen Namen, ein Passwort oder eine Passphrase. Darüber hinaus kann eine Benutzereingabe von einer biometrischen Eingabevorrichtung allein oder in Kombination mit der Benutzer-Kennung/dem Passwort verwendet werden. Zu einer biometrischen Eingabe gehört beispielsweise ein Fingerabdruck, eine Spracherkennungs-Phrase, ein Augen- oder Iris-Detektor, eine Netzhautprüfung usw.

[0016] Der Dokumenten-Verschlüsselungscode kann mit Hilfe vieler verschiedener Informationen erzeugt werden. Bei dem Mehrfachcode-Verschlüsselungssystem basiert der Dokumenten-Verschlüsselungscode auf Informationen über jeden Benutzer und einer entsprechenden Mehrfachcode-Komponente, die zum Wiederherstellen des Dokumenten-Verschlüsselungscodes benötigt wird. Als Alternative dazu kann der Verschlüsselungscode auf einer Kombination aus Benutzerinformation, der Mehrfachcode-Verschlüsselungskomponente und einer Kennung beruhen, die dem speziellen elektronischen Dokument zugeordnet ist. Auf diese Art und Weise kann für jede Benutzer/Dokument-Kombination ein eindeutiger Code erzeugt werden. Durch das Zuordnen einer Dokumentkennung zu jedem elektronischen Dokument wird eine größere Sicherheit ermöglicht.

[0017] Die Mehrfachcode-Verschlüsselungstabelle enthält keine Informationen, welche die Benutzer oder das Dokument erkennen lassen. Ebenso enthält der verschlüsselte Header keine den Benutzer identifizierenden Informationen oder andere Identifizierungsinformationen bzw. Informationen, die die Art des Dokuments kennzeichnen. Dies trägt zum Scheitern von Hackern bei, die versuchen, die Verschlüsselung zu knacken. Wenn der Hacker den Typ der Datei kennt (die meisten Dateien beginnen mit demselben Zeichen am Anfang der Datei), ist es außerdem einfacher, die Verschlüsselung zu knacken.

[0018] Bei dem elektronischen Dokument kann es sich um jede beliebige Art Dokument handeln, insbesondere sind es jene Dokumente, die Inhaltsinformationen und Formatierungsinformationen enthalten, die angeben, wie der Inhalt angezeigt werden soll. Die Formatierungsinformationen basieren auf einer Objektsprache, wie sie beispielsweise von Microsoft Word, Excel, Power Point, Adobe Acrobat usw. verwendet oder interpretiert wird oder in ihnen enthalten ist, und die einen Satz Formatierungsregeln aufweist.

[0019] Verschiedenen Teilen des elektronischen

Dokuments können unterschiedliche Benutzerberechtigungen zugeordnet sein, wodurch es möglich ist, dass unterschiedliche Benutzer Zugriff auf verschiedene Teile desselben elektronischen Dokuments haben. Mehrere elektronische Dokumente mit jeweils einer anderen Verschlüsselungsebene und einer unterschiedlichen Zugriffsebene können mit der Benutzerschnittstellen-Vorrichtung verknüpft sein. In dem verschlüsselten Header können Informationen über das elektronische Dokument enthalten sein, zu denen eine Benutzer-Berechtigungstabelle gehört, die angibt, welche Benutzer Zugriff auf das Dokument haben und welche Art von Zugriff.

[0020] Wenn das Objekt mit sicherem Inhalt gespeichert oder übertragen wird, ist das elektronische Dokument geschützt, da es verschlüsselt ist. Es kann entweder das gesamte elektronische Dokument verschlüsselt sein (einschließlich der Inhalts- und Formatierungsinformationen) oder es sind nur jene Teile verschlüsselt, deren Schutz gewünscht wird. Wenn ein Benutzer das elektronische Dokument oder einen Teil davon ansehen möchte, auf das/den er Zugriff hat, verhindert die Benutzerschnittstellen-Vorrichtung die Entschlüsselung und die Anzeige des elektronischen Dokuments (oder des Teils) solange, bis die erforderliche Benutzer-Berechtigung eingegeben worden ist.

[0021] Die Benutzerschnittstellen-Vorrichtung kann mit Hilfe der Dokumentensprache als weiteres elektronisches Dokument implementiert sein. Als Alternative dazu kann die Benutzerschnittstellen-Vorrichtung unter Verwendung eines Formats implementiert sein, das nicht rechnerspezifisch ist. Wenn die Benutzerschnittstellen-Vorrichtung als weiteres elektronisches Dokument implementiert ist, kann man es sich als „Deckblatt" vorstellen. Das Deckblatt enthält Informationen in Klartext, die das elektronische Dokument identifizieren, und bietet Zugriffsfunktionen.

[0022] Das erfindungsgemäße Objekt mit sicherem Inhalt ermöglicht es Benutzern, Anmerkungen zu einem vorhandenen elektronischen Dokument (das verschlüsselt oder unverschlüsselt sein kann) zu erzeugen und den Zugriff auf jene Anmerkungen zu begrenzen, während eine verschlüsselte Sicherheit für die Anmerkungen gewährleistet ist. Das Objekt mit sicherem Inhalt kann in jenen Fällen verwendet werden, in denen mehrere Autoren Anmerkungen oder Kommentare zu einem gemeinsamen elektronischen Dokument machen wollen und den Zugriff auf (und das Wissen über) ihre Anmerkungen unter diesen Benutzern steuern wollen. Beispielsweise kann das ursprüngliche elektronische Dokument keine Beschränkungen im Hinblick auf das Betrachten aufweisen (alle Benutzer können es ansehen), so dass es nicht verschlüsselt wird. Einer oder mehrere Benutzer/Autoren (einschließlich des ursprünglichen Autors) können möglicherweise Anmerkungen oder Kommentare zu dem elektronischen Dokument abgeben wollen. Dabei ist es möglich, dass jeder Autor von Anmerkungen den Zugriff auf eine oder mehrere der Anmerkungen begrenzen möchte. Jede dieser Anmerkungen kann verschlüsselt und der Zugriff auf bestimmte Benutzer begrenzt werden.

[0023] Zu dem Zeitpunkt, da der Benutzer seine Anmerkungen hinzufügt/bearbeitet und das elektronische Dokument aktualisiert, kann das vorhandene elektronische Dokument Anmerkungen von anderen Benutzern aufweisen oder auch nicht. In einer Gruppe von drei Benutzern, die gemeinsam ein elektronisches Dokument, wie beispielsweise eine PDF-Datei, nutzen, kann Benutzer 1 das vorhandene elektronische Dokument kommentieren und Benutzer 2 das Recht einräumen, die Anmerkungen anzusehen, dieses Recht jedoch Benutzer 3 vorenthalten. Somit ist Benutzer 3 in der Lage, das vorhandene elektronische Dokument zu betrachten, er kann jedoch nicht auf die Inhalte von Anmerkungen von Benutzer 1 in der gemeinsamen Datei zugreifen, ohne die Verschlüsselung der Anmerkungen von Benutzer 1 zu knacken.

[0024] Die Erfindung schafft ein Verfahren, mit dem Anmerkungen zu einem vorhandenen elektronischen Dokument hinzugefügt werden können, welches einer bestimmten Dokumentsprache entspricht, oder mit dem mehrere elektronische Dokumente mit einer einzigen Schnittstellenvorrichtung verknüpft werden können. Die Anmerkungen (während wahlweise das vorhandene elektronische Dokument in Klarschrift belassen wird) und die elektronischen Dokumente können verschlüsselt werden, um sie geheim zu halten. Das Mehrfachcode-Verschlüsselungsverfahren kann ebenfalls zum Verschlüsseln der Anmerkungen verwendet werden. Der Verschlüsselungscode eines Benutzers wird dazu verwendet, (die Tatsache, dass durch die Benutzerinformationen die Anmerkung entschlüsselt wurde) anzuzeigen, dass der Benutzer Zugriff auf die konkreten Anmerkungen oder auf ein elektronisches Dokument oder Teile davon hat. Ob bestimmte Anmerkungen oder das elektronische Dokument oder Teile davon angesehen werden können, hängt davon ab, wie die Benutzer-Berechtigungsinformationen in einem Mehrfach-Codesystem verwendet werden können.

[0025] **Fig.** 1 ist ein Blockdiagramm eines Objektes mit sicherem Inhalt nach einem erfindungsgemäßen Beispiel; und

[0026] **Fig.** 2 ist ein Blockdiagramm eines Objektes mit sicherem Inhalt, das unter Verwendung des PDF implementiert ist.

[0027] In **Fig.** 1 ist ein Objekt mit sicherem Inhalt **100** abgebildet. Das Objekt mit sicherem Inhalt **100** enthält ein verschlüsseltes elektronisches Dokument

12, einen verschlüsselten Header **11**, eine Mehrfachcode-Verschlüsselungstabelle **13** und Benutzerschnittstellen-Vorrichtung **10**. Die Benutzerschnittstellen-Vorrichtung **10** umfasst eine Klarschrift-Kennung zum Identifizieren des verschlüsselten elektronischen Dokuments **12** und ein interaktives Element, welches bei dieser Ausführungsform in Form von Benutzer-Eingabefeldern **14** abgebildet ist. Das Objekt mit sicherem Inhalt **100** kann in einem Speicher – entweder lokal oder in einem Netzwerk – gespeichert sein. Über einen lokalen Computer oder eine vernetzte Arbeitsstation mit Anzeige **16** kann ein Benutzer auf das Objekt mit sicherem Inhalt **100** zugreifen. Da das elektronische Dokument **12** verschlüsselt gespeichert ist, ist dessen Inhalt vor unbefugten Benutzern geschützt. Das Speichern (und Übertragen) verschlüsselter elektronischer Dokumente stellt sicher, dass der Inhalt vor unbeabsichtigtem Verlust oder Diebstahl geschützt wird (zumindest bis zu der Ebene der Verschlüsselung). Vertrauenswürdige oder befugte Benutzer können die Inhaltsinformationen des elektronischen Dokuments in Klarschrift ansehen, indem eine gewisse Sicherheitsanforderung erfüllt wird, z. B. die Benutzer-Berechtigung wie eine Benutzer-Kennung oder ein Name, ein Passwort oder eine Passphrase, oder eine Benutzereingabe aus einer biometrischen Eingabevorrichtung. Je nach der gewünschten Sicherheitsstufe können ein oder mehrere hinlänglich bekannte Verschlüsselungsverfahren verwendet werden.

[0028] Das elektronische Dokument **12** ist mit Hilfe eines Dokumenten-Verschlüsselungscodes verschlüsselt. Die Mehrfachcode-Verschlüsselungstabelle **13** enthält wenigstens eine Mehrfachcode-Komponente. Für jeden autorisierten Benutzer ist in der Tabelle eine gesonderte Komponente gespeichert. Aus der Kombination von Benutzer-Informationen (wenn autorisiert) und der Mehrfachcode-Komponente des Benutzers wird der Dokumenten-Verschlüsselungscode erzeugt.

[0029] Das Objekt mit sicherem Inhalt wird typischerweise in der Software implementiert, z. B. als Plug-In zu der vorhandenen Anwendung, die zum Erzeugen der konkreten Art des elektronischen Dokuments verwendet wird. Wenn der Benutzer das Anwendungsprogramm öffnet und Zugriff auf ein spezielles elektronisches Dokument anfordert, zeigt das Anwendungsprogramm mit Plug-In (von Computerprozessor ausgeführt) auf der Anzeige **16** einen interaktiven Bildschirm an, so dass der Benutzer die geforderte Berechtigungsinformation eingeben kann. Die Benutzerschnittstellen-Vorrichtung gibt die Benutzer-Berechtigungsinformationen an die Entschlüsselungsmaschine, die die Benutzer-Berechtigungsinformationen mit jeder der Mehrfachcode-Komponenten aus der Tabelle **13** kombiniert, um den verschlüsselten Header **11** zu entschlüsseln. Wenn der verschlüsselte Header gültig entschlüsselt ist, sendet die Benutzerschnittstellen-Vorrichtung das verschlüsselte elektronische Dokument **12** zu einem Entschlüsselungsmodul (ebenfalls vom Prozessor ausgeführt), wo es entschlüsselt wird. Nach Abschluss der Entschlüsselung wird das elektronische Dokument oder ein Teil von ihm – je nach Berechtigung des speziellen Benutzers – dem Benutzer auf der Anzeige **16** angezeigt.

[0030] Die Entschlüsselungsmaschine **18** bringt ein Mehrfachcode-Verschlüsselungsverfahren zur Anwendung. Das Mehrfachcode-Verschlüsselungsverfahren beruht auf einer Mehrzahl von Mehrfachcode-Komponenten, die in der Mehrfachcode-Verschlüsselungstabelle **13** gespeichert sind (die lokal oder entfernt gespeichert sein können). Wenn die Anzahl autorisierter Benutzer unter einer vorher festgelegten Schwellenzahl liegt, können zwecks höherer Sicherheit Scheincodes hinzugefügt werden, um zu verhindern, dass die weniger Fachkundigen die Benutzer-Berechtigungen ermitteln und Zugriff erlangen. Das Mehrfach-Codesystem muss die Benutzer-Berechtigung mit jeder Mehrfachcode-Komponente kombinieren, um den verschlüsselten Header zu entschlüsseln und somit festzustellen, ob die eingegebene Benutzer-Berechtigung (z. B. Benutzer-Kennung/ Passwort/Passphrase oder biometrische Informationen) korrekt ist. Die Entschlüsselungsmaschine **18** kombiniert die eingegebene Benutzer-Berechtigung solange mit jeder gespeicherten Komponente, bis der richtige Code gefunden ist, um den verschlüsselten Header **11** zu entschlüsseln. Der verschlüsselte Header kann eine besondere Verschlüsselungs-Markierung enthalten, die eine willkürliche Zahlenfolge umfasst, auf die eine herleitbare Abwandlung dieser willkürlichen Zahlenfolge folgt. Wenn also festgestellt wird, dass eine Verschlüsselungs-Markierung in dem verschlüsselten Header gültig ist, ist der richtige Code gefunden worden. Anschließend versetzt das interaktive Element die Verschlüsselungs-Markierung in die Lage, das verschlüsselte elektronische Dokument zu entschlüsseln.

[0031] Der Benutzer kann eine Zugriffsberechtigung zum Betrachten des gesamten elektronischen Dokuments in Klarschrift haben oder nicht. Verschiedene Benutzer können Zugriff lediglich auf Teile eines elektronischen Dokuments (z. B. Teilabschnitte, Management-Zusammenfassung, Anmerkungen usw.) haben, woraufhin nach Eingang der Berechtigungsinformationen nur jene Teile entschlüsselt und angezeigt werden.

[0032] Das Objekt mit sicherem Inhalt kann in einem oder mehreren der folgenden Szenarien zur Anwendung kommen: (1) Ein Benutzer mit einem Objekt, dessen Inhalt mit Mehrfachcode gesichert ist, sendet selbiges per Email zu einer Gruppe von Personen, von denen es jede mittels der eigenen Benutzer-Be-

rechtigung öffnen kann. Die Berechtigung zum „Kopieren in Zwischenablage", Drucken, zur Festlegung der Benutzungsdauer des Dokuments usw. unterscheidet sich zwischen den einzelnen Mitgliedern der Gruppe, die das Dokument empfangen. (2) Ein Benutzer hat einige sehr vertrauliche Daten, die in einer binären, formatierten Datei (Bilder, Ton, Marktforschung, Testergebnisse usw.) für eine externe Anwendung vorliegen, zusammen mit einem Dokument, welches genauere Informationen über diese Daten enthält, die ebenfalls hoch sensibel sind. Um diese Dateien verknüpft und sicher zu bewahren, erzeugt der Benutzer ein Objekt mit sicherem Inhalt, welches die Daten und das Dokument enthält. Der Benutzer kann gegebenenfalls einigen Benutzern die binäre Extraktion wahlweise vorenthalten. (3) Eine Personalabteilung verfügt über einige Dokumente, die nur innerhalb der Abteilung verwendet werden sollten, doch in der Vergangenheit sind einige davon auch von gültigen Benutzern innerhalb der Abteilung Außenstehenden zugänglich gemacht worden, die sie außerhalb der Abteilung öffneten. Um dies zu verhindern, stellen sie all ihre Dokumente so ein, dass sie sich nur in ihrem Netzwerk öffnen lassen. (Wenn der Netzwerkschutz richtig funktioniert, verhindert er auch, dass die Dokumente außerhalb der Abteilung gedruckt werden). (4) Ein Unternehmen verfügt über vertrauliche Dokumente, die durch eine hinlänglich bekannte Benutzer-Berechtigung nur ungenügend geschützt sind. Diese Dokumente sollten nicht verteilt werden, doch eines wird auf einem ungeschützten öffentlichen Server gefunden. Sie benutzen den „Fingerabdruck" (wird nachstehend beschrieben) in dem Objekt mit sicherem Inhalt, um das Dokument zu dem Benutzer zurückzuverfolgen, von dem das an falscher Stelle gelandete Objekt mit sicherem Inhalt ausging. (5) Ein Benutzer ist dabei, ein schutzbedürftiges Dokument zu erzeugen, und möchte die Quellendatei für den Fall schützen, dass er seinen Laptop-Computer verliert. Am Ende jeder Bearbeitungssitzung packt der Benutzer diese in ein Objekt mit sicherem Inhalt und löscht die ungeschützte Quellendatei. Eine Variante davon ist, dass der Benutzer ebenfalls die lokale Anwendung einsetzt, um ein PDF des Dokuments in das Objekt mit sicherem Inhalt einzufügen, und verwendet sie, um die Arbeit damit zu prüfen und sie solange mit Anmerkungen für künftige Veränderungen zu versehen, bis mehr Zeit zur Verfügung steht und/oder der Benutzer in einer sichereren Umgebung arbeitet.

[0033] Es sollte erwähnt werden, dass kein Verfahren, einschließlich des Objektes mit sicherem Inhalt, ein Dokument oder eine primäre Datei vor einem böswilligen Nutzer sichern kann, der eine gültige Kennung hat, mit der die Inhalte entschlüsselt werden können. Das Objekt mit sicherem Inhalt kann die Möglichkeiten des Benutzers im Umgang mit den Inhalten verhindern oder Beschränkungen umsetzen. Da jedoch der Benutzer mit dem Computer umgeht, wird es ihm unter Aufbietung einiger Anstrengung immer gelingen, die Inhalte in eine nicht sichere Form zu transferieren (z. B. kann der Benutzer den Bildschirm fotografieren, wenn das Dokument geöffnet ist).

[0034] Die Sicherheit des Objektes mit sicherem Inhalt gegenüber einem Angreifer, der keine gültige Kennung besitzt, ist nur so gut wie das verwendete Verschlüsselungsverfahren.

[0035] Die Sicherheit des gewählten Verfahrens und von dessen Implementierung wird von der konkreten Implementierung bestimmt.

[0036] Zwar kann ein Objekt mit sicherem Inhalt auf dem Personalcomputer eines Benutzers erzeugt werden, es wird jedoch in den meisten Fällen davon ausgegangen, dass die Erstellung auf einem Netzwerkserver stattfindet, bei dem es sich nicht um den Personalcomputer oder eine Arbeitsstation des Benutzers handelt. Allgemein ist ein solcher Server sicher, und er hat Zugriff auf einen zentralen Sicherheitsserver, der Benutzer-Kennungen für eine Gruppe von Benutzern bereitstellen kann. Auf dem Fachgebiet sind viele Wege bekannt, wie diese Benutzer-Kennungen verteilt werden können. Wenn ein Benutzer ein Objekt mit sicherem Inhalt hat, ein gültiger Benutzer des Objektes mit sicherem Inhalt ist und ein weiteres Objekt mit sicherem Inhalt für dieselbe Gruppe von Benutzern erstellen will, dann ist dies möglich, wenn einige Formen der Mehrfachcode-Verschlüsselung angewendet werden. Das nachstehend beschriebene Verfahren gibt die Kennungen der anderen Benutzer in keinem Fall frei, so dass es normalerweise auch auf Benutzer begrenzt ist, die lokale Dokumente schützen, bei denen sie die einzigen Benutzer sind.

[0037] Die Erfindung ist nicht auf ein bestimmtes Anwendungsprogramm zum Erzeugen und Bearbeiten elektronischer Dokumente beschränkt. Aus praktischen Gründen wird die Erfindung jedoch nun genauer mit Hilfe von PDF-Dokumenten beschrieben, die mit der Adobe Acrobat-Software erzeugt wurden.

[0038] BEISPIEL: PDF-Dokumente. Das Portable Document Format (PDF) ist eine Sprache zur Angabe des Dateiformats zur Darstellung von Dokumenten mit Hilfe der Acrobat-Software von Adobe Systems, Inc. Die von Adobe Systems, Inc. veröffentliche Adobe Acrobat-Spezifikation ist das „Portable Document Format Reference Manual, Version 1.3" (PDFRM), deren aktuellste Version unter http://www.adobe.com gefunden werden kann. Verweise in einzelnen Abschnitten betreffen die PDFRM-Version vom März 1999.

[0039] Die folgenden definierten Begriffe des PDFRM werden bei der Beispiel-Ausführungsform ver-

wendet, die durch Verweis auf den Definitionsabschnitt des PDFRM angegeben wird.

[0040] Objekt – Das grundlegende Element in einem PDF. Die Objekte können „direkt" oder „indirekt" sein und in einigen Fällen durch den Gebrauch auf eines von diesem beschränkt sein (Abschnitt 4 des PDFRM).

[0041] Verzeichnisobjekt (Dictionary Object) – Grundlegendes PDF-Objekt, das auf Paaren von Codes und Werten besteht (Abschnitt 4.7 des PDFRM). Das Verzeichnisobjekt kann auch einfach als „Verzeichnis" bezeichnet werden. Viele Verzeichnisse haben einen „Typ", der deren Verwendung definiert, und werden häufig nach ihrem Typ bezeichnet, ohne anzugeben, dass es sich um Verzeichnisse handelt (z. B. Datei-Spezifikation). Im vorliegenden Beispiel bedeutet die Bezeichnung nach dem Typ ein Verzeichnis gemäß PDFRM-Beschreibung.

[0042] Datenfeldobjekt – Wird in diesem Beispiel lediglich unter Verweis auf das Anmerkungs-Datenfeld eines Seitenobjekts verwendet, wie als Teil der Seitenobjekte von Abschnitt 6.4 des PDFRM definiert.

[0043] Datenstromobjekt – Eine der Grundobjektklassen, die ein Verzeichnis und eine Sequenz von Datenbytes enthält. Im vorliegenden Fall werden das Verzeichnis und die notwendigen Standardparameter gemäß Definition aus dem PDFRM verwendet. „Speichern als Datenstromobjekt" bedeutet, dass das Verzeichnis mit dem PDFRM konform gemacht wird und die fraglichen Daten in der Bytefolge des Objektes so angeordnet werden, wie durch das PDFRM definiert (Abschnitt 4.8 des PDFRM).

[0044] Anmerkung (Annotation) – Eine Hinzufügung zu einem PDF-Dokument von einem Benutzer und in Abschnitt 6.6 des PDFRM definiert. Allgemein auf eine beschränkt, die explizit in den Abschnitten 6.6 bis 6.6.15 des PDFRM definiert ist, aber nicht auf jene derart definierten begrenzt. Es ist zu beachten, dass die Pop-up-Anmerkung in diesen Abschnitten definiert ist, jedoch normalerweise nicht direkt als eine von einem Benutzer erstellte Anmerkung erscheint. Im normalen Gebrauch ist eine Pop-up-Anmerkung ein „untergeordnetes Objekt" von einer der anderen Arten von Anmerkungen, die in diesen Abschnitten definiert sind. ‚Nur als untergeordnetes Objekt vorhanden' bedeutet in dem vorliegenden Beispiel, es ist Teil des übergeordneten Objektes, ungeachtet dessen, ob dies explizit angegeben ist oder nicht. (Im Allgemeinen gehören zu den PDFRM-Anmerkungen, wie sie in diesem Beispiel verwendet werden, u. a. aber nicht ausschließlich Text, Stempel, Kreis, Quadrat, Durchgestrichen, Hervorgehoben, Unterstreichen, Farbe und Pop-up.) Weiterhin kann eine Anmerkung auch von anderen Objekten abhängen, die zu der aktuellen PDF-Version gehören. Im vorliegenden Fall schließt eine Anmerkung automatisch diese abhängigen Objekte ein, ungeachtet dessen, ob es direkte oder indirekte sind. Das heißt, eine einzelne Anmerkung könnte viele Teile aufweisen, wenn sie in ein anderes Dokument bewegt oder kopiert werden sollte; zum Zwecke der Erfindung werden diese Teile jedoch als eine einzige Anmerkung behandelt.

[0045] Aktion – Etwas, das geschieht, ausgelöst durch ein Ereignis, bei dem es sich um eines handeln kann, das in Abschnitt 6.8 des PDFRM definiert ist. Normalerweise können zusätzliche Aktionen durch Software-Anwendungen oder Plug-In-Software für diese Anwendungen definiert sein. Eine Aktion bedeutet hier normalerweise eine, die durch die Software definiert ist, um eine Aktivität auszulösen, die als Teil der vorliegenden erfindungsgemäßen Ausführungsform beschrieben und durch eines der Ereignisse aktiviert wird, die im Zusammenhang mit den Widget-Anmerkungen aus Abschnitt 6.14.4 des PDFRM stehen. Konkret kann die Aktion in dem Schaltflächen-Widget (Abschnitt 6.14.7) enthalten sein, mit dem die gesamte Ausführungsform oder Teile von ihr aufgerufen werden.

[0046] Laden der Vorschau – Anwendungen, die ein PDF-Dokument wiedergeben, lesen normalerweise die PDF-Datei und tun, was zum Organisieren der PDF-Objekte in einer Form notwendig ist, die zur Wiedergabe der Inhalte erforderlich ist, wie beispielsweise Seiten, Text, Grafiken usw. Die Operation erfolgt, ehe der Benutzer eine Wiedergabe einer Seite des Dokuments sieht. Im Falle des Objektes mit sicherem Inhalt liegt das Ergebnis dieses Vorbereitungsstadiums des PDF für den Benutzer vor, wenn es bevorzugt wird, dass das PDF durch Hinzufügen von Anmerkungen erfindungsgemäß verändert wird. Zwar ist dies nicht unbedingt der Fall, doch mitunter können die von der Erfindung diktierten Veränderungen künstliche Objekte im Wiedergabevorgang hervorbringen, die der Benutzer als störend empfindend. Das heißt, es ist günstiger, wenn die Veränderungen an dem PDF stattfinden, ehe der Benutzer sie sehen kann. Dies wäre der Fall, wenn sie beim Laden der Seitenansicht erscheinen.

[0047] Widget (Interaktionsbaustein) – Schaltflächen, Textfelder und andere Formen von Anmerkungen, wie in Abschnitt 6.14 des PDFRM angegeben. Von besonderem Interesse ist hierbei das Textfeld aus Abschnitt 6.14.11 und das Schaltflächenfeld aus Abschnitt 6.14.6. Das Textfeld stellt ein Verfahren bereit, mit dem von dem Benutzer Text eingegeben werden kann, und mit Hilfe von „benannten" Feldern kann jener Text mittels Software gelesen werden, während das Dokument betrachtet wird. Das Schaltflächenfeld stellt ein Ereignis bereit, das eine Aktion in Gang setzen kann, die für die erfindungsgemäße Software-Implementierung vertraulich ist. Im vorlie-

genden Beispiel wird durch die Textfeldeinträge ein Verfahren geschaffen, mit dem der Benutzer seine Kennung (Name, Passwort, Passphrase) gegenüber der Software angeben kann. (Der Name „Widget" rührt von dem Untertyp Annotation für diese Elemente her, die auf „Widget" eingestellt werden müssen.)

[0048] Weitere Begriffe, die bei der Ausführungsform des PDF-Beispiels verwendet werden, haben die folgenden Definitionen:

[0049] Plug-In – Software, die mit einer bestimmten Softwareanwendung zusammenarbeitet, welche PDF-Dokumente und Benutzeranmerkungen wiedergibt. Plug-Ins haben Möglichkeiten, die über jene der Grundanwendung hinausgehen, und können die Funktionalität eines Objektes mit sicherem Inhalt oder die Voraussetzung für eine Verschlüsselung betreffen. So kann beispielsweise die erfindungsgemäße Funktionalität eines Objektes mit sicherem Inhalt (einschließlich der Benutzerschnittstellen-Vorrichtung) durch ein Plug-In zu einem Produkt von Adobe Systems, Inc. gewährleistet werden, wobei explizite Verschlüsselungsverfahren durch ein anderes Plug-In für dasselbe Produkt bereitgestellt werden.

[0050] Mehrfachcode-Verschlüsselung – Eines von mehreren gemeinsamen Verfahren, mit denen Daten mit Hilfe eines im Wesentlichen willkürlichen Codes verschlüsselt werden können, die jedoch mit einer bestimmten Benutzer-Kennung von zwei oder mehr Benutzern entschlüsselt werden können. (Normalerweise werden ein Name, Passwort und/oder eine Passphrase oder biometrische Informationen und/oder Kombinationen aus diesen zur Identifizierung verwendet.) Bei korrekter Ausführung wird dadurch normalerweise die Sicherheit der verschlüsselten Daten nicht in Frage gestellt. Bei einer Art der Mehrfachverschlüsselung werden unverschlüsselte Informationen (die in der Mehrfachcode-Verschlüsselungstabelle gespeicherte Mehrfachcode-Komponente) mit den verschlüsselten Daten verknüpft, die es nach Kombination mit dem Verfahren mit Benutzer-Eingabeberechtigung ermöglichen, einen Entschlüsselungscode zu erzeugen, der beim Entschlüsseln der verschlüsselten Datei verwendet wird. Es wird davon ausgegangen, dass das Format dieses Klartextes von der Implementierung abhängig ist, es kann jedoch auch in Daten identifiziert werden, die das Mehrfachcode-Verfahren anwenden. Ein wesentliches Attribut des Verfahrens besteht darin, dass es keine Möglichkeit bietet, von der eingegebenen Benutzer-Berechtigung ausgehend die korrekte Operation zu ermitteln, die einen Entschlüsselungscode erzeugt. Das heißt, die verschlüsselten Daten (gewöhnlich der verschlüsselte Header) muss entschlüsselt und untersucht werden, um festzustellen, ob der richtige Code verwendet wurde. Im schlimmsten Fall kann diese Entschlüsselung und Prüfung so oft stattfinden, wie mögliche Benutzercodes vorhanden sind, und es kann erst, nachdem alle ausprobiert worden sind, festgestellt werden, dass die aktuelle Benutzer-Kennung ungültig ist.

[0051] Verschlüsselungs-Markierung – Eine kurze Datenfolge, die durch die nachstehend beschriebenen erfindungsgemäße Verfahren implementiert wird und die vor den zu verschlüsselnden Daten angeordnet ist, um die Sicherheit der verschlüsselten Daten zu verbessern (angenommen, es kommt eine Chiffrierblock-Kettenbildung zur Anwendung) und um eine Möglichkeit zu schaffen festzustellen, wann der richtige Code zur Entschlüsselung verwendet wurde. Die optimale Länge der Folge kann entsprechend dem Verschlüsselungsverfahren variieren, solange bei dem Versuch der Entschlüsselung der Daten die Markierung eindeutig identifiziert wird. Zum Beispiel könnte man alle verschlüsselten Daten mit 13 willkürlichen Bytes beginnen lassen, auf die eine herleitbare Abwandlung folgt (z. B. eine Permutation) der ersten 13 Bytes. Zwischen den beiden willkürlichen Zahlenfolgen kann eine optionale Klartextphrase eingefügt werden, allerdings wird dadurch die Verschlüsselungs-Markierung weniger sicher. Bei einem Test von Codes mit Mehrfachcode-Verschlüsselungsverfahren an den vorliegenden Daten würde das Auftreten dieser Markierung angeben, dass der richtige Code gefunden wurde, und zwar unabhängig von dem Inhalt der restlichen Daten, die verschlüsselt waren. Die willkürlichen Bytes werden nach dem Stand der Technik erzeugt und stellen sicher, dass es keinen „unveränderlichen Anfang" der zu verschlüsselnden Daten gibt, während dennoch klar angegeben wird, dass der richtige Code vorliegt, ohne dass die Entschlüsselungs-Sofware die geschützten Daten interpretiert.

[0052] Server-Modus – Bei den erfindungsgemäßen Verfahren ist die PDF-Quelle ein Server, der als Verteilerpunkt für alle Benutzer dient. In diesem Modus werden die Anmerkungen zu einem PDF, die allen Benutzern eines PDF-Dokuments zur Verfügung stehen sollen, zu einem Server geschickt, der sie mit den Anmerkungen anderer Benutzer zusammenlegt und allen Benutzern ein neues PDF zur Verfügung stellt. Unter diesem Modus ist nicht unbedingt zu verstehen, auf welchem Computer er läuft, sondern vielmehr die daraus entstehende Aktivität, die zur allgemeinen Verteilung der Anmerkungen erfolgen muss.

[0053] Lokaler Modus – Bei diesem Modus sind die Anmerkungen physisch lokal auf den aktuellen Benutzer begrenzt und stehen anderen Benutzern nicht zur Verfügung. Es wird normalerweise davon ausgegangen, dass diese Veränderungen auf einem einzigen Computer verbleiben, wenn jedoch alle Dateien bewegt werden, gibt es hier keine Einschränkung. Bei diesem Modus bleiben die Anmerkungen solange sicher und vertraulich, bis sie unter Verwendung des Server-Modus zusammengelegt werden. Es sei an-

gemerkt, dass jeder Unterschied im lokalen und Server-Modus mehr mit den ergriffenen Aktionen zu tun hat als mit dem Ort, an dem die Aktion stattfindet – d. h. Server-Modusaktionen könnten auf demselben Gerät erfolgen, das auch der aktuelle Benutzer verwendet.

[0054] Hash – Manchmal auch als „Message Digest" bezeichnet. Die Ergebnisse bzw. der Algorithmus, der aus einer Folge eingegebener Daten eine kurze binäre Folge berechnet. Bei Bezugnahme auf die Kennung eines Benutzers steht hier normalerweise nicht der Klartext des Namens eines Benutzers, ein Passwort oder eine Passphrase, sondern vielmehr wird auf das Ergebnis einer Hash-Funktion an einer Kombination dieser Klartextelemente und auf die Kennung des Objektes mit sicherem Inhalt (OSI) Bezug genommen. Da die Hash-Funktion eine „Einweg"-Funktion ist, versteckt sie wirksam den Text vor jemanden, der dessen Inhalt erfahren möchte, und macht derartige Darstellungen für nur ein einziges OSI. Es können viele verschiedene Hash-Algorithmen zur Anwendung kommen. Bei der aktuellen Implementierung kommt der Secure-Hash-Algorithm, SHA-1, gemäß Federal Information Processing Standards Publication (FIPS PUB) 180-1 zur Anwendung, er ist jedoch implementierungsabhängig. (Ein anderer, weit verbreiteter Algorithmus ist MD-5.)

[0055] Das erfindungsgemäße Objekt mit sicherem Inhalt bietet Sicherheit für ein PDF-Dokument, indem kontrolliert wird, wer ein PDF-Dokument ansehen, drucken, Text herauskopieren oder durch Anmerkungen verändern kann. Zusätzlich zu diesen Beschränkungen im Hinblick auf das Öffnen eines Dokuments zur Ansicht bieten diese Verfahren weiterhin zeitlich begrenzte Ansichten, Rechnerbeschränkungen durch angeschlossene Netzwerke, und sie lassen sich auf beliebige weitere Einschränkungen ausdehnen, die den der Implementierung zur Verfügung stehenden Informationen in dem Moment auferlegt werden können, in dem der Benutzer versucht, ein Dokument zu öffnen,. Es ist nicht notwendig, dass sich der gesicherte Inhalt „ansehen lässt", da diese Verfahren zum Sichern willkürlicher binärer Daten-Dateien über längere Zeiträume hinweg geeignet sind.

[0056] Das Objekt mit sicherem Inhalt kann entweder als ein Plug-In oder als Teil eines PDF-Viewers bzw. Viewer/Editors implementiert sein. Ein Benutzer, der ein PDF erhalten hat, welches sich in einem Objekt mit sicherem Inhalt befindet, würde den Plug-In-Viewer verwenden, um das PDF zu öffnen. Bei einer Ausführungsform des Objektes mit sicherem Inhalt, das mit der Acrobat-Software implementiert ist, kann die Benutzerschnittstellen-Vorrichtung als ein „Deckblatt" implementiert sein. Ein Deckblatt ist ein weiteres PDF-Dokument mit speziellen Attributen, die nachstehend definiert sind. Wenn also der Benutzer einen Plug-In-Viewer für das OSI verwendet, um das verschlüsselte elektronische Dokument zu öffnen, wird dem Benutzer ein einseitiges Dokument „Deckblatt" vorgelegt, das aus zwei Bereichen besteht (welches wie ein anderes PDF-Dokument mit einer Seite aussieht). Ein Bereich der angezeigten Seite enthält die Informationen, für die der Ersteller des PDF den ungehinderten Zugriff gestattet. Zum Beispiel die Art oder der Name des sicheren Dokuments, Einschränkungen, Hinweise zu Sicherheitsebenen, Gebrauchswarnungen, Daten, Zeitpunkte und andere uneingeschränkte, allgemeine Informationen, die für jemanden nützlich sind, der zufällig eine Kopie der Datei bekommen hat und diese öffnet.

[0057] Der andere Bereich des Deckblattes enthält Widget-Anmerkungen, die aus zwei oder drei Textfeldern bestehen (und optional Steuereinheiten zum Aktivieren einer Vorrichtung zwecks Eingeben biometrischer Daten des Benutzers) sowie aus ein oder zwei Schaltflächenfeldern. (Die Anzahl von Text- und Schaltflächenfeldern hängt von der Informationsmenge ab, die benötigt wird. Jede beliebige Anzahl kann verwendet werden.) Die Textfelder sind gekennzeichnete Eingabestellen für den Benutzer zum Eingeben des Namens (z. B. einfaches Textfeld), eines Passwortes (Rückmeldung erfolgt mit „*") und einer Passphrase (Rückmeldung erfolgt wie beim Passwort mit „*"). Es liegt an dem Ersteller des PDF, sowohl das Passwort als auch eine Passphrase anzugeben oder nur eines von ihnen als Teil der Benutzer-Kennung zu verwenden. Die Schaltflächenfelder sind mit dem Aktions-Verzeichnis verknüpft, welches vertrauliche Aktionen angibt, die von der erfindungsgemäßen Implementierung unterstützt werden. Die Implementierung dieser vertraulichen Aktionen ist verantwortlich dafür, dass entweder das PDF geöffnet wird oder eine binäre, sichere Datei aus dem PDF extrahiert wird, je nachdem, mit welchem Schaltflächenfeld es/sie verknüpft ist und ob der Benutzer die richtige Information eingegeben hat oder nicht.

[0058] Bei der PDF-Implementierung kann das verschlüsselte PDF-Dokument der verschlüsselte Inhalt sein (mit geringer oder gar keiner verschlüsselten Formatierung), wie oben beschrieben, oder ein vollständig verschlüsseltes PDF. Diese beiden Verschlüsselungsszenarien funktionieren innerhalb der Beschränkungen des PDF-Formats. Allerdings kann ein Benutzer ein PDF-Dokument mit Hilfe eines bekanten Verschlüsselungsverfahrens auch so verschlüsseln, dass das Format nicht erhalten bleibt. Ein Vorteil der Verwendung der von Acrobat definierten Verschlüsselung besteht darin, dass binäre Dateien (Teile des PDF-Dokuments) mühelos extrahiert werden können.

[0059] Wenn durch die Maus eine Aktion der Befehlsschaltfläche ausgelöst wird, liest das interaktive Element die Benutzer-Kennung von den Textfeldern ab und versucht mit ihr, einen verschlüsselten Ab-

schnitt des Zielobjekt-Datenstroms der Befehlsschaltfläche zu öffnen. Wenn sich dieser Abschnitt entschlüsseln lässt, zeigt dies an, dass die Benutzer-Kennung gültig ist, und, vorausgesetzt, dass es keine Berechtigungseinschränkungen für diesen Benutzer/Rechner gibt, kann die Dateiaktion abgeschlossen werden. Bei einem voll verschlüsselten PDF wird durch diese Aktion das Deckblatt durch das entschlüsselte PDF ersetzt, wie in den folgenden Abschnitten erläutert wird, oder bei dem binären Inhalt wird der Benutzer darüber befragt, wohin eine nicht verschlüsselte Version der binären Datei platziert werden soll, worauf die Extraktion der Datei an der angegebenen Stelle erfolgt.

[0060] Die vorliegende Ausführungsform verwendet das PDF, um die Information über die Benutzer-Berechtigung zu erhalten, und kein rechnerabhängiges Verfahren. Durch Ausnutzen der Möglichkeiten des PDF zur Erlangung dieser Informationen erhält die Implementierung einen gewissen, normalerweise nicht verfügbaren Grad der Unabhängigkeit von dem Betriebssystem des Rechners. Es ist anzumerken, dass es sich bei dem Deckblatt auch um ein rechnerabhängiges Verfahren handeln könnte, wenn dies gewünscht wird. Ob das entschlüsselte PDF das Deckblatt ersetzt oder sich in einem anderen Fenster öffnet, ist abhängig von der Implementierung und von dem Viewer. Gleiches gilt auch für die verwendeten Verfahren, durch die die Implementierung mit dem Benutzer in Interaktion tritt, um die Zielstelle zu erfahren, an der die extrahierte binäre Datei platziert werden soll.

[0061] Das Objekt mit sicherem Inhalt versteckt alle Informationen über das elektronische Dokument (z. B. das PDF), da die Inhalte und Formatierungsinformationen vollständig mittels eines Verschlüsselungsverfahrens verschlüsselt sind, das von dem konkreten Benutzer oder einer Implementierung oder durch die Tatsache ausgewählt wird, dass der verschlüsselte Header zuerst, vor dem verschlüsselten Dokument, entschlüsselt wird. Das Objekt mit sicherem Inhalt erzeugt ein offenes Deckblatt, das Benutzern allgemeine Zugangsinformationen über die Inhalte des PDF anzeigen kann, ehe sich das PDF-Dokument öffnet – ein Merkmal, das dem Benutzer eine erhebliche Zeitersparnis bringt, wenn er ein zuvor verwendetes Dokument in einer großen Sammlung sucht.

[0062] Ein Objekt mit sicherem Inhalt, das im PDF implementiert ist, ist symbolisch in **Fig.** 2 abgebildet. Das OSI enthält ein Deckblatt **210**, das auf bis zu drei verschlüsselte elektronische Dokumente **212** zugreifen kann (aus praktischen Erwägungen ist lediglich ein verschlüsseltes Dokument **212** abgebildet). Jedes verschlüsselte Dokument **212** enthält eine Kennung **240**, einen Klarschrift-Header **242**, der das Dokument gegenüber den Benutzern identifiziert, und die Mehrfachcode-Verschlüsselungstabelle, in der sich die von dem speziellen Mehrfachcode-Verschlüsselungsverfahren verwendeten Mehrfachcode-Komponenten befinden, einen verschlüsselten Header **250** mit einem Fingerabdruck **252** und den verschlüsselten Inhalt **260** mit einem zweiten Fingerabdruck **262**.

[0063] Bei der vorliegenden Ausführungsform ist das Deckblatt **210** als ein PDF-Dokument gemäß PDFRM implementiert. Das Deckblatt **210** enthält bis zu drei Datenstromobjekte **214**, **216**, **218**, die sichere Informationen und Aktions-Verknüpfungen **224**, **226**, **228** zwischen diesen Abschnitten enthalten. Es gibt zwei Schaltflächenfelder **230**, **232**, die das Deckblatt **210** mit den Datenstromobjekten **214**, **216**, **218** verbinden, welche die verschlüsselten Dateien und andere Informationen enthalten. Diese Schaltflächenfelder **230**, **232** können gegebenenfalls alle Optionen nutzen, die im PDFRM (in Tabelle 6.10) beschrieben sind, um das gewünschte Erscheinungsbild zu erzeugen. Wenngleich viele dieser Optionen nicht eingestellt zu werden brauchen, ist es notwendig, dass die Verzeichnis-Schaltfläche „AA" (Additional Action – zusätzliche Aktion – aus Tabelle 6.10 des PDFRM) im Definitionsverzeichnis eingestellt wird, um zu dem indirekten Objekt zu verweisen, welches die Aktion definiert, die die Verknüpfung zu der implementierungsregistrierten Aktion mittels der Schaltfläche „S" des Verzeichnisses herstellt (wie in Tabelle 6.36 des PDFRM definiert).

[0064] Bei diesem Beispiel können bis zu drei Datenstromobjekte **214**, **216**, **218** in dem Deckblatt **210** vorhanden sein, die einen Verweis zu bzw. eine Verknüpfung mit einem sicheren Objekt herstellt (z. B. als verschlüsseltes PDF, eine sichere binäre Datei oder eine sichere Anmerkungsdatei, wie nachstehend beschrieben wird). Jedes dieser Objekte ist ein Datenstromobjekt, dessen Verzeichniscode „Typ" auf „eingebettete Datei" eingestellt ist (PDFRM Abschnitt 7.4.3). Nicht dargestellt sind die Dateispezifikations-Verzeichnisse (PDFRM Abschnitt 7.4.2) für jede der Dateien, die als indirekte Objekte in den Anmerkungsverzeichnissen der Schaltflächenfelder **230**, **232** auf dem Deckblatt **210** verwendet werden. Der Verweis auf die Dateispezifikation wird von der Implementierungs-Software verwendet, um die Datenstromobjekte zum Zeitpunkt des Auslösens der Aktion durch ein Ereignis zu lokalisieren. (Die Verwendung der Dateispezifikation, falls sie verwendet wird, um das PDF konform zu machen, fügt keinen realen Wert hinzu, da die Dateien direkt mit den Anmerkungsverzeichnissen verknüpft werden könnten, denn aus Sicherheitsgründen kann die Dateispezifikation keine wertvollen Informationen über die Quelle oder Inhalte der Datenstrom-Objektdateien enthalten, auf die sie zeigen.)

[0065] Nach dem Öffnen stellt das Deckblatt **210** eine Benutzerschnittstelle für den Zugriff auf den si-

cheren Inhalt in einem verschlüsselten Dokument **212** zur Verfügung. Wenn der Benutzer die Befehlsschaltfläche **230**, **232** auswählt, beginnt eine entsprechend verknüpfte Aktion **224**, **226**, **228** mit der Verarbeitung des Datenstromobjektes **214**, **216**, **218**. Wenn beispielsweise die Befehlsschaltfläche **232** ausgewählt wird, wird die Aktion **226** implementiert, durch die die Verarbeitung des verschlüsselten PDF **214** in Gang gesetzt wird. In gleicher Art und Weise beginnt dann, wenn die Aktion **228** ausgewählt wird, die Verarbeitung der sicheren Anmerkungen **218**. Wenn die Schaltfläche **230** die Aktion **224** auswählt, beginnt die Verarbeitung der sicheren binären Datei **216**. Die Verarbeitung des ausgewählten Datenstromobjektes bedeutet im typischen Fall, dass Mittel für den Benutzer zur Verfügung gestellt werden, um die implementierungsspezifische Benutzer-Berechtigung einzugeben, gefolgt von der Implementierung des Mehrfachcode-Verschlüsselungsverfahrens, um festzustellen, ob die Benutzer-Berechtigung gültig ist, und falls ja, wird das ausgewählte Element anschießend entschlüsselt (wie nachstehend näher beschrieben wird).

[0066] Zwar ist es nicht im Diagramm abgebildet, doch die Textfelder für die Benutzer-Kennung (und/oder biometrische Eingabesteuerungen) sind Teil des Deckblattes **210**, und in ihren Anmerkungsverzeichnissen muss der Zeichenkettenwert des Codes „T" auf einen eindeutigen Namen eingestellt sein, der der Software-Implementierung bekannt ist. Dies ist notwendig, damit die Implementierung den Benutzereintrag für jedes Feld erhalten kann, wenn eine der Schaltflächen **230**, **232** aktiviert wird.

[0067] In der Praxis kann der Inhalt des OSI variieren; es kann die drei Objekte wie in **Fig.** 2 enthalten oder lediglich eine der Befehlsschaltflächen. In jenem Fall würde(n) das/die mit dem fehlenden Befehlschaltflächenfeld verknüpfte(n) Datenstromobjekt/e ebenfalls nicht erscheinen.

[0068] Das sichere, binäre Datenstromobjekt und das Datenstromobjekt des verschlüsselten PDF (beides verschlüsselte elektronische Dokumente) haben einen gemeinsamen Innenaufbau **212**. Die Kennung („ID") **240** steht am Anfang der Daten des Datenstroms und besteht aus einer Textmarke, die zum Markieren des Typs der nachfolgenden Daten verwendet wird. Es ist nicht erforderlich, dass sie in allen Implementierungen vorhanden ist, bietet aber ein schnelles Verfahren für die Verarbeitungs-Software um sicherzustellen, dass ein Datenstromobjekt des erwarteten Typs gelesen wird. Eine typische Länge dieses Abschnittes läge bei vier Zeichen.

[0069] Auf die Kennung **240** folgt der „Klarschrift-Header" **242**, der wenigstens so lang sein muss, dass die Software den Anfang des nächsten Abschnitts findet, eine Datenfolge, die nur für dieses eine OSI gilt (vermischt mit der klaren Benutzer-Kennung unter Zuhilfenahme der Hash-Funktion) und eine Mehrfachcode-Verschlüsselungsinformation, die benötigt wird, um mehr als einem Benutzer Zugang zu gewähren (die Mehrfachcode-Verschlüsselungstabelle, die die Mehrfachcode-Komponenten enthält). Allgemein würde dazu die Anzahl von Benutzern gehören, gefolgt von den Informationen über die Erzeugung des Benutzercodes nach dem Mehrfachcode-Verfahren (die Mehrfachcode-Komponenten). Alle anderen Informationen, die sich in diesem Abschnitt befinden, sind implementierungsabhängig; typisch für dessen Inhalt wäre aber eine Anzahl von Dokumenten und alle anderen Informationen, die der Benutzer zur Verfügung stellen will, die jedoch die Sicherheit nicht infrage stellen.

[0070] Nach der Kennung folgt der „verschlüsselte Header" **250**, der mit dem von der Implementierung ausgewählten Algorithmus verschlüsselt ist. Der Entschlüsselungscode zu diesem Abschnitt hängt von dem angewandten Mehrfachcode-Verfahren ab (ein willkürlich erzeugter Code) oder aber er ist eine Funktion der Kennung des einzigen Benutzers. Da normalerweise das Mehrfachcode-Verfahren und die Chiffrierblock-Kettenbildung zur Anwendung kommt, steht am Anfang eine Verschlüsselungs-Markierung für die Entschlüsselungsgültigkeit. Dies gestattet ein Lesen der Daten lediglich als sequenziellen Strom (kann nicht in den Daten gesichert werden) und das Entschlüsseln der die Markierung enthaltenen Blöcke solange, bis der richtige Code gefunden ist. Darauf folgen die realen Inhalte des Headers, einschließlich der Länge des verschlüsselten Headers, die Länge eines beliebigen Fingerdrucks **252**, der auf den Header folgt (die Summe davon teilt der Implementierung mit, wo die realen Dateidaten beginnen), eine Berechtigungs-Matrix oder eine andere Information über einen begrenzten Zugriff zu einer sicheren Datei, die möglicherweise von der Implementierung benötigt wird (z. B. könnte bei einer binären Datei der Name der Datei hier stehen). Auf diese Information folgen willkürliche Fülldaten, wenn die Blockverschlüsselung zur Anwendung kommt, um den Header mit einer geraden Anzahl von Blöcken zu erstellen. (Es ist von Vorteil, eine gewisse kleine, zufällige Anzahl von Blöcken hinzuzufügen, so dass die tatsächliche Länge des verschlüsselten Headers nicht einmal bei einem OSI gleich ist, welches dieselben gesicherten Daten enthält.) Es sei angemerkt, dass die Länge des verschlüsselten Headers nicht in Klarschrift zu sehen ist und man in der Lage sein muss, den Anfang zu entschlüsseln, um den verschlüsselten Dateiabschnitt zu lokalisieren, der ihm in dem sicheren Datenstromobjekt folgt.

[0071] Die in dem verschlüsselten Header verwendete Berechtigungsmatrix gleicht die Benutzer mit ihren jeweiligen Berechtigungen ab. Das eigentliche Format dieses Elementes ist implementierungsab-

hängig. Allerdings verfügt die zugehörige Implementierung über mehrere Code-Aspekte, die bei anderen Implementierungen berücksichtigt werden sollten. Dass zum Abgleichen eines Berechtigungssatzes angewandte Verfahren bietet keinerlei Informationen darüber, wer der Benutzer sein könnte. Das heißt, wenn man die entschlüsselte Berechtigungsmatrix erhält, bekommt man keinerlei Informationen über irgendeine Benutzer-Kennung (Benutzer werden von einem Hash angegeben). Berechtigungen, die enthalten sind, gewähren einem Benutzer das Recht zum „Kopieren in Zwischenablage", Drucken des Dokuments und Hinzufügen von Anmerkungen zu dem Dokument, wenn es geöffnet ist. Darüber hinaus können die Berechtigungen das Öffnen des Dokuments durch eine Implementierung einschränken, wenn es nach einem speziellen Datum erfolgt, wenn der Computer keine Netzwerkadresse aufweist, die von einer Netzwerkmaske angegeben wurde, kombiniert mit einer Netzwerkadresse, wenn der Computer keine spezielle Hardware bereitstellt, die abhängig von der „Rechner-Kennung" ist, oder wenn das Computersystem anzeigt, dass es über keine Netzwerkadresse verfügt (kann das Objekt mit sicherem Inhalt nicht öffnen, wenn das Netzwerk angeschlossen ist).

[0072] Auf den verschlüsselten Header **250** kann ein optionaler kleiner Fingerabdruck **252** folgen. Notwendig ist dies nicht, wenn jedoch die Quellenidentifikation des OSI erforderlich ist, ist dies eine der Stellen, an der solche Informationen positioniert werden können. Da der Fingerabdruck **252** nicht sicher ist, kann es vorteilhaft sein, ihn mit Hilfe eines bekannten Codes und einer Verschlüsselungs-Markierung zu verschlüsseln, gefolgt von den benötigten Daten, aufgefüllt mit zufälligen Bytes, so dass eine gerade Anzahl von Verschlüsselungsblöcken entsteht, gefolgt von einer kleinen willkürlichen Anzahl von Blöcken, die mit zufälligen Daten gefüllt sind. Da der gesamte Fingerabdruck verschlüsselt ist, ist die Länge des verschlüsselten Headers **250** nicht bekannt und schwankt, der Fingerabdruck kann von jemandem, der kein gültiger Benutzer ist, nur dann lokalisiert werden, wenn vom Anfang des verschlüsselten Header an solange vorwärts entschlüsselt wird, bis die Verschlüsselungs-Markierung des Fingerabdrucks gefunden ist. Dies würde nur vorkommen, wenn ein OSI nachverfolgt wird, da bei der normalen Verarbeitung von Daten die Länge aus der Entschlüsselung des verschlüsselten Headers bekannt ist, und sie in dem Datenstrom einfach übersprungen wird.

[0073] Der nächste Abschnitt ist der verschlüsselte Inhalt **260**, bei dem es sich um die eigentliche Datei mit sicheren Daten handelt. Als verschlüsselter Abschnitt beginnt er jedoch mit einer Verschlüsselungs-Markierung. Dadurch kann die Implementierung überprüfen, dass es sich um einen gültigen Code für ein Dateiformat handelt. Bevorzugt wird es zudem, wenn auf diese Markierung die tatsächliche Länge der Daten folgt, da diese normalerweise nicht genauso lang wie der Rest des Datenstromobjektes ist, wenn eine Blockverschlüsselung erfolgt und/oder auf den Abschnitt ein anderer Fingerabdruck **262** folgt. Auf die Hauptdaten **260** folgt ein weiterer optionaler Fingerabdruck **262** mit Daten, die zum Zurückverfolgen bis zum Eigentümer des OSI genutzt werden kann oder ein anderes implementierungsspezifisches Merkmal bereitstellt, z. B. Datum, Überarbeitungsnummer usw. Dieser könnte dieselbe Form haben wie der vorherige Fingerabdruck, wenn dies der Fall wäre, würde jedoch ein anderes Verschlüsselungsverfahren oder ein anderer Code eingesetzt werden. Ein willkürliches Auffüllen dieses Abschnittes mit zufälligen Daten könnte ebenfalls erfolgen.

[0074] Es sei angemerkt, dass die Fingerabdrücke laut vorliegender Definition nicht sicher vor einem speziellen Angreifer sind, doch genauso wie bei dem willkürlichen Auffüllen der Abschnitte, was dazu führt, dass OSIs mit demselben Inhalt eine unterschiedliche Länge erhalten, sind sie dazu gedacht, weniger kundige Angreifer abzuschrecken. (Dies gilt nicht für die zufälligen Daten, die in den Verschlüsselungs-Markierungen verwendet werden, mit denen „feststehender Text" vom Anfang einer Verschlüsselungssequenz entfernt wird.

[0075] Unter „zufälligen Daten", die an mehreren Stellen in dem OSI vorkommen, sind Daten zu verstehen, die von der Standardsoftware für Pseudozufalls-Sequenzen generiert werden. Normalerweise nimmt die Software „Startparameter", die so für jedes OSI abgewandelt werden, dass jedes OSI einzigartig innerhalb der Grenzen der Pseudozufalls-Sequenz ist. Diese Daten werden für den Anfangs-„Text" einer beliebigen Verschlüsselungssequenz und beliebiger Füllzeichen verwendet, die möglicherweise zum Chiffrierblock-Ausrichten von Elementen oder Abschnitten benötigt werden.

[0076] Jedes Datenstromobjekt **212** enthält einen unverschlüsselten Abschnitt, auf den ein fortlaufender Strom verschlüsselter Daten folgt, die mit zufälligen Daten vermischt sind. Der Klarschriftabschnitt enthält keine identifizierbare Benutzerinformation. Die OSI-Daten **240**, **242**, die in Klarschrift gehalten sind, werden lediglich als Eingabe für eine Code-Ermittlungsfunktion verwendet, die zum Erzeugen einer gültigen Ausgabe eine gehashte Benutzer-Kennung benötigt. Die richtige Entschlüsselung hängt davon ab, dass Codes aus dem Mehrfachcode-Verfahren solange getestet werden, bis eine gültige Verschlüsselungs-Markierung gefunden ist, wobei die Daten in dieser Markierung pseudozufällig von einem OSI zum anderen variieren. Die verschlüsselten Abschnitte können erst dann zuverlässig voneinander getrennt werden, wenn man den verschlüsselten Header **250** entschlüsseln kann. (Abschreckend wirkt dies nur auf weniger kundige Angreifer.) Das Ver-

schlüsselungsverfahren hängt von der Implementierung ab und könnte von einem OSI zum anderen variieren. Es ist für ein rudimentäres Erstellen von Fingerabdrücken **252**, **263** des OSI gesorgt, wodurch sich zurückverfolgen lässt, an wen das OSI zu Beginn gegeben wurde (wer dessen Erstellung anforderte). Für jede Benutzer-Kennung sind Benutzer-Berechtigungen codiert. Für den verschlüsselten Header **250** und den verschlüsselten Inhalt **260** können verschiedene Hauptcodes und unterschiedliche Mehrcode-Funktionen zur Anwendung kommen.

[0077] Das OSI wird verwendet, wenn ein Benutzer das verschlüsselte PDF öffnet oder die sichere binäre Datei extrahiert. Zuerst öffnet der Benutzer das OSI in einem Viewer/Editor, der das Deckblatt **210** anzeigt. Anschließend gibt der Benutzer seine Kennungsinformation (nicht abgebildet) ein und klickt auf eines der Schaltflächenfelder **230**, **232**. Allgemein ist die Verarbeitung für beide Schaltflächenfelder bis zu dem Punkt gleich, an dem die sichere Datei entschlüsselt werden kann, so dass der nachfolgende sie bis zu diesem Punkt nicht voneinander unterscheiden kann.

[0078] Die Schaltflächenfelder **230**, **232** verfügen über eine vertrauliche (in dem PDFRM nicht definierte) Aktion, die in einem Plug-In oder als Teil des Viewer/Editors implementiert ist (vertrauliche Aktionen sind im PDF-Viewer bei gemeinsamer Verwendung erlaubt). Die Software zur Unterstützung dieser Aktion **224**, **226**, **228** beginnt mit ihrer Verarbeitung, wenn der Benutzer die Maus auf die Schaltflächenfelder **230**, **232** setzt. Zu diesem Zeitpunkt wird ihr entweder ein Verzeichnis für die Aktion vorgelegt oder ein Verzeichnis, das es gestattet, eines der möglichen Verzeichnisse zu lokalisieren, die zur Aufnahme des indirekten Objektverweises auf das Datenstromobjekt **214**, **216**, **218** verwendet wird, welches mit der Schaltfläche **230**, **232** verknüpft ist.

[0079] Nach Eingang des Datenstromobjektes werden die darin enthaltenen Daten vom Anfang nacheinander verarbeitet. Zuerst wird die Kennung ausgelesen und überprüft und anschließend werden die Mehrfachcode-Informationen und die OSI-Kennung gelesen und gesichert. Daraufhin werden die Benutzer-Kennungsinformationen zusammen mit der OSI-Kennung aus den Textfeldern ausgelesen und zu Einweg-Hash-Werten verarbeitet, die das Offenlegen der tatsächlichen Werte verhindern. Am besten hat sich bewährt, die Textfelder des Passwortes und der Passphrase zu diesem Zeitpunkt durch die Implementierung zu löschen, so dass deren „Klartext"-Werte nicht länger im Computer vorhanden sind. Danach werden diese Hash-Werte von der Mehrfachcode-Funktion als Benutzereingaben verwendet.

[0080] Im Anschluss wird das Datenstromobjekt solange ausgelesen, bis feststeht, dass wenigstens die Verschlüsselungs-Markierung mit einem gültigen Code decodiert werden kann. Danach wird für jeden möglichen Benutzer versucht, die Markierung zu entschlüsseln, indem deren Mehrfachcode-Daten für den verschlüsselten Header in die Codeerzeugungsfunktion eingegeben werden. Wenn für die Markierung bei einem der Codes kein gültiger entschlüsselter Wert gefunden wird, wird davon ausgegangen, dass die Benutzer-Kennung nicht richtig ist, und die Verarbeitung des OSI endet hier.

[0081] Nachdem der Code für den verschlüsselten Header **250** gefunden ist, ist dessen Länge bekannt und der Rest kann entschlüsselt, und die Berechtigungen des aktuellen Benutzers können erhalten werden. Jene Berechtigungen, die nicht im Zusammenhang mit dem Öffnen eines PDF stehen, werden nun überprüft. Wenn alle Bedingungen in den Berechtigungen nicht erfüllt sind, endet die Verarbeitung (z. B. ist das aktuelle Datum abgelaufen, für das die Berechtigungen erteilt wurden). Wenn die Verarbeitung fortgesetzt wird, springt der Lesevorgang des Datenstromobjektes vorwärts bis zum Anfang des verschlüsselten Inhalts **260**, zum Ablesen und Entschlüsseln der Verschlüsselungs-Markierung, so dass überprüft wird, ob alles gültig ist. Möglicherweise müssen je nach Implementierung nicht alle Codes bei dieser Entschlüsselung ausprobiert werden und auch dann nicht, wenn der „Index" des Benutzers, dessen Mehrfachcode-Informationen den verschlüsselten Header entschlüsselten, verwendet werden kann.

[0082] Nachdem die Verschlüsselungs-Markierung am Anfang des Inhaltes überprüft ist, verzweigt sich die Verarbeitung je nachdem, welches Schaltflächenfeld **230**, **232** betätigt wurde. Im Falle der Dateiextraktion legt die Software dem Benutzer eine standardmäßige Dateisicherungs-Benutzerschnittstelle für das Betriebssystem vor und entschlüsselt die Daten aus dem Datenstromobjekt in eine neue Datei, wenn nicht der Benutzer die Option Abbruch wählt. Ab diesem Punkt fällt die weitere Sicherheit in den Verantwortungsbereich des Benutzers, da sie nun unabhängig von dem OSI ist.

[0083] Wenn das aktivierte Schaltflächenfeld **232** mit dem verschlüsselten PDF **214** verknüpft ist, wird es, ohne entschlüsselt zu werden, aus dem Datenstromobjekt in den Speicher eingelesen. (Dies ist erforderlich, da das Datenstromobjekt in dem Deckblatt möglicherweise geschlossen wird, aber die Daten innerhalb des verschlüsselten PDF immer noch verfügbar sein müssen.) Anschließend wird ein Speicherdateiobjekt für den Viewer/Reader erzeugt und auf niedriger Stufe geöffnet (Öffnen ohne Ansicht). Zu diesem Zeitpunkt oder wenn der Viewer/Reader zuerst die Beschränkungen im Hinblick auf die Verwendung des Dokuments akzeptiert, werden die Berech-

tigungen für das Dokument mit Hilfe der Berechtigungen aus dem verschlüsselten Header eingestellt. Während der Viewer/Editor das PDF verarbeitet, nutzt er die Speicherdatei, welche die Daten in dem PDF gegebenenfalls entschlüsselt. Es sei angemerkt, dass es nicht notwendig ist, die verschlüsselten PDF-Daten im Speicher zu halten, da sie als lokale Dateien gespeichert werden könnten, während sie verschlüsselt bleiben. Bei Verwendung des lokalen Datenträgersystems sollten die Inhalte nicht offen gelegt werden, doch die bevorzugte Implementierung verwendet den Speicher, um Probleme zu vermeiden, die auftreten könnten, falls die Datenträgerdatei nicht entfernt worden ist, wenn sich das PDF in dem Viewer geschlossen hatte.

[0084] Nachdem das verschlüsselte PDF ohne Fehler als ein Dokument auf niedriger Sicherheitsstufe geöffnet worden ist, wird der Viewer/Editor angefordert, das offene Deckblatt des PDF durch das neu geöffnete PDF zu ersetzen, und der Benutzer kann es ansehen. Dadurch wird die Aktion abgeschlossen, die mit der Mausbetätigung auf dem Schaltflächenfeld begann.

[0085] Es wird angemerkt, dass bei diesem Verfahren die PDF-Inhalte **260** oder binäre Dateiinhalte **260** erst dann entschlüsselt werden, wenn die Berechtigungen als gültig überprüft worden sind. Das verschlüsselte PDF wird niemals vollständig entschlüsselt, da die Entschlüsselung nur dann erfolgt, wenn der Reader/Viewer während der Verarbeitung einen Datenblock aus dem PDF anfordert. Die Implementierung behält keine Klarschriftversionen der Benutzer-Kennung, sondern verwendet vielmehr eine Hash-Funktion, die die Benutzerinformation mit der OSI-Kennung für sämtliche Verarbeitungsschritte vermischt. Alle verschlüsselten Inhalte können auch eine Verschlüsselungs-Markierung enthalten. Besonders nützlich ist dies, wenn das Format bzw. der Typ des verschlüsselten Inhalts nicht bekannt ist. Wenn es sich beispielsweise bei dem verschlüsselten Inhalt um binäre Testdaten handelt, gibt es keine Möglichkeit für einen Benutzer, die „entschlüsselten" Daten zu überprüfen, um festzustellen, ob sie gültig sind. Somit wird durch das Wissen, dass die Verschlüsselungs-Markierung dem entschlüsselten Inhalt vorausgeht, eine gültige Entschlüsselung des Inhaltes gewährleistet.

[0086] Bei einer weiteren Ausführungsform der Erfindung kann das Objekt mit sicherem Inhalt dazu verwendet werden, Anmerkungen **218** zu schützen, selbst wenn das Hauptdokument nicht geschützt werden soll. Wie bereits angeführt, kann das Anmerkungsmerkmal in einem Anwendungsprogramm zum Einsatz kommen, welches für die Erzeugung von Anmerkungen sorgt. Allgemein hat ein derartiges Anwendungsprogramm seine eigenen Regelsätze für die Erzeugung von Anmerkungen. Die Anmerkungsimplementierung wird anhand von PDF-Dokumenten geschrieben und umfasst die Speicherung bzw. Übertragung neuer Anmerkungen durch einen Benutzer; das Verschmelzen von Anmerkungen verschiedener Benutzer zu einem Objekt innerhalb des PDF; das Öffnen eines Dokuments, welches lokale und/oder verteilte Anmerkungen aufweist.

[0087] Wenn man davon ausgeht, dass der Benutzer das ursprüngliche PDF durch Hinzufügen von Anmerkungen bearbeitet hat, gibt es zwei Möglichkeiten: Erstens, der Benutzer möchte in dem lokalen Modus verbleiben (vertrauliche Anmerkungen des Benutzers) oder zweitens, der Benutzer ist Teil eines Netzwerkes und befindet sich im Server-Modus (verteilte Anmerkungen). Eine Software, die diese beiden erfindungsgemäßen Modi implementiert, kann entweder in einer Viewer/Editor-Anwendung direkt oder als ein Plug-In zu der Anwendung vorliegen.

[0088] Der Ablauf von Schritten zum Erzeugen eines Dokuments mit sicherem Inhalt und mit verschlüsselten Anmerkungen unterscheidet sich wie folgt von der normalen Erstellung einer neuen PDF-Version: Zuerst werden die zu dem aktuellen Benutzer gehörenden Anmerkungen extrahiert oder es wird eine Liste für die Extraktion während des Verschlüsselungsschrittes aus dem editierten PDF erzeugt. Dieser Prozess umfasst nicht nur die wichtigsten Anmerkungen, sondern auch Pop-up-Anmerkungen, bei den es sich um nachgeordnete Objekte anderer Anmerkungen handelt. Da sich eine Anmerkung auf einer Seite befindet, wird während des Auflistungs- oder Extraktionsprozesses davon ausgegangen, dass alle Verzeichnisse für Anmerkungsobjekte mit der Seitenzahl markiert sind, auf der sie sich befinden. Während der Extraktion werden die Anmerkungen des aktuellen Benutzers von Anmerkungen anderer Benutzer mit Hilfe eines Code/Wert-Paares unterschieden, welches in das Anmerkungsverzeichnis eingestellt worden ist, als die Anmerkungen der anderen Benutzer zur Ansicht hinzugefügt wurden.

[0089] Wenn man davon ausgeht, dass ein Benutzercode für ein Verschlüsselungsverfahren vorhanden ist oder erlangt werden kann, dann werden die Anmerkungsobjekte und alle Objekte, von denen sie abhängen, mit Hilfe des Codes des aktuellen Benutzers verschlüsselt und in eine Datenfolge formatiert. Die genaue Form, die die extrahierten Anmerkungen annehmen können, ist nicht kritisch; es ist lediglich notwendig, dass die Implementierung der Erfindung in der Lage ist, zu einem späteren Zeitpunkt die extrahierten Anmerkungen in ein PDF zurückzubringen. Anschließend stehen zwei Aktionen zur Verfügung. Im lokalen Modus werden die Daten auf einen lokalen Datenträger als Datei geschrieben, die aus einem Klarschrift-Header besteht, der die Datei identifiziert, und aus Benutzerdaten, die nicht vertraulich sind, und aus Mehrfachcodes, falls sie verwendet werden.

Auf diesen Klarschriftdaten folgen ein oder mehrere verschlüsselte Teile, welche sämtliche Anmerkungen und die Objekte enthalten, von denen sie abhängen. Normalerweise ist dieses Dateiformat dasselbe, das für die zusammengelegten, eingebetteten Anmerkungsdateien verwendet wird, die auf PDF beruhen, allerdings entsteht dadurch lediglich eine verbesserte Software-Effizienz und es ist keine notwendige Voraussetzung. Es ist nicht notwendig, dass diese Datei den aktuellen Benutzer, den Eigentümer der Anmerkungen in einer anderen Art und Weise kenntlich macht, als durch Verschlüsselung – d. h. der Benutzer kann die Datei entschlüsseln. Im Server-Modus wird diese formatierte Datensequenz zu dem Server übertragen, wenn der Benutzer seine neuen Anmerkungen den anderen Benutzern zur Kenntnis geben will. Während der Übertragung erfährt der Server die Benutzer-Kennung, so dass durch die sicheren Informationen der Weg zu den Codes für die verschlüsselten Abschnitte frei wird. Es ist anzumerken, dass bei Vorhandensein einer sicheren Server/Client-Verbindung diese Übertragung keine verschlüsselten Abschnitte enthalten muss. Da jedoch eine Option auftreten kann, bei der eine zuvor erzeugte Datei im lokalen Modus von einer vorherigen Extraktion herrührt, führt das Beibehalten eines gemeinsamen Formates zu einer höheren Software-Effizienz.

[0090] Am Ende des vorhergehenden Schrittes ist das aktuelle PDF-Dokument als „gesichert" betrachtet worden und das angesehene PDF wird als „unverändert" markiert (d. h., es bedarf keiner Sicherung). Unter keinen Umständen wird das aktuelle PDF in modifizierter Form in den lokalen Datenträger oder in den Server eingeschrieben. Das heißt, sämtliche Veränderungen durch den aktuellen Benutzer sind innerhalb der in den vorherigen Schritten erzeugten Anmerkungsdatei enthalten und das modifizierte PDF, das in dem Viewer/Editor aktiv ist, wird einfach gelöscht, ohne dass Restinformationen für andere über die Anmerkung verbleiben, die zu einem späteren Zeitpunkt abgerufen werden könnten.

[0091] Das erzeugte Objekt mit sicherem Inhalt umfasst eine verschlüsselte Datei, die alle von dem aktuellen Benutzer geschaffenen oder veränderten Anmerkungen enthält und das Original PDF-Dokument bleibt unverändert. Bei der Verschlüsselung dieser Anmerkungen wird ein Code verwendet, der von den Informationen abhängig ist, die nur jenem Benutzer und im Server-Modus den sicheren Systemen der Organisation bekannt sind, zu der der Benutzer gehört. Das Verfahren zum Verschlüsseln und festlegen des Hauptcodes für diese Verschlüsselung kann ein beliebiges bekanntes Verschlüsselungsverfahren sein. Es ist anzumerken, dass diesen Schritten gemeinsam ist, dass die Anmerkungen des Benutzern zu dem PDF hinzugefügt werden und dass eine neue Version des PDF-Dokuments durch das Speichern seitens des Benutzers erzeugt wird.

[0092] Es ist nicht erforderlich, dass der Benutzers jemals den Server-Modus verwendet. Wenn der Benutzer es nicht tut, dann bleiben die Anmerkungen des Benutzers vertraulich und durch die Verschlüsselung geschützt. Die einzige Einschränkung im vorliegenden Fall besteht darin, dass nun zwei Dateien auf dem lokalen Datenträger vorhanden sind: Das nicht modifizierte PDF (das auch durch die Verschlüsselung gesichert werden kann) und das Dokument mit den Anmerkungen des Benutzers. Normalerweise sind diese Dokumente miteinander verbunden, indem sie sich im gleichen Verzeichnis befinden, denselben Namen haben, aber eine unterschiedliche Namenserweiterung (z. B. myfile.pdf und myfile.ant). Ein Beispiel dafür, wo derartige vertrauliche Anmerkungen sinnvoll sein können, ist ein Verkäufer, der eine Preisliste mit Informationen (Anmerkungen) versieht, die er für wichtig hält. Da die beiden Modi viel gemeinsam haben, liegt es an dem Benutzer zu entscheiden, wann und ob überhaupt die Anmerkungen des Benutzers zu verteilen sind.

[0093] Wenn ein Benutzer seine Anmerkungen im Server-Modus sichert, sollen sie dadurch anderen zugänglich gemacht werden können, die das Dokument ansehen können. Möglicherweise gibt es aber einige Benutzer, die das Dokument ansehen können, für das der Benutzer das Recht zum Ansehen seiner Anmerkungen einräumen möchte. Ein einfaches Beispiel dafür ist ein Manager, der möchte, dass sein Vorgesetzter seine Anmerkungen sieht, seine untergeordneten Mitarbeiter aber nicht einmal wissen sollten, dass die Anmerkungen existieren. Dies sollte sogar dann zutreffen, wenn sie alle dasselbe PDF-Dokument haben (exakte Kopien, da eine einzige Kopie von dem Server geholt und durch den Manager verteilt wurde).

[0094] An einem gewissen Punkt hat der Server eine Anmerkungsmatrix für das Dokument und dessen Anmerkungen. Diese Matrix gleicht die „Leser der Anmerkungen" mit den „Erzeugern der Anmerkungen" ab. Es kann vermutet werden, dass es wenigstens einen Leser einer Anmerkung gibt – den Erzeuger der Anmerkungen –, so dass die Matrix niemals leer ist. Ein Benutzer kann ein beliebiges praktisches Verfahren anwenden, um festzulegen, wer seine Anmerkungen zu einem Dokument lesen kann. Es wird ebenfalls vermutet, dass der Server die Matrix über die Leser der Anmerkungen erhalten und behalten kann. Weiterhin ist das Verfahren, mit dem der Server alle ihm von den Benutzern zugeführten Anmerkungen speichert und lokalisiert, nicht kritisch, solange die Anmerkungen verfügbar sind und ihr Eigentümer (Schöpfer) und ihre Leser identifiziert sind.

[0095] Zur Verteilung an Benutzer, denen das Ansehen des PDF-Dokuments gestattet ist, wird vom Server eine neue Version des PDF-Dokuments erzeugt, indem eine „Zusammenlegung" der neuen Anmer-

kungen mit dem ursprünglichen PDF-Dokument erfolgt (das Zusammenlegen erfolgt typischerweise nur, wenn das Dokument geöffnet oder angesehen wird). Je nach Implementierungsvorgang kann dieser Schritt dann erfolgen, wenn ein Benutzer eine Kopie des Dokuments anfordert, oder vorher.

[0096] Der Prozess des Zusammenlegens modifiziert das originale PDF durch Hinzufügen aller Anmerkungen in sicherer Art und Weise. Jede Anmerkung wird mit Hilfe des bereits definierten Mehrfachcode-Verfahrens verschlüsselt. Zusätzlich zu der Verschlüsselungs-Markierung, die an den Anfang der Anmerkungsdaten gestellt wird, ist eine Eigentümer-Markierung vorhanden (im Allgemeinen ist es kein Klartext, sondern ein Hash oder etwas aus dem Mehrfachcode-Verfahren), die den Eigentümer/Erzeuger der Anmerkung gegenüber der Software identifiziert, die den Abschnitt entschlüsselt. Anschließend wird zu dem Anfang jeder verschlüsselten Anmerkung Klartext hinzugefügt, der die Länge der Datei und alle anderen Informationen neben denen angibt, die von dem Mehrfachcode-Verfahren benötigt werden, so dass das Erproben von Codes, das Lokalisieren der verschlüsselten Teile und/oder das Ermitteln der Größe der entstehenden Sequenz mit der darin enthaltenen Anmerkung ermöglicht werden. Die Codes, die zu der Mehrfachcode-Verschlüsselung gehören, sind nur für jene Benutzer gedacht, denen das Recht zum Ansehen jener Anmerkung eingeräumt wurde. Somit müssten jene, die diese Anmerkung erhalten haben, aber nicht das Recht zum Ansehen besitzen, die Verschlüsselung knacken, um Zugriff auf den Inhalt der Anmerkungsdatei zu erhalten.

[0097] Alle oben erzeugten Anmerkungsdatensequenzen (Dateien) werden zu einer einzigen Sequenz verkettet. Je nach der Implementierung kann Klartext gegebenenfalls während dieses Schrittes hinzugefügt werden, um der Sequenz eine Struktur zu verleihen, die zu einem späteren Zeitpunkt eine Trennung in Teile der Anmerkungsdatei ermöglichen würde.

[0098] Anschließend wird die oben erzeugte Datensequenz zu dem ursprünglichen PDF-Dokument hinzugefügt, oder falls das PDF-Dokument innerhalb eines anderen PDF-Dokuments als sicherer Inhalt vorliegt, zu dem PDF auf niedriger Ebene als Datenstromobjekt hinzugefügt. Dieser Datenstrom gehört zu dem Typ „eingebettete Datei", so dass sie mit dem PDFRM konform ist. Zum leichteren Verständnis künftiger Bezugnahmen sei erwähnt, dass beim Öffnen des PDF das Objekt zu dem Namensbaum (PDFRM Abschnitt 7.2) hinzugefügt und mit einer durch ein Plug-In-unterstützten Aktion verknüpft werden kann. In dem PDFRM sind verschiedene Verfahren zur Bezugnahme auf dieses Datenstromobjekt definiert und die Auswahl des zur Anwendung kommenden Verfahrens ist von der Implementierung abhängig.

[0099] Das neue PDF-Dokument mit dem ursprünglichen Dokument und dem Anmerkungsdokument wird an einen Benutzer oder mehrere Benutzer ausgegeben, bei dem der Server das Recht auf Besitz einer Kopie des Dokuments ermittelt hat. Es ist anzumerken, dass beim Hinzufügen des Datenstromobjektes zu dem PDF-Dokument durch den Server zum Zeitpunkt der Anforderung einer Kopie durch einen Benutzer jene Anmerkungen, die nicht von diesem Benutzer angesehen werden können, nicht in dem PDF-Dokument enthalten zu sein brauchen. Ob sie enthalten sind oder nicht, hängt von der Implementierung ab.

[0100] In diesem Prozess steht die Verschlüsselung jeder Anmerkung in keinem Zusammenhang mit einer anderen, außer durch die Verwendung von Mehrfachcode-Verschlüsselungsverfahren für eine bestimmte Benutzergruppe. Die Handhabung der Benutzer-Kennung und die Erzeugung der notwendigen Elemente zur Anwendung der Mehrfachcode-Verschlüsselung erfolgt auf dem Server, von dem angenommen wird, dass er sicher ist. Das erzeugte Datenstromobjekt kann laut PDFRM als „eingebettete Datei" markiert sein, es muss aber keine „Dateispezifikation" für das Objekt vorhanden sein (PDFRM Abschnitt 7.4), da es normalerweise nicht als „Datei" im Sinne des PDFRM angewendet wird. Die Verknüpfung mit dem Datenstromobjekt existiert an irgendeiner Stelle in dem PDF auf oberster Ebene, so dass es sich öffnen lässt und es davor bewahrt wird, verwaist zu werden (verwaiste Objekte werden mitunter durch Anwendung aus den PDF-Dateien entfernt).

[0101] Wenn der Benutzer ein Objekt mit sicherem Inhalt, welches wenigstens eine Anmerkung enthält, zum Ansehen öffnet, muss eine Sequenz von Ereignissen stattfinden, um die Anmerkungen als Teil des PDF zu präsentieren. Natürlich kann der Benutzer auch eine Anmerkung im lokalen Modus für dieses Dokument haben, die in diesem Prozess berücksichtigt werden muss. Wodurch und wie die Sequenz ausgelöst wird, hängt sowohl von dem Viewer als auch von der Implementierung ab, genauso wie davon, ob die Ereignisse eintreten, bevor der Benutzer einen Teil des Dokuments sieht oder nachdem es teilweise oder vollständig geöffnet ist. Das Endergebnis sollte in allen Fällen gleich sein, ob nun der Viewer automatisch das modifizierte Dokument anzeigt oder ob er am Ende der Anmerkungsverarbeitung eine „Aktualisierung" (Refresh) vornimmt.

[0102] Zwar ist es nicht notwendig, doch im Nachfolgenden wird angenommen, dass alle Anmerkungsaktionen erfolgen, bevor der Benutzer das Dokument sieht. Weiterhin wird davon ausgegangen, dass ein Verfahren vorhanden ist, mit dem die Benutzer-Ken-

nungsinformationen, die zum Erzeugen des Verschlüsselungscodes notwendig sind, ermittelt werden oder worden sind. Wie dies erfolgt, ist implementierungsspezifisch.

[0103] Weiterhin wird angenommen, dass die Viewer-Anwendung die grundlegende Struktur des PDF-Dokuments verändern kann, dessen Verarbeitung im Speicher begonnen worden ist und bei dem es ein Ereignis gab, welches die Anmerkungsverarbeitung in Gang setzt. Dies ist normalerweise der Fall, da selbst der einfache Akt des Öffnens des zu einer Anmerkung gehörenden Pop-up zu einem bearbeiteten Wert in einem Verzeichnis führt – eine Veränderung der Art, die angenommen wird. Die genauen Implementierungen der Verfahren dieses Abschnitts können unterschiedlich sein.

[0104] Zu dem Zeitpunkt, da dem Viewer die zugrunde liegende Struktur des PDF-Dokuments zur Verfügung steht, können die folgenden Schritte ausgeführt werden, um die Anmerkungen in die ansehbare PDF-Datei einzufügen. Der lokale Datenträger wird im Hinblick auf eine Anmerkung im lokalen Modus überprüft. Wenn sie gefunden ist, wird sie zuerst so verarbeitet, wie nachstehend für andere Anmerkungen angegeben ist. Der einzige Unterschied besteht darin, dass darin enthaltene Anmerkungen in das PDF eingestellt werden, wobei das Flag „read only" nicht gesetzt ist (PDFRM-Tabelle 6.10 unter dem Verzeichniscode „F").

[0105] Der von dem Server in dem PDF erzeugte Objektstrom ist lokalisiert und alle Klartext-Header-Informationen, die zur Verarbeitung der Anmerkungen benötigt werden, werden ausgelesen und verarbeitet. Jegliche Benutzer-Kennung, die für die Entschlüsselung benötigt wird, muss vor Abschluss dieses Schrittes vorhanden sein. Anschließend erfolgt die Verarbeitung der ersten Anmerkung, die in dem Datenstromobjekt enthalten ist.

[0106] Mit Hilfe der aktuellen Benutzer-Kennung wird versucht, den vorderen Abschnitt der verschlüsselten Anmerkungen zu entschlüsseln. In den meisten Fällen bedeutet dies, dass der Verschlüsselungs-Markierungsabschnitt am Anfang der Anmerkungen für jeden möglichen Code nach dem Mehrfachcode-Verfahren entschlüsselt wird. Das heißt, es gibt keine Möglichkeit festzustellen, welcher der Mehrfachcodes die Daten für diesen Benutzer entschlüsselt, so dass jeder ausprobiert werden muss. Wenn keiner der Entschlüsselungsversuche für die Mehrfachcodes die erwarteten Werte für den verschlüsselten Header ergibt, wird vermutet, dass der aktuelle Benutzer nicht die Erlaubnis besitzt, die in diesem Dokument enthaltenen Anmerkungen zu lesen, und die vorliegende Anmerkungsgruppe wird bei der Verarbeitung in diesem Schritt ausgelassen und die Verarbeitung beginnt erst wieder erneut mit der nächsten Anmerkung im Datenstromobjekt. Wenn der verschlüsselte Header richtig entschlüsselt worden ist, geht es bei der Verarbeitung weiter zum nächsten Schritt.

[0107] Bei der Entschlüsselung des verschlüsselten Headers kann eine Verschlüsselung der Eigentümerinformationen innerhalb des Anmerkungsdokuments erreicht werden. Wenn der aktuelle Benutzer der Eigentümer dieser Anmerkung ist und es eine Anmerkung im lokalen Modus war, die verarbeitet wurde, dann wird diese Anmerkung übersprungen, da davon ausgegangen wird, dass sie durch die Anmerkung im lokalen Modus ersetzt wird. Die entschlüsselte Eigentümerinformation wird weiterhin dazu verwendet, das für den nächsten Schritt erforderliche Flag „read only" einzustellen oder zu löschen, da es nur den Lesern, die auch Eigentümer sind, gestattet ist, eine Anmerkung zu bearbeiten.

[0108] Als Nächstes wird jede der Anmerkungen in dem Dokument decodiert, zusammen mit abhängigen Objekten, und zu der PDF-Struktur des Viewers hinzugefügt. Für jede Pop-up-Anmerkung auf oberster Ebene und zweiter Ebene wird die indirekte Objektnummer notiert, genauso wie die Seite, auf der sich die Anmerkung befinden soll. Nach dem Platzieren der Anmerkung oder einer Pop-up-Anmerkung in der PDF-Struktur wird ein besonderes Code/Wert-Paar zu dem Verzeichnis hinzugefügt, welches anzeigt, dass der aktuelle Benutzer nicht der Eigentümer dieser Anmerkung ist. Wie bereits beschrieben, wird dieses Code/Wert-Paar während des Extraktionsprozesses verwendet, um herauszufinden, welche Anmerkungen in dem PDF gesichert werden sollten.

[0109] Nachdem alle Anmerkungsobjekte und deren abhängige Objekte zu der Form des PDF-Dokuments im Viewer hinzugefügt worden sind, werden die Anmerkungen und deren Pop-up-Objekte zu einem vorhandenen Seitenobjekt-Datenfeldobjekt unter dem Code „annots" als indirekte Objekte hinzugefügt. Wenn der Code „annots" nicht existiert, wird er erzeugt. Mit Hilfe der gespeicherten Seitenzahlen aus dem vorherigen Schritt werden die Seitenobjekte lokalisiert. Dies entspricht Abschnitt 6.4 des PDFRM.

[0110] Nachdem alle Anmerkungen in dieser Datenstromdatei hinzugefügt worden sind, geht es bei der Verarbeitung zu dem nächsten Element im Datenstromobjekt, und es wird der Entschlüsselungsschritt wiederholt. Wenn sich keine weiteren Anmerkungen in dem Datenstrom befinden, endet die Verarbeitung und der Viewer, im Falle, dass er sich im Stadium des Ladens der Vorschau befindet, wird angewiesen, dem Benutzer das Dokument anzuzeigen.

[0111] Die Anmerkungen sind so sicher, wie dies das Verschlüsselungsverfahren gewährleisten kann,

da die Benutzer-Kennungs-Informationen selbst dann nicht bekannt sind, wenn sie sich auf einem unsicheren Computer befinden. Es gibt nichts in dem im Objektstrom eingebetteten Anmerkungen, was entweder auf den Eigentümer oder den Inhalt von Anmerkungen eines Benutzers hinweist. Die sichtbare Struktur kann nur dazu verwenden werden, die Anzahl von Anmerkungen zu finden, die verarbeitet werden sollen – eine eher begrenzte Informationsmenge. Die Entscheidung darüber, ob der aktuelle Benutzer eine Anmerkungsgruppe ansehen kann, die sich innerhalb einer der Dateien des Datenstroms befindet, hängt lediglich von dem Verschlüsselungsverfahren und von der Qualität des Verschlüsselungscodes ab. Das heißt, es gibt keine „versteckten" Flags oder andere Hinweise darauf, wer Leser einer Anmerkungsgruppe ist, die sich innerhalb des Datenstromobjektes oder der Anmerkungsdatei im lokalen Modus befindet. Die Information über den Eigentümer befindet sich im verschlüsselten Abschnitt und kann nicht durch jemanden verändert werden, der nicht die Datei entschlüsseln und wieder herstellen kann.

Patentansprüche

1. Verfahren zum Schützen eines elektronischen Dokumentes, das umfasst:
Verschlüsseln des elektronischen Dokumentes unter Verwendung eines Dokumenten-Verschlüsselungscodes;
Erzeugen einer Mehrfachcode-Verschlüsselungstabelle zur Verwendung in einem Mehrfachcode-Verschlüsselungsverfahren, wobei die Tabelle wenigstens eine Mehrfachcode-Komponente umfasst;
Erzeugen eines verschlüsselten Headers (**250**), der Informationen umfasst, die das elektronische Dokument betreffen;
Verknüpfen einer Benutzerschnittstellen-Vorrichtung (**10**) mit dem verschlüsselten Header (**250**), der Mehrfachcode-Verschlüsselungstabelle und dem verschlüsselten elektronischen Dokument (**260**), wobei die Benutzerschnittstellen-Vorrichtung unverschlüsselte Informationen zum Identifizieren des elektronischen Dokumentes und ein interaktives Element umfasst, das den Benutzer befähigt, eine Benutzer-Berechtigung zum Zugriff auf wenigstens einen Teil des verschlüsselten elektronischen Dokumentes einzugeben;
Kombinieren der Benutzer-Berechtigung mit jeder der gespeicherten Mehrfachcode-Komponenten in der Mehrfachcode-Verschlüsselungscodetabelle, um den verschlüsselten Header (**250**) zu entschlüsseln; und
bei einer gültigen Entschlüsselung des verschlüsselten Headers (**250**) Entschlüsseln des Abschnitts des verschlüsselten elektronischen Dokuments (**260**), **dadurch gekennzeichnet**, dass der verschlüsselte Header (**250**) oder das verschlüsselte Dokument eine Verschlüsselungs-Markierung enthält, die eine willkürliche Zahlenfolge umfasst, auf die eine herleitbare Abwandlung dieser willkürlichen Zahlenfolge folgt, wobei eine gültige Entschlüsselung der Verschlüsselungs-Markierung anzeigt, dass der Dokumenten-Verschlüsselungscode gefunden worden ist.

2. Verfahren nach Anspruch 1, wobei die Benutzerschnittstellen-Vorrichtung (**10**) ein zweites elektronisches Dokument umfasst.

3. Verfahren nach einem der vorangehenden Ansprüche, wobei der verschlüsselte Header (**250**) und das verschlüsselte elektronische Dokument (**260**) unter Verwendung verschiedener Verschlüsselungscodes verschlüsselt werden, und wobei die Mehrfachcode-Verschlüsselungstabelle wenigstens eine Mehrfachcode-Komponente für jeden Verschlüsselungscode enthält.

4. Verfahren nach Anspruch 3, wobei der verschlüsselte Header (**250**) eine Verschlüsselungs-Markierung enthält, die eine willkürliche Zahlenfolge umfasst, auf die eine herleitbare Abwandlung dieser willkürlichen Zahlenfolge folgt, und eine gültige Entschlüsselung der Verschlüsselungs-Markierung anzeigt, dass der Header-Verschlüsselungscode gefunden worden ist.

5. Objekt mit sicherem Inhalt, das umfasst:
ein verschlüsseltes elektronisches Dokument (**12**), das mit einem Dokumenten-Verschlüsselungsschlüssel verschlüsselt worden ist;
einen verschlüsselten Header (**250**), der Informationen umfasst, die das elektronische Dokument betreffen;
eine Mehrfachcode-Verschlüsselungstabelle zur Verwendung in einem Mehrfachcode-Verschlüsselungsverfahren, wobei die Tabelle wenigstens eine Mehrfachcode-Komponente umfasst;
eine Benutzerschnittstellen-Vorrichtung (**10**), die unverschlüsselte Informationen zum Identifizieren des elektronischen Dokumentes (**12**) und ein interaktives Element umfasst, das einen Benutzer befähigt, eine Benutzer-Berechtigung zum Zugriff auf wenigstens einen Teil des verschlüsselten elektronischen Dokumentes einzugeben, zum Eingeben der Benutzer-Berechtigung in eine Entschlüsselungs-Maschine, die das Mehrfachcode-Verschlüsselungsverfahren verwendet, um die Benutzer-Berechtigung mit jeder der Mehrfachcode-Komponenten in der Mehrfachcode-Verschlüsselungscodetabelle zu kombinieren und den verschlüsselten Header zu entschlüsseln, und
zum Ermöglichen der Entschlüsselung des Teils des verschlüsselten elektronischen Dokumentes bei einer gültigen Entschlüsselung des verschlüsselten Headers, dadurch gekennzeichnet, dass der verschlüsselte Header (**250**) oder das verschlüsselte Dokument eine Verschlüsselungs-Markierung enthält, die eine willkürliche Zahlenfolge umfasst, auf die eine herleitbare Abwandlung dieser willkürlichen

Zahlenfolge folgt, wobei eine gültige Entschlüsselung der Verschlüsselungs-Markierung anzeigt, dass der Dokumenten-Verschlüsselungscode gefunden worden ist.

6. System zum Schützen eines elektronischen Dokumentes, das umfasst:
einen Speicher, der ein Objekt mit sicherem Inhalt und eine Mehrfachcode-Verschlüsselungscodetabelle zur Verwendung in einem Mehrfachcode-Verschlüsselungsverfahren speichert, wobei die Tabelle wenigstens eine Mehrfachcode-Komponente umfasst;
wobei das Objekt mit sicherem Inhalt ein verschlüsseltes elektronisches Dokument (**12**), das mit einem Dokumenten-Verschlüsselungscode verschlüsselt worden ist, und einen verschlüsselten Header (**250**) umfasst, wobei der verschlüsselte Header Informationen umfasst, die das elektronische Dokument betreffen, und eine Benutzerschnittstellen-Vorrichtung (**10**), die unverschlüsselte Informationen zum Identifizieren des elektronischen Dokumentes und ein interaktives Element umfasst, das einem Benutzer befähigt, eine Benutzer-Berechtigung zum Zugriff auf wenigstens einen Teil des verschlüsselten elektronischen Dokumentes einzugeben und bei einer gültigen Entschlüsselung des verschlüsselten Headers Entschlüsselung des Teils des verschlüsselten elektronischen Dokumentes ermöglicht;
eine Entschlüsselungs-Maschine (**18**), die ein Mehrfachcode-Verschlüsselungsverfahren verwendet; und
einen Prozessor zum Ausführen des interaktiven Elementes und zum Eingeben der Benutzer-Berechtigung in die Entschlüsselungs-Maschine;
wobei die Entschlüsselungs-Maschine (**18**) die Benutzer-Berechtigung mit jeder der Mehrfachcode-Komponenten in der Mehrfachcode-Tabelle kombiniert, um den verschlüsselten Header zu entschlüsseln, wobei eine gültige Entschlüsselung des verschlüsselten Headers anzeigt, dass der Dokumenten-Verschlüsselungscode gefunden worden ist, dadurch gekennzeichnet, dass der verschlüsselte Header (**250**) eine Verschlüsselungs-Markierung enthält, die eine willkürliche Zahlenfolge umfasst, auf die eine herleitbare Abwandlung dieser willkürlichen Zahlenfolge folgt, wobei eine gültige Entschlüsselung der Verschlüsselungs-Markierung anzeigt, dass der Dokumenten-Verschlüsselungsschlüssel gefunden worden ist.

7. System nach Anspruch 6, wobei das elektronische Dokument (**12**) eine Dokumenten-Kennung enthält und der Dokumenten-Verschlüsselungscode eine Kombination aus der Dokumenten-Kennung, der Benutzer-Information und der Mehrfachcode-Komponente für jeden berechtigten Benutzer enthält.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

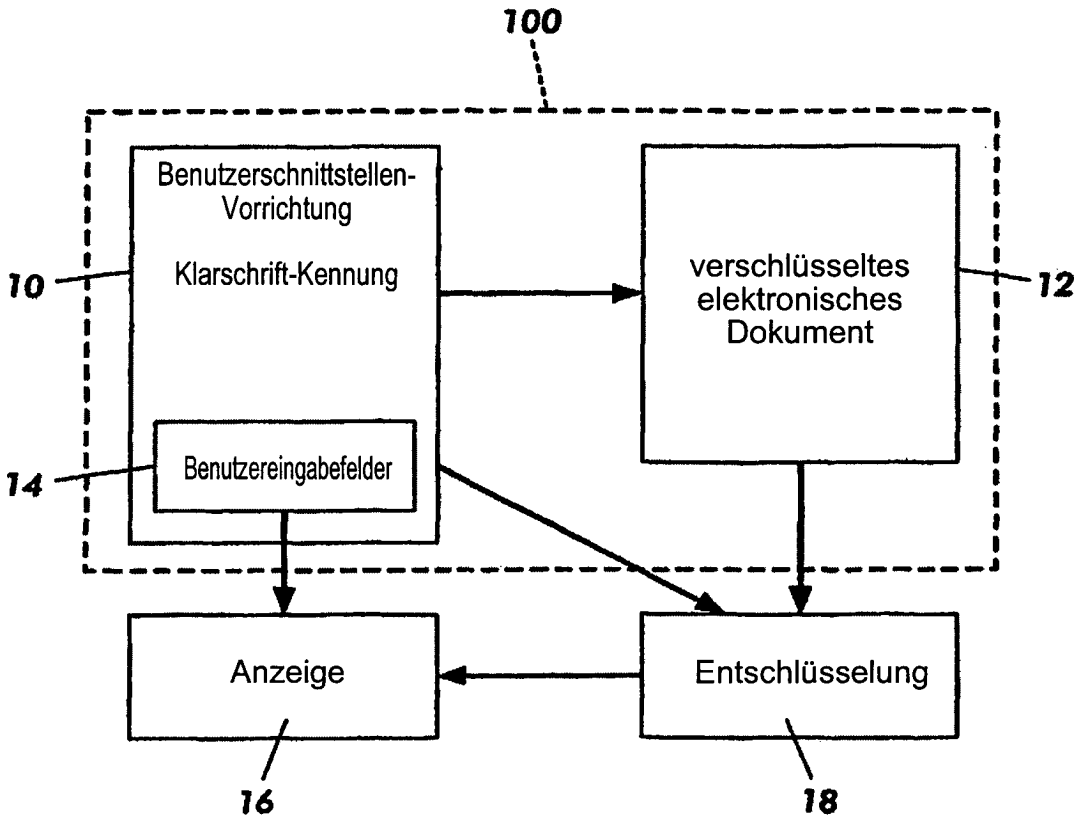

FIG. 1

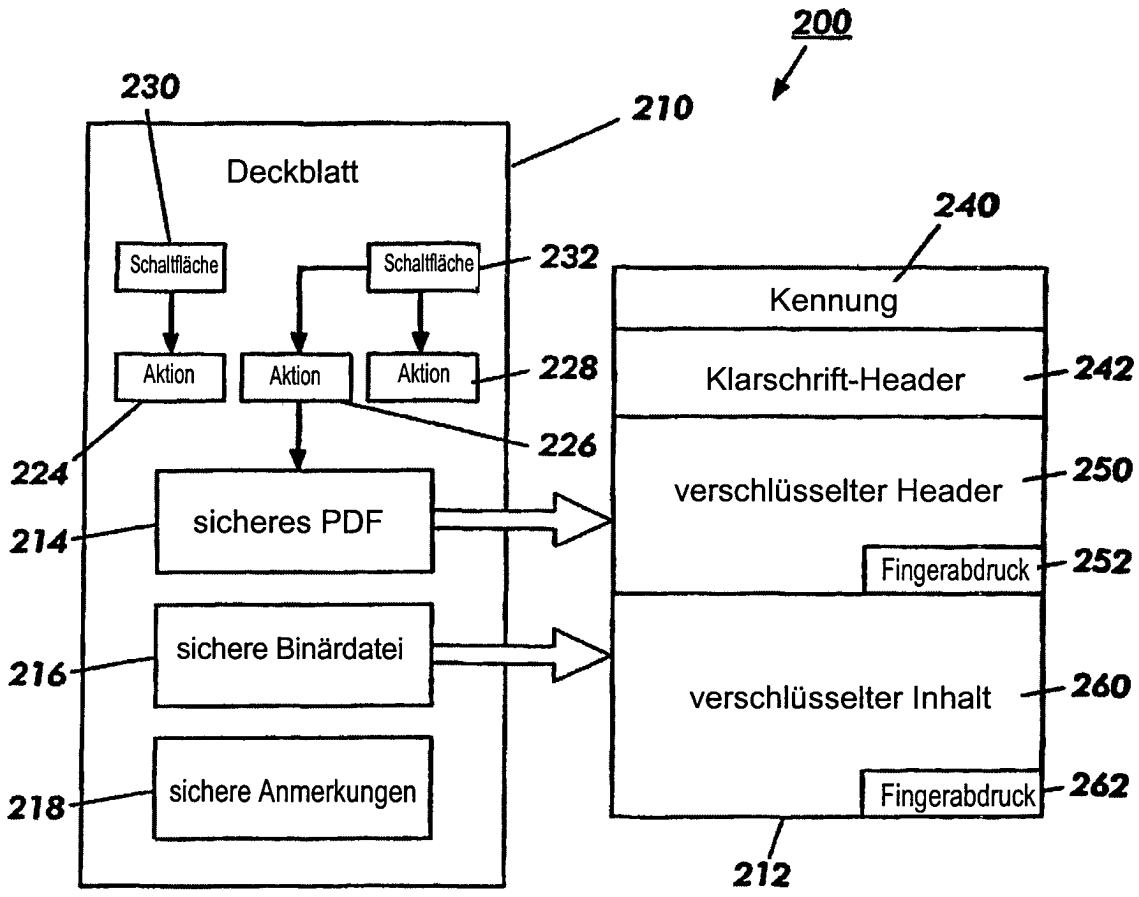
200
230
210
Deckblatt
240
Schaltfläche
Schaltfläche
232
Kennung
Aktion
Aktion
Aktion
228
Klarschrift-Header
242
226
224
verschlüsselter Header
250
214
sicheres PDF
Fingerabdruck
252
216
sichere Binärdatei
verschlüsselter Inhalt
260
218
sichere Anmerkungen
Fingerabdruck
262
212

FIG. 2