(19) Deutsches Patent- und Markenamt

(10) **DE 695 35 199 T3** 2016.01.14

(12) # Übersetzung der geänderten europäischen Patentschrift

(97) **EP 1 329 791 B2**
(21) Deutsches Aktenzeichen: **695 35 199.0**
(96) Europäisches Aktenzeichen: **03 00 8068.3**
(96) Europäischer Anmeldetag: **23.11.1995**
(97) Erstveröffentlichung durch das EPA: **23.07.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **23.08.2006**
(97) Veröffentlichungstag des geänderten Patents beim EPA: **26.08.2015**
(47) Veröffentlichungstag im Patentblatt: **14.01.2016**

(51) Int Cl.: ***G06F 1/00*** (2006.01)
H04L 29/06 (2006.01)
H04L 12/14 (2006.01)

Patentschrift wurde im Einspruchsverfahren geändert

(30) Unionspriorität:
344041 **23.11.1994** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
ContentGuard Holdings Inc., Wilmington, Del., US

(72) Erfinder:
Stefik, Mark J., Portola Valley, CA 94028, US

(74) Vertreter:
Grünecker Patent- und Rechtsanwälte PartG mbB, 80802 München, DE

(54) Bezeichnung: **Verfahren und System zur Steuerung der Verteilung und Benutzung von Digitalwerken, die eine Nutzungsrechtsgrammatik verwenden**

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

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf das Gebiet der Verteilung und Verwendung von Rechten, die geltend gemacht werden, für digital codierte Arbeiten (bzw. digital codierten Werke).

[0002] Eine grundsätzliche Maßnahme, die an die publizierende und informierende Industrie hin gerichtet ist, wenn sie eine elektronische Veröffentlichung vorsehen, ist diejenige, wie die nicht autorisierte und unbezahlte Verteilung oder Verwendung von elektronisch veröffentlichten Materialien zu verhindern ist. Elektronisch veröffentlichte Materialien werden typischerweise in einer digitalen Form verteilt und wieder auf einem auf einem Computer basierenden System erzeugt, das die Fähigkeit besitzt, die Materialien wieder zu erzeugen. Audio- und Video-Aufzeichnungen, Software, Bücher und Multimedia-Arbeiten (bzw. Multimedia-Werken) werden alle elektronisch veröffentlicht. Firmen in diesen Industrien erhalten Gebühren für alles, was zum Liefern von Materialien berechnet ist, z. B. den Verkauf einer Audio-CD in einem Verkaufsladen. Irgendeine nicht erfasste Verteilung einer Arbeit (bzw. eines Werkes) führt zu einer nicht bezahlten Gebühr (z. B. Kopieren der Audio-Aufzeichnungs-CD auf ein anderes, digitales Medium).

[0003] Die Einfachheit, mit der elektronisch veröffentlichte Arbeiten ”perfekt” wiedergegeben und verteilt werden können, ist ein Hauptpunkt. Die Übertragung von digitalen Arbeiten (bzw. digitalen Werken) über Netzwerke ist heute üblich. Ein solches weit verwendetes Netzwerk ist das Internet. Das Internet ist eine weitverbreitete Netzwerkeinrichtung, mit der Computer-Benutzer in vielen Universitäten, Firmen und staatlichen Einrichtungen kommunizieren und Ideen und Informationen austauschen. Computer Bulletin Boards gefunden in dem Internet, und kommerzielle Netzwerke, wie beispielsweise CompuServ und Prodigy, ermöglichen das Versenden und das Empfangen von digitalen Informationen. Informations-Service Dienste, wie beispielsweise Dialog und LEXIS/NEXIS, liefern Datenbanken von vorliegenden Informationen über eine breite Vielfalt von Themen. Ein anderer Faktor, der die Situation noch verschärfen wird, ist die Entwicklung und Erweiterung der National Information Infrastructure (NII). Es wird erwartet, dass sich, wenn die NII anwächst, die Übertragung von digitalen Werken über Netzwerke viele Male erhöhen wird. Es wäre wünschenswert, die NII zur Verteilung von digitalen Arbeiten ohne die Gefahr von weit verbreiteten, nicht autorisierten Kopien zu verwenden.

[0004] Die einfachste Art und Weise, um eine unbezahlte Verteilung zu erfassen, ist diejenige, ein nicht autorisiertes Kopieren und eine Übertragung zu verhindern. Für existierende Materialien, die in digitaler Form verteilt werden, werden verschiedene Sicherungen (Safe Guards) verwendet. In dem Fall einer Software sind Kopie-Schutz-Schemata, die die Zahl von Kopien begrenzen, die vorgenommen werden können, oder die die Ausgabe unterbrechen, wenn ein Kopieren erfasst ist, eingesetzt worden. Ein anderes Schema bewirkt, dass die Software gesperrt wird, nachdem eine vorbestimmte Zeitperiode abgelaufen ist. Eine Technik, die für eine auf einer Arbeitsstation basierenden Software verwendet wird, ist diejenige, zu fordern, dass eine spezielle Hardware-Vorrichtung an der Arbeitsstation vorhanden sein muss, damit die Software läuft; siehe z. B. US-A-4,932,054 mit dem Titel ”Method and Apparatus for Protecting Computer Software Utilizing Coded Filter Network in Conjunction with an Active Coded Hardware Device”. Solche Vorrichtungen sind mit der Software versehen und werden üblicherweise als ”Dongle” bezeichnet.

[0005] Ein noch anderes Konzept ist dasjenige, Software zu verbreiten, die allerdings einen ”Schlüssel” erfordert, um deren Verwendung zu ermöglichen. Dies wird in Verbreitungs-Schemata eingesetzt, wo ”Demos” der Software auf einem Medium zusammen mit dem gesamten Produkt vorgesehen sind. Die Demos können frei verwendet werden, allerdings muß, um das tatsächliche Produkt zu verwenden, der Schlüssel erhalten werden. Diese Schemata behindern nicht ein Kopieren der Software, wenn einmal der Schlüssel zu Anfang erworben ist.

[0006] PERRITT H H: „Knowbots, Permission Headers and Contract Law„ PROCEEDINGS TECHNOLOGICAL STRATEGIES FOR PROTECTING INTELLECTUAL PROPERTY IN THE NETWORKED MULTIMEDIA ENVIRONMENT, [Online] 30 April 1993, pages 39 to 50, Retrieved from the Internet an 2003-03-04 <URL: http://www.ifla.org/documents/infopol/copyright/perh2.txt>, beschreibt ein Konzept für eine digitale Bibliothek für Informationsobjekte, die über ein elektronisches Netzwerk verbreitet werden. Diese Objekte verbleiben auf Servern und können von entfernten Benutzern unter Benutzung von Client-Geräten abgerufen werden. Das Konzept dieser digitalen Bibliothek sieht vor, dass vollständige Informationsressourcen und nicht lediglich bibliographische Informationen abgerufen werden. Das Konzept der digitalen Bibliothek betrachtet drei grundsätzliche architektonische Elemente, nämlich eine Anfrage (die auch als „Knowbot” bezeichnet wird), einen Genehmigungskopf (Permission Header), der an jedes Informationsobjekt angehangen ist und eine Vorgehensweise zum Abgleichen der Anfrage mit dem Genehmigungskopf. Nachdem die Informationsobjekte die digitale Bibliothek verlassen haben, kann ein Vertrag regeln was ein Käufer mit der Information anfangen darf.

[0007] US 5,138,712 offenbart eine Vorrichtung und ein Verfahren zum Lizenzieren von Software in einem Computernetzwerk, wobei die Softwareanwendung mit einem Lizenzserver mittels einer Lizenzierungsbibliothek kommuniziert. Wenn ein Benutzer einer Softwareanwendung ausführen möchte, erzeugt die Lizenzierungsbibliothek einen Aufruf, der einen Lizenz-Token von dem Lizenzserver anfordert. Der Lizenzserver ermittelt den richtigen Lizenz-Token für die Softwareanwendung und übermittelt diesen zu der Lizenzierungsbibliothek.

[0008] Es ist deshalb die Aufgabe der vorliegenden Erfindung ein verbessertes System und Verfahren zum Steuern der Verbreitung und Benutzung von digitalen Werken bereitzustellen.

[0009] Diese Aufgabe wird durch den Gegenstand der unabhängigen Ansprüche 1 und 21 gelöst.

[0010] Bevorzugte Ausführungsformen sind in den abhängigen Ansprüchen beschrieben.

[0011] Ein System zum Steuern der Verwendung und Verteilung von digitalen Werken ist offenbart. Ein digitales Werk ist jedes geschriebene, mündliche, grafische oder videobasierte Werk, das in eine digitale Form übersetzt wurde oder in dieser geschaffen wurde, und welches wiedererzeugt werden kann unter Verwendung geeigneter Wiedergabeeinrichtungen, wie beispielsweise Softwareprogramme. Die vorliegende Erfindung erlaubt dem Besitzer eines digitalen Werks Benutzungsrechte an ihr Werk beizufügen. Die Benutzungsrechte legen fest wie das digitale Werk benutzt und verteilt werden kann. Diese Benutzungsrechte werden ein Teil des digitalen Werks und werden immer gewürdigt.

[0012] Instanzen von Benutzungsrechten werden definiert unter Verwendung einer flexiblen und erweiterbaren Syntax für Verwendungsrechte. Begrifflich ist ein Recht in der Syntax für Verwendungsrechte eine Bezeichnung, der ein vorbestimmtes Verhalten und Bedingungen zum Ausführen des Rechts zugeordnet sind. Beispielsweise ein Kopierrecht bedeutet, dass eine Kopie des digitalen Werks gemacht werden kann. Eine Bedingung zum Ausführen des Rechtes ist, dass der Anfragende gewisse Sicherheitskriterien erfüllen muss. Bedingungen können auch angehängt sein, um das Recht selbst zu begrenzen. Zum Beispiel ein Leihrecht kann definiert werden, um die Dauer, mit welcher ein Werk ausgeliehen werden kann, zu begrenzen.

[0013] In der vorliegenden Erfindung umfasst ein Verwendungsrecht einen Rechte-Code zusammen mit verschiedenen Bedingungen zum Ausführen des Rechts. Solche Bedingungen schließen eine Kopier-Zählbedingung zum Begrenzen der Anzahl ein, wie oft ein Recht aufeinanderfolgend ausgeführt werden kann (beispielsweise Begrenzen der Anzahl von Kopien zur Leihe auf eine vorbestimmte Anzahl), eine Sicherheitsklassenbedingung zum Sicherstellen, dass ein Verwahrungsort einen ausreichenden Grad an Sicherheit hat, Zugriffsbedingungen zum Festlegen von Zugriffstests, die erfüllt werden müssen, eine zeitliche Festlegung zum Anzeigen zeitbasierter Einschränkungen für das Ausführen eines Rechts und eine Gebührenspezifikation zum Anzeigen von Verwendungsgebühren für das Ausführen eines Rechts. Einem digitalen Werk können verschiedene Versionen eines Rechtes angehangen werden. Eine Version eines Rechts wird den gleichen Rechte-Code wie andere Versionen haben, aber die Bedingungen (und typischerweise die Gebühren) würden unterschiedlich sein.

[0014] Digitale Werke und ihre angehängten Verwendungsrechte werden in Verwahrungsorten gespeichert. Digitale Werke werden übertragen zwischen Verwahrungsorten. Verwahrungsorte interagieren zum Austauschen digitaler Werke gemäß einem vorbestimmten Satz von Verwendungstransaktionsschritten. Das Verhalten eines Verwendungsrechts wird verkörpert in einem vorbestimmten Satz von Verwendungsübertragungsschritten. Die Verwendungsübertragungsschritte prüfen weiterhin alle Bedingungen, welche erfüllt sein müssen, bevor das Recht ausgeführt werden kann. Diese Verwendungsübertragungsschritte definieren ein Protokoll, das von den Verwahrungsorten verwendet wird zum Anfragen des Ausübens eines Rechts und des Durchführens eines Rechts.

[0015] Ein System und ein Verfahren gemäß der Erfindung werden nun, anhand eines Beispiels, unter Bezugnahme auf die beigefügten Zeichnungen beschrieben, in denen:

[0016] Fig. 1 zeigt ein Flussdiagramm, das einen einfachen Fall der Betriebsweise der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung darstellt.

[0017] Fig. 2 zeigt ein Blockdiagramm, das die verschiedenen Verwahrungs-Typen und den Verwahrungsstellen-Transaktions-Fluss dazwischen in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung darstellt.

[0018] Fig. 3 zeigt ein Blockdiagramm, das eine Verwahrungsstelle, verbunden mit einem Kredit-Server, in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung zeigt.

[0019] Fig. 4a und **Fig.** 4b zeigen Beispiele von Gestaltungssystemen, wie sie in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung verwendet werden können.

[0020] Fig. 5 stellt ein Inhalt-Datei-Layout für eine digitale Arbeit dar, wie es in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung verwendet werden kann.

[0021] Fig. 6 stellt ein Inhalt-Datei-Layout für eine individuelle, digitale Arbeit der digitalen Arbeit der **Fig.** 5 dar, wie es in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung verwendet werden kann.

[0022] Fig. 7 stellt die Komponenten eines Beschreibungsblocks der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung dar.

[0023] Fig. 8 stellt einen Beschreibungsbaum für das Inhalt-Datei-Layout der digitalen Arbeit, dargestellt in **Fig.** 5, dar.

[0024] Fig. 9 stellt einen Bereich eines Beschreibungsbaums entsprechend der individuellen, digitalen Arbeit, dargestellt in **Fig.** 6, dar.

[0025] Fig. 10 stellt ein Layout für den Rechte-Bereich des Beschreibungsblocks dar, wie er in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung verwendet werden kann.

[0026] Fig. 11 zeigt einen Beschreibungsbaum, wo bestimmte d-Blöcke PRINT Benutzungsrechte haben, und der dazu verwendet wird ”strikte” und ”nachsichtige” Regeln zum Auflösen von Nutzungsrechte-Konflikten darzustellen.

[0027] Fig. 12 zeigt ein Blockdiagramm der Hardware-Komponenten einer Verwahrungsstelle, wie sie in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung verwendet werden.

[0028] Fig. 13 zeigt ein Blockdiagramm der funktionalen (logischen) Komponenten einer Verwahrungsstelle, wie sie in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung verwendet werden.

[0029] Fig. 14 zeigt ein Diagramm, das die Basis-Komponenten eines Benutzungsrechts in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung darstellt.

[0030] Fig. 15 listet die Verwendungs-Rechte-Grammatik der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung auf.

[0031] Fig. 16 zeigt ein Flussdiagramm, das die Schritte einer Zertifikat-Lieferung, einer Notlist-Prüfung und eines Funktions-Testens darstellt, wie dies in einer Registrierungs-Transaktion durchgeführt wird, so, wie dies in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung vorgenommen werden kann.

[0032] Fig. 17 zeigt ein Flussdiagramm, das die Schritte von einem Sitzungs-Informations-Austausch und der Takt-Synchronisierung darstellt, wie dies in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung durchgeführt werden kann, nachdem jede Verwahrungsstelle in der Registrierungs-Transaktion erfolgreich die Schritte, beschrieben in **Fig.** 16, abgeschlossen hat.

[0033] Fig. 18 zeigt ein Flussdiagramm, das den Basis-Fluss für eine Benutzungs-Transaktion darstellt, umfassend den üblichen Öffnungs- und Schließ-Schritt, wie dies in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung durchgeführt werden kann.

[0034] Fig. 19 zeigt ein Zustands-Diagramm von Server und Client-Verwahrungsstellen gemäß einem Transport-Protokoll, dem gefolgt wird, wenn eine digitale Arbeit von dem Server zu den Client-Verwahrungsstellen bewegt wird, wie dies in der derzeit bevorzugten Ausführungsform der vorliegenden Erfindung durchgeführt werden kann.

ÜBERSICHT

[0035] Ein System zum Kontrollieren einer Verwendung und Verteilung von digitalen Arbeiten ist offenbart. Die vorliegende Erfindung ist auf ein Unterstützen kommerzieller Transaktionen, digitale Arbeiten einsetzend, gerichtet.

[0036] Hier beziehen sich die Ausdrücke ”digitale Arbeit”, ”Arbeit” und ”Inhalt” auf irgendeine Arbeit, die zu einer digitalen Darstellung umgesetzt worden ist. Dies würde irgendeine Audio-, Video-, Text- oder Multimedia-Arbeit und irgendeinen begleitenden Interpretierer (z. B. Software), die zum erneuten Erzeugen der Arbeit erforderlich sein können, umfassen. Der Ausdruck Composit-Arbeit bezieht sich auf eine digitale Arbeit, aufgebaut aus einer Zusammenstellung von anderen, digitalen Arbeiten. Der Ausdruck ”Verwendungs-Benutzungsrechte” oder ”Rechte” ist ein Ausdruck, der sich auf Rechte bezieht, die einem Empfänger einer digitalen Arbeit erteilt sind. Allgemein definieren diese Rechte, wie eine digitale Arbeit verwendet werden kann, und ob sie weiter verteilt werden kann. Jedes Benutzungsrecht kann eine oder mehrere, spezifizierte Bedingung(en) haben, die erfüllt werden müssen, bevor das Recht ausgeübt werden kann.

[0037] **Fig.** 1 zeigt ein Flussdiagramm auf hohem Niveau, das verschiedene Details weglässt, das allerdings die Basis-Operation der vorliegenden Erfindung demonstriert. Wie **Fig.** 1 zeigt, erzeugt ein Erzeuger eine digitale Arbeit, Schritt **101**. Der Erzeuger wird dann geeignete Benutzungsrechte und Gebühren bestimmen, sie an die digitale Arbeit anhängen und sie in einer Verwahrungsstelle 1 speichern, Schritt **102**. Die Beendigung geeigneter Benutzungsrechte und von Gebühren wird von verschiedenen, ökonomischen Faktoren abhängen. Die digitale Arbeit verbleibt sicher in der Verwahrungsstelle 1, bis eine Anforderung für einen Zugriff empfangen ist. Die Anforderung für einen Zugriff beginnt mit einer Sitzungs-Initiierung durch eine andere Verwahrungsstelle. Hier zeigt eine Verwahrungsstelle 2 eine Sitzung mit Verwahrungsstelle 1 an, Schritt **103**. Wie im größeren Detail nachfolgend beschrieben werden wird, umfasst diese Sitzungs-Initiierung Schritte, die dabei helfen, sicherzustellen, dass die jeweiligen Verwahrungsstellen vertrauenswürdig sind. Unter der Annahme, dass eine Sitzung eingerichtet werden kann, kann die Verwahrungsstelle 2 dann einen Zugriff auf die digitale Arbeit für einen angegebenen Zweck anfordern, Schritt **104**. Der Zweck kann, zum Beispiel, derjenige sein, die digitale Arbeit zu drucken oder eine Kopie der digitalen Arbeit zu erhalten. Der Zweck wird einem spezifischen Benutzungsrecht entsprechen. In jedem Fall prüft die Verwahrungsstelle 1 die Benutzungsrechte, die der digitalen Arbeit zugeordnet sind, um zu bestimmen, ob der Zugriff auf die digitale Arbeit erteilt werden kann, Schritt **105**. Die Prüfung der Benutzungsrechte umfasst im Wesentlichen eine Bestimmung, ob ein Recht, zugeordnet der Zugriffs-Anforderung, an die digitale Arbeit angehängt worden ist und ob alle Bedingungen, zugeordnet dem Recht, erfüllt sind. Wenn der Zugriff verweigert wird, beendet die Verwahrungsstelle 1 die Sitzung mit einer Fehler-Nachricht, Schritt **106**. Falls ein Zugriff erteilt ist, überträgt die Verwahrungsstelle 1 die digitale Arbeit zu der Verwahrungsstelle 2, Schritt **107**. Wenn einmal die digitale Arbeit zu der Verwahrungsstelle 2 übertragen worden ist, erzeugen die Verwahrungsstellen 1 und 2 jeweils Zahlinformationen für den Zugriff, die zu einem Kredit-Server übertragen werden, Schritt **108**. Ein solcher Doppel-Zahlungs-Bericht wird vorgenommen, um gegen Versuche sicher zu sein, den Zahlvorgang zu umgehen.

[0038] **Fig.** 2 stellt die Basis-Interaktionen zwischen Verwahrungs-Typen in der vorliegenden Erfindung dar. Wie anhand von **Fig.** 2 ersichtlich werden wird, werden die verschiedenen Verwahrungs-Typen unterschiedlichen Funktionen dienen. Es ist grundsätzlich, dass die Verwahrungsstellen einen Kernsatz einer Funktionalität gemeinsam teilen werden, der sichere und vertrauensvolle Kommunikationen sicherstellen wird. Wie **Fig.** 2 zeigt, stellt eine Verwahrungsstelle **201** den allgemeinen Fall einer Verwahrungsstelle dar. Die Verwahrungsstelle **201** besitzt zwei Betriebsmoden; einen Server-Modus und einen Anforderer-Modus. Wenn in dem Server-Modus gearbeitet wird, wird die Verwahrungsstelle Zugriffsanforderungen auf digitale Arbeiten empfangen und verarbeiten. Wenn in dem Anforderer-Modus gearbeitet wird, wird die Verwahrungsstelle Anforderungen für einen Zugriff auf digitale Arbeiten initiieren. Die Verwahrungsstelle **201** ist allgemein in dem Sinne, dass deren primärer Zweck derjenige ist, ein Medium für digitale Arbeiten auszutauschen. Während des Betriebs kann die Verwahrungsstelle **201** mit einer Vielzahl von anderen Verwahrungsstellen kommunizieren, nämlich einer Autorisierungs-Verwahrungsstelle **202**, einer Gestaltungs-Verwahrungsstelle **203** und einer Master-Verwahrungsstelle **204**. Eine Kommunikation zwischen Verwahrungsstellen tritt unter Verwendung eines Verwahrungsstellen-Transaktions-Protokolls **205** auf. Eine Kommunikation mit einer Autorisierungs-Verwahrungsstelle **202** kann dann auftreten, wenn eine digitale Arbeit, auf die gerade zugegriffen wird, eine Bedingung besitzt, die eine Autorisierung erfordert. Demzufolge ist eine Autorisierung ein digitales Zertifikat, so dass ein Besitz des Zertifikats erforderlich ist, um einen Zugriff auf die digitale Arbeit zu erhalten. Eine Autorisierung ist selbst eine digitale Arbeit, die zwischen Verwahrungsstellen bewegt werden kann und Gebühren und Bedingungen von Benutzungsrechten unterworfen werden kann. Eine Autorisierung kann durch beide Verwahrungsstellen erforderlich sein, die bei einem Zugriff auf eine digitale Arbeit betroffen sind.

[0039] Eine Kommunikation mit einer gestaltenden Verwahrungsstelle **203** tritt in Verbindung mit der Gestaltung einer digitalen Arbeit auf. Wie in größerem Detail nachfolgend beschrieben werden wird, ist eine gestaltende Verwahrungsstelle mit einer gestaltenden Vorrichtung (z. B. einer Druckervorrichtung) verbunden, um ein Gestaltungssystem aufzuweisen.

[0040] Eine Kommunikation mit einer Master-Verwahrungsstelle **205** tritt in Verbindung mit einem Erhalten eines Identifikations-Zertifikats auf. Identifikations-Zertifikate sind die Mittel, mit denen eine Verwahrungsstelle als ”vertrauenswürdig” identifiziert ist. Die Verwendung von Identifikations-Zertifikaten wird nachfolgend in Bezug auf die Registrierungs-Transaktion beschrieben.

[0041] **Fig.** 3 stellt die Verwahrungsstelle **201**, verbunden mit einem Kredit-Server **301**, dar. Der Kredit-Server **301** ist eine Vorrichtung, die Zahlungsinformationen für die Verwahrungsstelle **201** sammelt. Der Kredit-Server **301** kommuniziert mit der Verwahrungsstelle **201** über Zahlungstransaktionen **302**, um Zahlungstransaktionen aufzuzeichnen. Zahlungstransaktionen werden an eine Rechnungs-Verrechnungsstelle **303** durch den Kredit-Server **301** auf einer periodischen Basis hin berichtet. Der Kredit-Server **301** kommuniziert mit der Zahlungs-Verrechnungsstelle **303** über Zahlungsstellen-Transaktionen **304**. Die Zahlungsstellen-Transaktionen **304** ermöglichen eine sichere und verschlüsselte Übertragung der Informationen zu der Zahlungs-Verrechnungsstelle **303**.

GESTALTUNGSSYSTEME

[0042] Ein Gestaltungssystem ist allgemein als ein System definiert, das eine Verwahrungsstelle und eine Gestaltungsvorrichtung aufweist, die eine digitale Arbeit zu deren erwünschter Form gestalten kann. Beispiele eines Gestaltungssystems können ein Computersystem, ein digitales Audio-System, oder ein Drucker sein. Ein Gestaltungssystem besitzt dieselben Sicherheitsmerkmale wie eine Verwahrungsstelle. Die Verbindung einer gestaltenden Verwahrungsstelle mit der Gestaltungsvorrichtung kann in einer Art und Weise auftreten, die für den Typ einer Gestaltungsvorrichtung geeignet ist.

[0043] **Fig.** 4 stellt einen Drucker als ein Beispiel eines Gestaltungssystems dar. Wie **Fig.** 4 zeigt, besitzt das Druckersystem **401** darin enthalten eine Drucker-Verwahrungsstelle **402** und eine Druckvorrichtung **403**. Es sollte angemerkt werden, dass die unterbrochene Linie, die das Druckersystem **401** definiert, eine Sicherheitssystemgrenze definiert. Kommunikationen innerhalb der Grenze werden dahingehend angenommen, dass sie sicher sind. In Abhängigkeit von dem Sicherheitsniveau stellt die Grenze auch eine Barriere dar, die dazu vorgesehen ist, eine physikalische Integrität zu erzielen. Die Drucker-Verwahrungsstelle **402** wird in einigen Fällen eine kurzlebige Kopie einer digitalen Arbeit enthalten, die verbleibt, bis sie durch die Druckmaschine **403** ausgedruckt ist. In anderen Fällen kann die Drucker-Verwahrungsstelle **402** digitale Arbeiten enthalten, wie beispielsweise Schriftzeichen, die verbleiben werden und die basierend auf der Verwendung in Rechnung gestellt werden können. Dieses Design stellt sicher, dass alle Kommunikationsleitungen zwischen Druckern und Druckvorrichtungen verschlüsselt sind, ohne dass sie sich innerhalb einer physikalischen Sicherheitsgrenze befinden. Das Design-Merkmal eliminiert einen potentiellen ”Fehler” Punkt, über den die digitale Arbeit geeignet erhalten werden könnte. Die Druckervorrichtung **403** stellt die Druckerkomponenten dar, die dazu verwendet werden, die gedruckte Ausgabe zu erzeugen.

[0044] Auch ist in **Fig.** 4a die Verwahrungsstelle **404** dargestellt. Die Verwahrungsstelle **404** ist mit der Drucker-Verwahrungsstelle **402** verbunden. Die Verwahrungsstelle **404** stellt eine externe Verwahrungsstelle dar, die digitale Arbeiten enthält.

[0045] **Fig.** 4b stellt ein Beispiel eines Computersystems als ein Gestaltungssystem dar. Ein Computersystem kann eine ”Multifunktions-”Vorrichtung bilden, da sie digitale Arbeiten (z. B. Software-Programme) ausführen und digitale Arbeiten (z. B. eine digitalisierte Fotografie) anzeigen kann. Logischerweise kann jede Gestaltungsvorrichtung so angesehen werden, dass sie deren eigene Verwahrungsstelle besitzt, obwohl nur eine physikalische Verwahrungsstelle benötigt wird. Wie **Fig.** 4b zeigt, besitzt ein Computersystem **410** darin enthalten eine Anzeige/Ausführungs-Verwahrungsstelle **411**. Die Anzeige/Ausführungs-Verwahrungsstelle **411** ist mit einer Anzeigevorrichtung **412** und einer Ausführungsvorrichtung **413** verbunden. Der Kasten in unterbrochener Linie, der das Computersystem **410** umgibt, stellt eine Sicherheitsgrenze dar, innerhalb der Kommunikationen dahingehend angenommen werden, dass sie sicher sind. Die Anzeige/Ausführungs-Verwahrungsstelle **411** ist weiterhin mit einem Kredit-Server **414** verbunden, um irgendwelche Gebühren, die in Rechnung gestellt werden sollen, für einen Zugriff auf eine digitale Arbeit und eine Verwahrungsstelle **415** zum Zugreifen auf digitale Arbeiten, gespeichert darin, zu berichten.

[0046] Benutzungsrechte werden direkt an digitale Arbeiten angehängt. Demzufolge ist es wichtig, die Struktur einer digitalen Arbeit zu verstehen. Die Struktur einer digitalen Arbeit, insbesondere von digitalen Composit-Arbeiten, kann natürlich in einer azyklischen Struktur organisiert werden, wie beispielsweise einer Hierarchie. Zum Beispiel besitzt ein Magazin verschiedene Artikel und Fotografien, die erzeugt worden sein können und unterschiedlichen Personen gehören. Jeder dieser Artikel und jede der Fotografien kann einen Knoten in einer hierarchischen Struktur darstellen. Demzufolge können Kontrollen, d. h. Benutzungsrechte, an jedem Knoten durch den Erzeuger bzw. Urheber platziert werden. Durch Ermöglichen einer Kontrolle und einer Gebührenberechnung, die jedem Knoten zugeordnet werden, kann ein Erzeuger einer Arbeit sicher sein, dass die Rechte und die Gebühren nicht umgangen werden.

[0047] In der derzeit bevorzugten Ausführungsform werden die Datei-Informationen für eine digitale Arbeit in zwei Dateien unterteilt: Eine ”Inhalt” Datei und eine ”Beschreibungsbaum” Datei. Von der Perspektive einer Verwaltungsstelle aus gesehen ist die ”Inhalt” Datei eine Folge von adressierbaren Bytes, deren Format vollständig von dem Interpretierer abhängt, der verwendet wird, um die digitale Arbeit abzuspielen, anzuzeigen oder zu drucken. Die Beschreibungsbaum-Datei macht es möglich, die Rechte und die Gebühren für eine Arbeit ohne Bezugnahme auf den Inhalt der digitalen Arbeit zu prüfen. Es sollte angemerkt werden, dass sich der Ausdruck Beschreibungsbaum so, wie er hier verwendet wird, auf irgendeinen Typ einer azyklischen Struktur bezieht, die verwendet wird, um die Beziehung zwischen den verschiedenen Komponenten einer digitalen Arbeit darzustellen.

[0048] **Fig.** 5 stellt das Layout der Inhalt-Datei dar. Wie **Fig.** 5 zeigt, ist eine digitale Arbeit aus einer Geschichte A **510**, einer Anzeige **511**, einer Geschichte B **512** und einer Geschichte C **513** aufgebaut. Es wird angenommen, dass die digitale Arbeit gespeichert ist, beginnend an einer relativen Adresse von 0. Jeder der Teile der digitalen Arbeit ist linear so gespeichert, dass die Geschichte A **510** an ungefähr Adressen 0–30.000 gespeichert ist, die Anzeige **511** an Adressen 30.001–40.000 gespeichert ist, die Geschichte B **512** an Adressen 40.001–60.000 gespeichert ist, und die Geschichte C **513** an Adressen 60.001-85K gespeichert ist. Das Detail in der Geschichte A **510** ist in **Fig.** 6 dargestellt. Wie **Fig.** 6 zeigt, ist die Geschichte A **510** weiter aufgeteilt, um einen Text **614** zu zeigen, der an der Adresse 0–1500 abgespeichert ist, ein Foto **615** eines Soldaten an Adressen 1501–10.000, Grafiken **616**, gespeichert an Adressen 10.001–25.000, und einen Seitenbalken **617**, gespeichert an einer Adresse 25.001–30.000. Es ist anzumerken, dass die Daten in der Inhalt-Datei komprimiert (zum Einsparen von Speicher) oder verschlüsselt (zur Sicherheit) sein können.

[0049] Aus den **Fig.** 5 und **Fig.** 6 ist leicht zu beobachten, dass eine digitale Arbeit durch deren Komponenten-Teilen als eine Hierarchie dargestellt werden kann. Der Beschreibungsbaum für eine digitale Arbeit ist aus einem Satz von in Bezug stehenden Deskriptor-Blöcken, (descriptor-blocks), (d-Blöcken) aufgebaut. Die Inhalte jedes d-Blocks werden in Bezug auf **Fig.** 7 beschrieben. Wie **Fig.** 7 zeigt, umfasst ein d-Block **700** einen Identifizierer **701**, der ein eindeutiger Identifizierer für die Arbeit in der Verwahrungsstelle ist, eine Startadresse **702**, die die Startadresse des ersten Bytes der Arbeit liefert, eine Länge **703**, die die Anzahl von Bytes in der Arbeit angibt, einen Rechte-Bereich **704**, wo die gewährten Benutzungsrechte und deren Status-Daten beibehalten werden, einen Parent-Hinweiszeiger **705** zum Hinweisen auf einen Parent-d-Block und einem Child-Hinweiszeiger **706** zum Hinweisen auf die Child-d-Blöcke. In der derzeit bevorzugten Ausführungsform besitzt der Identifizierer **701** zwei Teile. Der erste Teil ist eine eindeutige Zahl, die der Verwahrungsstelle bei der Herstellung zugeordnet ist. Der zweite Teil ist eine eindeutige Zahl, die der Arbeit bei der Erzeugung zugeordnet ist. Der Rechte-Bereich **704** wird eine Datenstruktur enthalten, wie beispielsweise eine Durchsichtstabelle, wo die verschiedenen Informationen, zugeordnet zu einem Recht, beibehalten werden. Die Informationen, die durch die jeweiligen Nutzungsrechte erforderlich sind, werden in weiterem Detail nachfolgend beschrieben. D-Blöcke bilden eine strikte Hierarchie. Der obere d-Block einer Arbeit besitzt kein Parent; alle anderen d-Blöcke besitzen ein Parent. Die Beziehung von Benutzungsrechten zwischen Parent- und Child-d-Blöcken, und wie Konflikte gelöst werden, wird nachfolgend beschrieben. Ein spezieller Typ eines d-Blocks ist ein ”Mantel” (”Shell”) d-Block. Ein Mantel-d-Block fügt einen neuen Inhalt über den Inhalt seiner Teile hinaus hinzu. Ein Mantel-d-Block wird dazu verwendet, Rechte und Gebühren-Informationen, typischerweise durch Distributoren von digitalen Arbeiten, hinzuzufügen.

[0050] **Fig.** 8 stellt einen Beschreibungsbaum für die digitale Arbeit von **Fig.** 5 dar. Wie **Fig.** 8 zeigt, weist ein oberer d-Block **820** für die digitale Arbeit auf die verschiedenen Geschichten und Anzeigen, die darin enthalten sind, hin. Hierbei weist der obere d-Block **820** auf einen d-Block **821** (darstellend eine Geschichte A **510**), auf einen d-Block **822** (die Anzeige **511** darstellend), auf einen d-Block **823** (die Geschichte B **512** darstellend) und einen d-Block **824** (eine Geschichte C **513** darstellend) hin.

[0051] Der Bereich des Beschreibungsbaums für die Geschichte A **510** ist in **Fig.** 9 dargestellt. Ein d-Block **925** stellt einen Text **614** dar, ein d-Block **926** stellt ein Foto **615** dar, ein d-Block **927** stellt Grafiken **616** dar und ein d-Block **928** stellt einen Seitenbalken **617** dar.

[0052] Der Rechte-Bereich **704** eines Deskriptor-Blocks ist weiterhin in **Fig.** 10 dargestellt. **Fig.** 10 stellt eine Struktur dar, die in dem Rechte-Bereich **704** für jedes Recht wiederholt wird. Wie **Fig.** 10 zeigt, wird jedes Recht ein Rechte-Code-Feld **1050** und ein Status-Informations-Feld **1052** haben. Das Rechte-Code-Feld **1050** wird einen eindeutigen Code, zugeordnet zu einem Recht, enthalten. Das Status-Informations-Feld **1052** wird Informationen enthalten, die sich auf den Zustand eines Rechts und die digitale Arbeit beziehen. Solche Informationen sind nachfolgend in Tabelle 1 angegeben. Die Rechte, wie sie in dem Rechte-Bereich **704** gespeichert sind, können typischerweise in einer nummerischen Reihenfolge basierend auf dem Rechte-Code vorhanden sein.

Eigenschaft	Wert	Benutzung
Kopien in Verwendung (Copies-in-Use)	Zahl (Number)	Ein Zähler der Zahl von Kopien einer Arbeit, die in Benutzung ist. Erhöht, wenn eine andere Kopie verwendet wird; erniedrigt, wenn die Verwendung abgeschlossen ist
Leih-Periode (Loan-Period)	Zeit-Einheiten (Time-Units)	Indikator der maximalen Zahl von Zeit-Einheiten, für die ein Dokument ausgeliehen werden kann
Leiher-Kopie (Loaner-Copy)	Bool'sche (Boolean)	Indikator, dass die momentane Arbeit eine ausgeliehene Kopie einer autorisierten, digitalen Arbeit ist.
Verbleibende Zeit (Remaining-Time)	Zeit-Einheiten (Time-Units)	Indikator der verbleibenden Zeit einer Verwendung in Bezug auf ein erfasstes Dokumenten-Recht.
Dokumenten-Deskriptor (Document-Descr)	Folge (String)	Eine Folge, die verschiedene, identifizierende Information über ein Dokument enthält. Das exakte Format hiervon ist nicht spezifiziert, sondern es kann Informationen umfassen, wie beispielsweise einen Namen eines Verlegers, Autor-Name, ISBN-Nummer, usw..
Einnahmen-Besitzer (Revenue-Owner)	RO-Deskriptor (RO-Descr)	Ein Instrument, das einen Einnahmen-Besitzer für eine digitale Arbeit identifiziert. Dies wird zum Berichten über Benutzungsgebühren verwendet.
Veröffentlichungsdatum (Publication-Date)	Datum-Deskriptor (Date-Descr)	Das Datum, zu dem die digitale Arbeit veröffentlicht wurde.
Historie-Aufzeichnung (History-list)	Historie-Recht (History-Rec)	Eine Liste von Ereignissen, die die Verwahrungsstellen und die Daten für Operationen, die eine digitale Arbeit kopieren, übertragen, aktualisieren oder erneut speichern, aufzeichnen.

TABELLE 1

ZUSTAND-INFORMATIONEN FÜR DIE DIGITALE ARBEIT

[0053] Die Maßnahme zum Darstellen von digitalen Arbeiten durch Separieren von Beschreibungsdaten von einem Inhalt nimmt an, dass Teile einer Datei fortlaufend sind, nimmt allerdings keine Position auf der tatsächlichen Darstellung eines Inhalts vor. Insbesondere ist sie neutral zu der Frage, ob eine Inhalt-Darstellung eine Objektorientierte Maßnahme annehmen kann. Sie würde natürlich einen Inhalt als Objekte darstellen. Im Prinzip kann es passend sein, Inhalt-Objekte zu haben, die die Zahlungs-Struktur und die Rechte-Informationen umfassen, die in den d-Blöcken dargestellt sind. Solche Variationen in dem Design der Darstellung sind möglich und sind lebensfähige Alternativen, können allerdings ein Verarbeitungs-Overhead, z. B. die Interpretation der Objekte, einführen.

[0054] Digitale Arbeiten werden in einer Verwahrungsstelle als Teil eines hierarchischen Datei-Systems gespeichert. Folder (auch bezeichnet als Directories und Sub-Directories) enthalten die digitalen Arbeiten eben-

so wie andere Folder. Digitale Arbeiten und Folder in einem Folder sind in einer alphabetischen Reihenfolge geordnet. Die digitalen Arbeiten werden geschrieben um wiederzugeben, wie die Dateien verwendet werden. Benutzungsrechte können an Folder angehängt werden, so dass der Folder selbst als eine digitale Arbeit behandelt wird. Ein Zugriff auf den Folder würde dann in derselben Art und Weise wie irgendeine andere digitale Arbeit gehandhabt werden. Wie in weiterem Detail nachfolgend beschrieben werden wird, werden die Inhalte des Folders deren eigenen Rechten unterworfen. Weiterhin können Datei-Management-Rechte an den Folder angehängt werden, die definieren, wie Folder-Inhalte gemanagt werden können.

ANHÄNGEN VON BENUTZUNGS-RECHTEN AN EINE DIGITALE ARBEIT

[0055] Es ist für die vorliegende Erfindung grundsätzlich, dass die Benutzungsrechte als Teil der digitalen Arbeit behandelt werden können. Wenn die digitale Arbeit verteilt wird, wird der Umfang der erteilten Benutzungsrechte derselbe verbleiben oder kann geringer gemacht werden. Zum Beispiel können, wenn eine digitale Arbeit von einem Dokumenten-Server zu einer Verwahrungsstelle übertragen wird, die Benutzungsrechte das Recht umfassen, eine Kopie für eine vorbestimmte Zeitperiode auszuleihen (bezeichnet als die Original-Rechte). Wenn die Verwahrungsstelle eine Kopie der digitalen Arbeit ausleiht, könnten die Benutzungsrechte in der Verleiher-Kopie (bezeichnet als der nächste Satz von Rechten) so eingestellt werden, um zu verhindern, dass irgendwelche weiteren Rechte die Kopie ausleihen. Die grundsätzliche Idee ist diejenige, dass man nicht mehr Rechte erteilen kann als man hat.

[0056] Das Anhängen von Benutzungsrechten an eine digitale Arbeit kann in einer Vielzahl von Arten und Weisen auftreten. Wenn die Benutzungsrechte für eine gesamte, digitale Arbeit dieselben sein werden, könnten sie angehängt werden, wenn die digitale Arbeit für ein Niederlegen in dem digitalen Arbeits-Server verarbeitet wird. In dem Fall einer digitalen Arbeit, die unterschiedliche Benutzungsrechte für die verschiedenen Komponenten besitzt, wird dies vorgenommen, wenn die digitale Arbeit erzeugt wird. Ein Autorisierungswerkzeug oder ein eine digitale Arbeit zusammenstellendes Werkzeug könnte verwendet werden, das für eine automatisierte Verarbeitung eines Anhängens der Benutzungsrechte dient. Wie nachfolgend beschrieben werden wird, kann, wenn eine digitale Arbeit kopiert wird, übertragen wird oder ausgeliehen wird, eine ”nächster Satz von Rechten” spezifiziert werden. Der ”nächste Satz von Rechten” wird an die digitale Arbeit angehängt werden, wenn sie transportiert wird.

Auflösen von in Konflikt tretenden Rechten

[0057] Da jeder Teil einer digitalen Arbeit seine eigenen Benutzungsrechte haben kann, werden dabei Fälle vorhanden sein, wo die Rechte eines ”enthaltenen Teils” unterschiedlich von deren Parent- oder Container-Teil sind. Als Folge müssen Konflikt-Regeln eingerichtet werden, um vorzugeben, wann und wie ein Recht ausgeübt werden kann. Die hierarchische Struktur einer digitalen Arbeit erleichtert die Durchsetzung solcher Regeln. Eine ”strikte” Regel würde wie folgt sein: ein Recht für einen Teil in einer digitalen Arbeit wird sanktioniert, falls und nur falls sie für den Teil sanktioniert ist, für Vorbesitzer (Ancestor) d-Blöcke, die den Teil enthalten, und für alle abfallenden d-Blöcke. Mit sanktioniert ist gemeint, dass (1) jeder der jeweiligen Teile das Recht haben muss und (2) irgendwelche Bedingungen zum Ausüben des Rechts erfüllt sind.

[0058] Es ist auch möglich, die vorliegende Erfindung unter Verwendung einer mehr nachsichtigen Regel auszuführen. In der mehr nachsichtigen Regel kann ein Zugriff auf den Teil zu den abfallenden Teilen freigegeben werden, die das Recht haben, wobei allerdings ein Zugriff zu den Nachkommen abgelehnt wird, die dies nicht haben.

[0059] Ein Beispiel eines Anwendens sowohl der strikten Regel als auch der nachsichtigen Regel wird unter Bezugnahme auf **Fig.** 11 dargestellt. Wie **Fig.** 11 zeigt, besitzt ein Root-d-Block **1101** Child-d-Blöcke **1102**–**1105**. In diesem Fall stellt ein Root-d-Block ein Magazin dar und jeder der Child-d-Blöcke **1102**–**1105** stellt Artikel in dem Magazin dar. Es wird angenommen, dass eine Anforderung vorgenommen wird, um die digitale Arbeit, dargestellt durch den Root-d-Block **1101**, zu DRUCKEN, wobei der strikten Regel gefolgt wird. Die Rechte für den Root-d-Block **1101** und die Child-d-Blöcke **1102**–**1105** werden dann geprüft. Der Root-d-Block **1101** und die Child-d-Blöcke **1102** und **1105** sind als DRUCK-Rechte erteilt worden. Der Child-d-Block **1103** hat keine DRUCK-Rechte erteilt und der Child-d-Block **1104** hat DRUCK-Rechte, konditioniert bei der Bezahlung einer Benutzungsgebühr, erteilt.

[0060] Unter der strikten Regel kann das DRUCK-Recht nicht ausgeübt werden, da der Child-d-Block nicht das DRUCK-Recht besitzt. Unter der nachsichtigen Regel würde das Ergebnis unterschiedlich sein. Die digitalen Arbeiten, dargestellt durch Child-d-Blöcke **1102** und **1105**, könnten gedruckt werden, und die digitale Arbeit,

dargestellt durch den d-Block **1104**, könnte so lange gedruckt werden, wie die Benutzungsgebühr bezahlt ist. Nur die digitale Arbeit, dargestellt durch den d-Block **1103**, könnte nicht gedruckt werden. Dasselbe Ergebnis würde unter der strikten Regel erreicht werden, wenn die Anforderungen zu jeder der individuellen, digitalen Arbeiten gerichtet werden.

[0061] Die vorliegende Erfindung unterstützt verschiedene Kombinationen, um einen Zugriff zuzulassen und nicht zuzulassen. Weiterhin erlaubt, wie nachfolgend beschrieben werden wird, die Benutzungsrechte-Grammatik dem Eigentümer einer digitalen Arbeit zu spezifizieren, ob Beschränkungen der Arbeit auferlegt werden müssen, und zwar durch einen Container-Teil. Die Art und Weise, in der digitale Arbeiten sanktioniert werden können, aufgrund von Benutzungsrechten Konflikten, würden ausführungs-spezifisch sein und würden von der Art der digitalen Arbeiten abhängen.

VERWAHRUNGSSTELLEN

[0062] In der Beschreibung der **Fig.** 2 wurde angezeigt, dass die Verwahrungsstellen in verschiedenen Formen vorkommen. Alle Verwahrungsstellen liefern einen Kernsatz von Serviceleistungen für die Übertragung von digitalen Arbeiten. Die Art und Weise, in der digitale Arbeiten ausgetauscht werden, ist die Basis für alle Transaktionen zwischen Verwahrungsstellen. Die verschiedenen Verwahrungsstellen-Typen unterscheiden sich in den letztendlichen Funktionen, die sie durchführen können. Verwahrungsstellen können Vorrichtungen selbst sein, oder sie können in andere Systeme eingeschlossen werden. Ein Beispiel ist die gestaltende Verwahrungsstelle **203** der **Fig.** 2.

[0063] Eine Verwahrungsstelle wird ihr zugeordnet einen Verwahrungsstellen-Identifizierer haben. Typischerweise würde der Verwahrungsstellen-Identifizierer eine eindeutige Zahl sein, die der Verwahrungsstelle zu dem Zeitpunkt einer Herstellung zugeordnet ist. Jede Verwahrungsstelle wird auch so klassifiziert werden, dass sie in einer bestimmten Sicherheitsklasse liegt. Bestimmte Kommunikationen und Transaktionen können in Bezug auf eine Verwahrungsstelle konditioniert werden, die sich in einer bestimmten Sicherheitsklasse befindet. Die verschiedenen Sicherheitsklassen werden in größerem Detail nachfolgend beschrieben.

[0064] Als eine Voraussetzung für einen Betrieb wird eine Verwahrungsstelle den Besitz eines Identifikations-Zertifikats erfordern. Identifikations-Zertifikate sind verschlüsselt, um eine Fälschung zu verhindern, und werden durch eine Master-Verwahrungsstelle ausgegeben. Eine Master-Verwahrungsstelle spielt die Rolle eines Autorisierungs-Agenten, um Verwahrungsstellen zu ermöglichen, digitale Arbeiten zu empfangen. Identifikations-Zertifikate müssen auf einer periodischen Basis aktualisiert werden. Identifikations-Zertifikate werden in größerem Detail nachfolgend unter Bezugnahme auf die Registrierungs-Transaktion beschrieben. Eine Verwahrungsstelle besitzt sowohl eine Hardware als auch eine funktionale Ausführungsform. Die funktionale Ausführungsform ist typischerweise eine Software, die auf der Hardware-Ausführungsform läuft. Alternativ kann die funktionale Ausführungsform in die Hardware-Ausführungsform eingebettet sein, wie beispielsweise in einem Application Specific Integrated Circuit (ASIC) Chip.

[0065] Die Hardware-Ausführungsform einer Verwahrungsstelle wird in einem sicheren Gehäuse eingeschlossen werden, das, falls es gefährdet ist, bewirken kann, dass die Verwahrungsstelle gesperrt wird. Die Basis-Komponenten der Hardware-Ausführungsform einer Verwahrungsstelle werden unter Bezugnahme auf **Fig.** 12 beschrieben. Wie **Fig.** 12 zeigt, ist eine Verwahrungsstelle aus einer Verarbeitungseinrichtung **1200**, einem Speichersystem **1207**, einem Takt **1205** und einer externen Schnittstelle **1206** aufgebaut. Die Verarbeitungseinrichtung **1200** ist aus einem Prozessorelement **1201** und einem Prozessorspeicher **1202** aufgebaut. Die Verarbeitungseinrichtung **1201** sieht eine Steuereinheit, eine Verwahrungsstellen-Transaktion- und Benutzungsrechte-Transaktions-Funktionen für die Verwahrungsstelle vor. Verschiedene Funktionen in dem Betrieb der Verwahrungsstelle, wie beispielsweise Entschlüsselung und/oder Dekompression von digitalen Arbeiten und Transaktions-Nachrichten, werden auch durch die Verarbeitungseinrichtung **1200** durchgeführt. Das Prozessorelement **1201** kann ein Mikroprozessor oder eine andere, geeignete Berechnungskomponente sein. Der Prozessorspeicher **1202** würde typischerweise aus Read Only Memories (ROM) und Random Access Memories (RAM) aufgebaut sein. Solche Speicher würden die Software-Instruktionen enthalten, verwendet durch das Prozessorelement **1201**, beim Durchführen der Funktionen der Verwahrungsstelle.

[0066] Das Speichersystem **1207** ist weiterhin aus einem Deskriptor-Speicher **1203** und einem Inhaltsspeicher **1204** aufgebaut. Der Beschreibungsbaum-Speicher **1203** wird den Beschreibungsbaum für die digitale Arbeit speichern und der Inhaltsspeicher wird den zugeordneten Inhalt speichern. Der Beschreibungsbaum-Speicher **1203** und der Inhaltsspeicher **1204** müssen weder von demselben Typ eines Speichermediums sein noch müssen sie notwendigerweise dieselbe physikalische Vorrichtung haben. So kann, zum Beispiel, der

Deskriptor-Speicher **1203** auf einem Festspeicher gespeichert sein (für ein schnelles Aufsuchen der Beschreibungsbaum-Informationen), während der Inhaltsspeicher **1204** ein Hochkapazitätsspeicher sein kann, wie beispielsweise eine optische Platte.

[0067] Der Takt **1205** wird dazu verwendet, verschiedene auf einer Zeit basierende Zustände bzw. Bedingungen für Benutzungsrechte zeitmäßig zu stempeln oder Benutzungsgebühren zu berechnen, die den digitalen Arbeiten zugeordnet sein können. Der Takt **1205** wird eine nicht unterbrechenbare Energieversorgung haben, z. B. eine Batterie, um die Integrität der Zeitstempel beizubehalten. Die externe Schnittstelleneinrichtung **1206** dient für die Signalverbindung zu anderen Verwahrungsstellen und zu einem Kredit-Server. Die externe Schnittstelleneinrichtung **1206** dient für den Austausch von Signalen über solche Standardschnittstellen, wie beispielsweise RS-232, oder Personal Computer Manufactures Card Industry Association (PCMCIA) Standards, oder FDDI. Die externe Schnittstelleneinrichtung **1206** kann auch eine Netzwerk-Verbindungsfähigkeit vorsehen.

[0068] Die funktionale Ausführungsform einer Verwahrungsstelle wird unter Bezugnahme auf **Fig.** 13 beschrieben. Wie die **Fig.** 13 zeigt, ist die funktionale Ausführungsform aus einem Betriebssystem **1301**, Kern-Verwahrungsstellen-Services **1302**, Benutzungs-Transaktions-Handhabungseinrichtungen **1303**, Verwahrungsstellenspezifischen Funktionen **1304** und eine Benutzerschnittstelle **1305** aufgebaut. Das Betriebssystem **1301** ist für die Verwahrungsstelle spezifisch und würde typischerweise von dem Typ eines Prozessors, der verwendet wird, abhängen. Das Betriebssystem **1301** würde auch die Basis-Servicedienste zum Steuern und schnittstellenmäßigen Verbinden zwischen den Basis-Komponenten der Verwahrungsstelle liefern.

[0069] Die Kern-Verwahrungsstellen-Servicedienste **1302** weisen einen Satz von Funktionen auf, die durch jede einzelne Verwahrungsstelle erforderlich sind. Die Kern-Verwahrungsstellen-Servicedienste **1302** umfassen die Sitzungs-Initiierungs-Transaktionen, die in größerem Detail nachfolgend definiert sind. Dieser Satz von Service-Diensten umfasst auch einen generischen Ticket-Agenten, der dazu verwendet wird, ein digitales Ticket zu ”stanzen”, und einen generischen Autorisierungs-Server zum Verarbeiten von Autorisierungs-Spezifikationen. Digitale Tickets und Autorisierungen sind spezifische Mechanismen zum Steuern der Verteilung und der Verwendung von digitalen Arbeiten und werden im weiteren Detail nachfolgend beschrieben. Es ist anzumerken, dass mit den Kern-Verwahrungsstellen-Servicediensten eine Vielzahl von Identifikations-Zertifikaten **1306** verbunden sind. Die Identifikations-Zertifikate **1306** sind erforderlich, um die Verwendung der Verwahrungsstelle freizugeben.

[0070] Die Verwendungs-Transaktions-Handhabungseinrichtungen **1303** weisen eine Funktionalität zum Verarbeiten von Zugriffsanforderungen auf digitale Arbeiten und zum Berechnen von Gebühren basierend auf einem Zugriff auf. Die Benutzungs-Transaktionen, die unterstützt werden, werden für jeden Verwahrungsstellen-Typ unterschiedlich. Zum Beispiel kann es notwendig sein, für dieselben Verwahrungsstellen, Zugriffsanforderungen für digitale Arbeiten zu handhaben.

[0071] Die Verwahrungsstellen-spezifische Funktionalität **1304** weist eine Funktionalität auf, die eindeutig für eine Verwahrungsstelle ist. Zum Beispiel besitzt die Master-Verwahrungsstelle eine spezielle Funktionalität zum Herausgeben von digitalen Zertifikaten und zum Beibehalten von Verschlüsselungs-Schlüsseln. Die Verwahrungsstellen-spezifische Funktionalität **1304** würde die Benutzer-Schnittstellen-Ausführung für die Verwahrungsstelle umfassen.

Verwahrungsstellen-Sicherheits-Klassen

[0072] Für einige digitale Arbeiten sind die Verluste, verursacht durch irgendeinen individuellen Fall eines nicht autorisierten Kopierens unwesentlich, und der ökonomische Hauptpunkt liegt in dem Sicherstellen eines passenden Zugriffs und eines in Rechnungstellens mit geringem Overhead. In solchen Fällen können einfache und kostengünstige in der Hand haltbare Verwahrungsstellen und auf einem Netzwerk basierende Arbeitsstationen geeignete Verwahrungsstellen sein, gerade obwohl die Maßnahmen und Garantien einer Sicherheit am moderatesten sind.

[0073] Auf der anderen Seite würden einige digitale Arbeiten, wie beispielsweise eine digitale Kopie einer Uraufführung eines Films oder einer Inhaberobligation oder eines Wertpapierzertifikats, von einem sehr hohen Wert sein, so dass es vernünftig ist, achtsame und angemessen sorgfältige Sicherheitsmaßnahmen einzusetzen, um sicherzustellen, dass sie nicht kopiert oder gefälscht werden. Eine Verwahrungsstelle, geeignet zum Halten einer solchen digitalen Arbeit, könnte sorgfältige Maßnahmen zum Sicherstellen einer physikalischen Integrität und zum Verifizieren einer Autorisierung vor einer Verwendung haben.

[0074] Durch Anordnen eines universellen Protokolls können alle Arten von Verwahrungsstellen miteinander im Prinzip kommunizieren. Allerdings werden es Urheber einiger Arbeiten wünschen, zu spezifizieren, dass deren Arbeiten nur zu Verwahrungsstellen übertragen werden, deren Sicherheitsniveau hoch genug ist. Aus diesem Grund besitzen Dokumenten-Verwahrungsstellen ein Rangsystem für Klassen und Sicherheitsniveaus. Die Sicherheitsklassen in der derzeit bevorzugten Ausführungsform sind in Tabelle 2 beschrieben.

Level	Beschreibung der Sicherheit
0	Offenes System. Dokumenten-Übertragung ist nicht verschlüsselt. Kein digitales Zertifikat ist zur Identifizierung erforderlich. Die Sicherheit des Systems hängt hauptsächlich von einer Benutzer-Ehrlichkeit ab, da nur eine geringe Kenntnis benötigt wird, um die Sicherheitsmaßnahmen zu umgehen. Die Verwahrungsstelle besitzt keine Vorsehungen, um zu verhindern, dass nicht autorisierte Programme laufen und auf Dateien zugreifen oder diese kopieren. Das System verhindert nicht die Verwendung eines entnehmbaren Speichers und verschlüsselt keine gespeicherten Dateien.
1	Minimale Sicherheit. Ähnlich der vorherigen Klasse, mit der Ausnahme, dass die gespeicherten Dateien minimal verschlüsselt sind, umfassend solche auf einem entnehmbaren Speicher.
2	Basis-Sicherheit. Ähnlich der vorherigen Klasse, mit der Ausnahme, dass spezielle Werkzeuge und Kenntnisse erforderlich sind, um das Programmieren, die Inhalte der Verwahrungsstelle oder den Zustand des Takts zu beeinflussen. Alle digitalen Kommunikationen sind verschlüsselt. Ein digitales Zertifikat ist als eine Identifikation vorgesehen. Eine Verschlüsselung auf einem mittleren Level wird verwendet. Eine Verwahrungsstellen-Identifikations-Nummer ist unfälschbar.
3	Allgemeine Sicherheit. Ähnlich der vorherigen Klasse, plus dem Erfordernis, dass spezielle Tools benötigt werden, um die physikalische Integrität der Verwahrungsstelle zu beeinflussen, und dass eine passende Verschlüsselung bei allen Übertragungen verwendet wird. Ein Passwort-Schutz ist erforderlich, um die lokale Benutzerschnittstelle zu verwenden. Das digitale Takt-System kann nicht ohne Autorisierung zurückgesetzt werden. Keine Arbeiten würden auf einem entnehmbaren Speicher gespeichert werden. Wenn Arbeiten als Programme ausgeführt werden, laufen sie in deren eigenem Adressen-Raum, und es wird ihnen kein direkter Zugriff zu irgendeinem Detailspeicher oder einem anderen Speicher, der einen System-Code oder Arbeiten enthält, gegeben. Sie können auf Arbeiten nur über das Übertragungs-Transaktions-Protokoll zugreifen.
4	Ähnlich der vorherigen Klasse mit der Ausnahme, dass eine Verschlüsselung unter hohem Level bei allen Kommunikationen verwendet wird. Sensoren werden verwendet, um Versuche bei physikalischen und elektronischen Fälschungen aufzuzeichnen. Nach einer solchen Fälschung wird die Verwahrungsstelle nicht andere Transaktionen durchführen, bis sie über eine solche Fälschung einem bezeichneten Server berichtet hat.
5	Ähnlich der vorherigen Klasse, mit der Ausnahme, dass dann, wenn die physikalischen oder digitalen Versuche bei einer Fälschung bestimmte, vorab eingestellte Schwellwerte übersteigen, die die physikalische Integrität der Verwahrungsstelle oder die Integrität von digitalen und kryptografischen Barrieren bedrohen, dann die Verwahrungsstelle nur Dokumenten-Beschreibungs-Aufzeichnungen einer Historie sichern wird, allerdings irgendwelche digitalen Identifizierer löschen oder zerstören wird, die missbraucht werden könnten, falls sie an eine gewissenlose Partei freigegeben werden. Dies modifiziert auch irgendwelche Zertifikate einer Authentizität, um anzuzeigen, dass das physikalische System beeinträchtigt worden ist. Dies löscht auch die Inhalte von bezeichneten Dokumenten.
6	Ähnlich der vorherigen Klasse mit der Ausnahme, dass die Verwahrungsstelle eine drahtlose Kommunikation versuchen wird, um über einen unberechtigten Eingriff zu berichten, und wird einen hörbaren Alarm einsetzen.
10	Dies würde einem sehr hohen Level einer Sicherheit entsprechen. Dieser Server würde konstante Kommunikationen mit Fernsicherheitssystemen beibehalten, indem er Transaktionen, Sensor-Lesungen und Versuche, die Sicherheit zu umgehen, berichten würde.

TABELLE 2

VERWAHRUNGSSTELLEN-SICHERHEITS-LEVEL

[0075] Die Charakterisierung der Sicherheits-Level, beschrieben in Tabelle 2, ist nicht dazu vorgesehen, dass sie festgelegt ist. Wichtiger ist die Idee, unterschiedliche Sicherheits-Level für unterschiedliche Verwahrungsstellen zu haben. Es ist vorgesehen, dass sich neue Sicherheitsklassen und Erfordernisse entsprechend den sozialen Situationen und den Änderungen in der Technologie entwickeln werden.

Verwahrungstellen-Benutzerschnittstelle

[0076] Eine Benutzerschnittstelle ist breit als Mechanismus definiert, mit dem ein Benutzer mit einer Verwahrungsstelle wechselwirken wird, um Transaktionen aufzurufen, um einen Zugriff zu einer digitalen Arbeit zu erhalten, oder Benutzungsrechte ausüben wird. Wie vorstehend beschrieben ist, kann eine Verwahrungsstelle in verschiedenen Formen ausgeführt werden. Die Benutzerschnittstelle für eine Verwahrungsstelle wird sich unterscheiden in Abhängigkeit von der bestimmten Ausführungsform. Die Benutzerschnittstelle kann eine grafische Benutzerschnittstelle sein, die Icons bzw. Bildzeichen hat, die die digitalen und die verschiedenen Transaktionen, die durchgeführt werden können, darstellen. Die Benutzerschnittstelle kann ein erzeugter Dialog sein, in dem ein Benutzer nach Informationen gefragt wird.

[0077] Die Benutzerschnittstelle selbst muss nicht ein Teil der Verwahrungsstelle sein. Da eine Verwahrungsstelle in eine bestimmte andere Vorrichtung eingebettet sein kann, kann die Benutzerschnittstelle nur ein Teil der Vorrichtung sein, in der die Verwahrungsstelle eingebettet ist. Zum Beispiel könnte die Verwahrungsstelle in eine ”Karte” eingebettet sein, die in einen verfügbaren Schlitz in einem Computersystem eingesetzt wird. Die Benutzerschnittstelle kann eine Kombination einer Anzeige, eines Tastenfelds, einer Cursor-Steuervorrichtung und einer Software, die auf dem Computersystem läuft, sein.

[0078] Minimal muss die Benutzerschnittstelle einem Benutzer ermöglichen, Informationen einzugeben, wie beispielsweise Zugriffsanforderungen und alphanummerische Daten, und muss ein Feedback liefern, wie über einen Transaktions-Status. Die Benutzerschnittstelle wird dann bewirken, dass die Verwahrungsstelle die geeigneten Transaktionen initiiert, um die Anforderung zu bedienen. Andere Facetten einer bestimmten Benutzerschnittstelle werden von der Funktionalität abhängen, die eine Verwahrungsstelle liefern wird.

KREDIT-SERVER

[0079] Bei der vorliegenden Erfindung können Gebühren der Ausübung eines Rechts zugeordnet sein. Das Erfordernis zum Bezahlen von Gebühren ist in jeder Version eines Benutzungsrechts in der Benutzungsrechte-Sprache beschrieben. Die Aufzeichnung und das Berichten über solche Gebühren wird durch den Kredit-Server durchgeführt. Eine der Fähigkeiten, die eine Zuordnung von Gebühren zu Rechten ermöglicht, ist die Möglichkeit, einen breiten Bereich von Berechnungsmodellen zu unterstützen. Das einfachste Modell, das durch herkömmliche Software verwendet ist, ist dasjenige, dass dort eine einzelne Gebühr zum Zeitpunkt eines Erwerbs vorhanden ist, wonach der Erwerber das unbegrenzte Recht erhält, die Arbeit so oft und so lange zu verwenden, wie er dies wünscht. Alternative Modelle umfassen eine dosierte Verwendung und variable Gebühren. Eine einzelne Arbeit kann unterschiedliche Gebühren für unterschiedliche Verwendungen haben. Zum Beispiel könnte ein Betrachten einer Fotografie auf einer Anzeige unterschiedliche Gebühren haben, als eine Hardcopy davon zu erstellen oder diese in eine neu erzeugte Arbeit einzuschließen. Ein Schlüssel zu diesen alternativen Berechnungsmodellen ist derjenige, eine Einrichtung mit niedrigem Overhead zum Einrichten von Gebühren und zum Berechnen eines Kredites über diese Transaktionen zu haben.

[0080] Ein Kredit-Server ist ein Berechnungssystem, das zuverlässig autorisiert und diese Transaktionen aufzeichnet, so dass die Gebühren in Rechnung gestellt und gezahlt werden können. Der Kredit-Server berichtet über Gebühren an eine Verrechnungsstelle. Die Verrechnungsstelle managt die finanziellen Transaktionen, wie sie auftreten. Als Folge können Rechnungen erzeugt werden und Konten können abgeglichen werden. Bevorzugt würde der Kredit-Server die Gebühren-Transaktionen speichern und periodisch über ein Netzwerk mit der Verrechnungsstelle für einen Abgleich kommunizieren. In einer solchen Ausführungsform würden Kommunikationen mit der Verrechnungsstelle aus Integritäts- und Sicherheitsgründen verschlüsselt werden. In einer anderen Ausführungsform arbeitet der Kredit-Server als eine ”Lastschrift-Karte” (Debit-Card), wo Transaktionen in einer ”Realzeit” gegenüber einem Benutzerkonto auftreten.

[0081] Ein Kredit-Server ist aus einem Speicher, einer Verarbeitungseinrichtung, einem Takt und einer Schnittstelleneinrichtung zum Verbinden mit einer Verwahrungsstelle und einer Finanzinstitution (z. B. einem Modem) aufgebaut. Der Kredit-Server muss eine Sicherheits- und Autentifikations-Funktionalität haben. Diese

Elemente sind im Wesentlichen dieselben Elemente wie solche einer Verwahrungsstelle. Demzufolge kann eine einzelne Vorrichtung sowohl eine Verwahrungsstelle als auch ein Kredit-Server sein, vorausgesetzt, dass sie die geeigneten Verarbeitungselemente zum Ausführen der entsprechenden Funktionen und Protokolle besitzt. Typischerweise würde allerdings ein Kredit-Server ein mit Karte arbeitendes System, im Besitz des Inhabers des Kredits, sein. Der Kredit-Server ist mit einer Verwahrungsstelle verbunden und würde über finanzielle Transaktionen wechselwirken, wie dies nachfolgend beschrieben ist. Interaktion mit einer finanziellen Institution können über Protokolle auftreten, eingerichtet durch die Finanz-Institutionen selbst.

[0082] In der derzeit bevorzugten Ausführungsform berichten Kredit-Server, zugeordnet sowohl dem Server als auch der Verwahrungsstelle, über die finanzielle Transaktion an die Zahlstelle. Zum Beispiel werden, wenn eine digitale Arbeit durch eine Verwahrungsstelle zu einer anderen gegen eine Gebühr kopiert wird, Kredit-Server, verbunden mit jeder der Verwahrungsstellen, über die Transaktionen an die Zahlstelle berichten. Dies ist dahingehend erwünscht, dass dies sicherstellt, dass eine Transaktion in dem Fall eines bestimmten Unterbrechens in der Kommunikation zwischen einem Kredit-Server und der Zahlstelle berechnet wird. Allerdings können einige Ausführungen nur einen einzelnen Kredit-Server einsetzen, der über die Transaktion berichtet, um die Transaktions-Verarbeitung unter dem Risiko, dass einige Transaktionen verloren gehen, zu minimieren.

BENUTZUNGSRECHTE-SPRACHE

[0083] Die vorliegende Erfindung verwendet Angaben bzw. Statements in einer ”Benutzungsrechte-Sprache” unter einem hohen Level, um Rechte zu definieren, die digitalen Arbeiten und deren Teilen zugeordnet sind. Benutzungsrecht-Angaben werden durch Verwahrungsstellen interpretiert und werden dazu verwendet, zu bestimmen, welche Transaktionen erfolgreich für eine digitale Arbeit ausgeführt werden können, und auch um Parameter für diese Transaktionen zu bestimmen. Zum Beispiel bestimmen Sätze in der Sprache, ob eine digitale Arbeit kopiert werden kann, wann und wie sie verwendet werden kann und welche Gebühren (falls welche vorhanden sind) für diese Verwendung berechnet werden sollen. Wenn einmal Benutzungsrecht-Angaben erzeugt sind, werden sie in eine geeignete Form für ein Zugreifen während der Verarbeitung von Transaktionen codiert.

[0084] Ein Definieren von Benutzungsrechten im Hinblick auf eine Sprache in Kombination mit der hierarchischen Darstellung einer digitalen Arbeit ermöglicht die Unterstützung einer breiten Vielfalt von Verteilungs- und Gebührenschemata. Ein Beispiel ist die Fähigkeit, mehrere Versionen, eines Rechts an eine Arbeit anzuhängen. So kann ein Urheber ein DRUCK-Recht anhängen, um 5 Kopien für $10,00 herzustellen, und ein DRUCK-Recht, um unbegrenzte Kopien für Dollar $100,00 herzustellen. Ein Erwerber kann dann auswählen, welche Option am besten seine Bedürfnisse anpasst. Ein anderes Beispiel ist dasjenige, dass Rechte und Gebühren additiv sind. So werden in dem Fall einer Composit-Arbeit die Rechte und Gebühren jeder der Komponenten-Arbeiten dazu verwendet, die Rechte und Gebühren für die Arbeit als Ganzes zu bestimmen.

[0085] Die Basis-Inhalte eines Rechts sind in **Fig.** 14 dargestellt. Wie **Fig.** 14 zeigt, besitzt ein Recht **1450** eine transaktionsmäßige Komponente **1451** und eine Spezifikations-Komponente **1452**. Ein Recht **1450** besitzt ein Label bzw. Etikett (z. B. KOPIE oder DRUCK), das die Verwendungs- oder Verteilungs-Privilegien anzeigt, die durch das Recht verkörpert sind. Die Transaktions-Komponente **1451** entspricht einer bestimmten Art und Weise, in der eine digitale Arbeit verwendet oder verteilt werden kann. Die transaktionsmäßige Komponente **1451** ist typischerweise in Softwareinstruktionen in einer Verwahrungsstelle ausgeführt, die die Verwendungs- oder Verteilungs-Privilegien für das Recht ausführt. Die Spezifikations-Komponenten **1452** werden dazu verwendet, Bedingungen zu spezifizieren, die erfüllt werden müssen, bevor das Recht ausgeübt wird, oder um verschiedene zu einer Transaktion in Bezug gesetzte Parameter zu bezeichnen. In der derzeit bevorzugten Ausführungsform umfassen diese Spezifikationen eine Kopie-Zählung **1453**, Gebühren und Prämien **1454**, Zeit **1455**, Zugriff und Sicherheit **1456** und Steuerung **1457**. Jede dieser Spezifikationen wird in größerem Detail nachfolgend unter Bezugnahme auf die Sprach-Grammatik-Elemente beschrieben.

[0086] Die Benutzungsrechte-Sprache ist auf der Grammatik basierend, die nachfolgend beschrieben ist. Eine Grammatik ist eine herkömmliche Einrichtung, um eine gültige Sequenz von Symbolen für eine Sprache zu definieren. Beim Beschreiben der Grammatik wird die Notation ”[a|b|c]” verwendet, um bestimmte Auswahlen unter Alternativen anzuzeigen. In diesem Beispiel kann ein Satz entweder ein ”a”, ein ”b” oder ein ”c” haben. Er muss exakt eines davon umfassen. Die Klammern {} werden dazu verwendet, optionale Elemente bzw. Items anzuzeigen. Es ist anzumerken, dass Klammern (Brackets), Striche (Bars) und Klammern (Braces) dazu verwendet werden, die Sprache von Benutzungsrechte-Sätzen zu beschreiben, allerdings erscheinen sie nicht in tatsächlichen Sätzen in der Sprache.

[0087] Im Gegensatz dazu sind Gedankenstriche Teil der Benutzungsrechte-Sprache. Gedankenstriche bzw. Parenthesen werden dazu verwendet, Elemente zusammen in Listen zu gruppieren. Die Bezeichnung (x*) wird dazu verwendet, eine Variabel-Längen-Liste anzuzeigen, das bedeutet eine Liste, die ein oder mehrere Elemente des Typs x enthält. Die Bezeichnung (x*) wird dazu verwendet, eine variable Zahl von Listen, die x enthalten, anzuzeigen.

[0088] Schlüsselworte in der Grammatik sind Worte, gefolgt durch Doppelpunkte. Schlüsselworte sind ein gemeinsamer oder sehr spezieller Fall in der Sprache. Sie werden oftmals dazu verwendet, einen einzelnen Wert, typischerweise einen Identifizierer, anzuzeigen. In vielen Fällen sind das Schlüsselwort und der Parameter völlig optional. Wenn ein Schlüsselwort angegeben ist, nimmt es oftmals einen einzelnen Identifizierer als seinen Wert. In einigen Fällen nimmt das Schlüsselwort eine Liste von Identifizierern.

[0089] In der Benutzungsrechte-Sprache wird eine Zeit in einer Darstellung Stunden:Minuten:Sekunden (oder hh:mm:ss) spezifiziert. Zeitzonen-Indikatoren, z. B. PDT für Pacific Daylight Time, können auch spezifiziert werden. Ein Datum wird als Jahr/Monat/Tag (oder YYYY/MMM/DD) dargestellt. Es ist anzumerken, dass diese Zeit- und Datum-Darstellungen Momente in der Zeit oder in Einheiten der Zeit spezifizieren können. Geld-Einheiten sind in Angaben von Dollars spezifiziert.

[0090] Schließlich müssen, in der Benutzungsrechte-Sprache, verschiedene ”Dinge” miteinander wechselwirken. Zum Beispiel kann ein Fall eines Benutzungsrechts ein Bankkonto, ein digitales Ticket, usw., spezifizieren. Solche Dinge müssen identifiziert werden und werden hier unter Verwendung des Zusatzes”-ID” spezifiziert. Die Benutzungsrechte-Grammatik wird in ihrer Gesamtheit in **Fig.** 15 aufgelistet und ist nachfolgend beschrieben.

[0091] Ein Grammatik-Element **1501** ”Digital Work Rights:=(Rights*)” definiert die digitalen Arbeitsrechte als einen Satz von Rechten. Der Satz von Rechten, angehängt an eine digitale Arbeit, definiert, wie die digitale Arbeit übertragen, verwendet, durchgeführt oder angezeigt werden kann. Ein Satz von Rechten wird sich an die gesamte, digitale Arbeit, und, in dem Fall einer zusammengesetzten, digitalen Arbeit, jede der Komponenten der digitalen Arbeit anhängen. Die Benutzungsrechte von Komponenten einer digitalen Arbeit können unterschiedlich sein.

[0092] Grammatik-Element **1502** ”Right : = (Right-Code {Copy-Count} {Control-Spec} {Time-Spec} {Access-Spec} {Fee-Spec})” zählt den Inhalt eines Rechts auf. Jedes Benutzungsrecht muss einen Rechte-Code spezifizieren. Jedes Recht kann auch optional Bedingungen spezifizieren, die erfüllt werden müssen, bevor das Recht ausgeübt werden kann. Diese Bedingungen sind Kopie-Zählungen, Steuerung bzw. Kontrolle, Zeit, Zugriff und Gebührenbedingungen. In der derzeit bevorzugten Ausführungsform gilt, für die optionalen Elemente, die folgende Voreinstellungs-Anwendung: Kopie-Zählung entspricht 1, kein Zeit-Limit in Bezug auf die Verwendung des Rechts, keine Zugriffs-Tests oder ein Sicherheits-Level, erforderlich dazu, das Recht zu benutzen, und keine Gebühren sind erforderlich. Diese Bedingungen werden jeweils in größerem Detail nachfolgend geschrieben werden.

[0093] Es ist wichtig anzumerken, dass eine digitale Arbeit mehrere Versionen eines Rechts haben kann, wobei jede denselben Rechte-Code besitzt. Die Mehrfach-Version würde alternative Bedingungen und Gebühren für ein Zugreifen auf die digitale Arbeit liefern.

[0094] Grammatik-Element **1503** ”Right-Code : = Render-Code | Transport-Code | File-Management-Code | Derivative-Works-Code Configuration-Code” unterscheidet jedes der spezifischen Rechte zu einem bestimmten Rechte-Typ (obwohl jedes Recht durch bestimmte Rechte-Code identifiziert ist). Auf diese Art und Weise liefert die Grammatik einen Katalog von möglichen Rechten, die Teilen von digitalen Arbeiten zugeordnet werden können. Nachfolgend werden Rechte in Kategorien unterteilt, um die Beschreibung davon zu vereinfachen.

[0095] Grammatik-Element **1504** ”Render-Code : = [Plag : {Player:Player-ID} | Print: {Printer:Printer-ID}]” listet eine Kategorie von Rechten auf, die alle das Erstellen von kurzlebigen, Übergangs- oder nicht digitalen Kopien der digitalen Arbeit einschließen. Nach der Verwendung werden die Kopien gelöscht.

- Play — Ein Verfahren zum Gestalten oder Durchführen einer digitalen Arbeit auf einem bestimmten Prozessor. Dies umfasst solche Dinge, wie beispielsweise Abspielen von digitalen Filmen, Abspielen einer digitalen Musik, Abspielen eines Videospiels, Laufenlassen eines Computerprogramms oder Anzeigen eines Dokuments auf einer Anzeige.
- Print — Gestalten der Arbeit zu einem Medium, das nicht weiter durch Benutzungsrechte geschützt ist, wie beispielsweise Drucken auf Papier.

[0096] Grammatik-Element **1505** "Transport-Code : = [Copy | Transfer | Loan {Remaining-Rights:Next-Set-of-Rights}]{(Next-Copy-Rights: Next-Set of Rights)}" listet eine Kategorie von Rechten auf, umfassend das Erstellen von dauerhaften, verwendbaren Kopien der digitalen Arbeiten an anderen Verwahrungsstellen. Die optionale Next-Copy-Rights bestimmen die Rechte in Bezug auf die Arbeit, nachdem sie transportiert ist. Falls dies nicht spezifiziert ist, dann werden die Rechte auf der transportierten Kopie dieselben wie auf dem Original. Die optionalen Remaining-Rights spezifizieren die Rechte, die mit einer digitalen Arbeit verbleiben, wenn sie ausgeliehen ist. Falls dies nicht spezifiziert ist, dann ist die Voreinstellung diejenige, dass keine Rechte ausgeübt werden können, wenn ausgeliehen wird.

- Copy — Erstelle eine neue Kopie einer Arbeit
- Transfer — Bewegen einer Arbeit von einer Verwahrungsstelle zu einer anderen.
- Loan — Temporäres Verleihen einer Kopie zu einer anderen Verwahrungsstelle für eine spezifizierte Zeitperiode.

[0097] Grammatik-Element **1506** "File-Management-Code : = Backup {Back-Up-Copy-Rights: Next-Set of Rights}| Restore | Delete | Folder | Directory {Name: Hide-Local | Hide-Remote} {Parts:Hide-Local | Hide-Remote}" listet eine Kategorie von Rechten auf, die Operationen für ein Datei-Management einsetzt, wie beispielsweise das Erstellen von Sicherungskopien, um den Kopie-Besitzer gegenüber einem katastrophalen Ausrüstungsausfall zu schützen.

[0098] Viele Software-Lizenzen und auch das Copyright-Gesetz geben einem Kopie-Besitzer das Recht, Sicherungs-Kopien vorzunehmen, um sich gegenüber eines Katastrophen-Ausfalls einer Ausrüstung zu schützen. Allerdings ist das Erstellen von nicht kontrollierten Sicherungskopien nicht im Einklang mit der Fähigkeit eine Benutzung zu kontrollieren, da eine nicht kontrollierte Sicherungskopie verwahrt werden kann und dann wieder erstellt werden kann, nachdem die autorisierte Kopie verkauft wurde.

[0099] Die Datei-Management-Rechte ermöglichen, Sicherungskopien in einer Art und Weise herzustellen und wieder zu erstellen, die Benutzungsrechte respektiert, was den Erfordernissen sowohl des Kopie-Besitzers als auch des Gebers der Rechte und des Besitzers der Einkünfte Rechnung trägt. Sicherungskopien von Arbeitsbeschreibungen (umfassend Benutzungsrechte und Gebührendaten) können unter einem geeigneten Protokoll und einer Kontrolle von Benutzungsrechten zu anderen Dokumenten-Verwahrungsstellen einer ausreichend hohen Sicherheit geschickt werden. Weiterhin lassen Rechte eine Organisation von digitalen Arbeiten zu Foldern zu, wenn sie selbst als digitale Arbeiten behandelt werden, und diese Inhalte können gegenüber einer Partei "verdeckt werden", die danach sucht, die Inhalte einer Verwahrungsstelle zu bestimmen.

- Backup — Eine Sicherungskopie einer digitalen Arbeit als Schutz gegen einen Ausfall eines Mediums zu erstellen.
- Restore — Eine Sicherungskopie einer digitalen Arbeit wieder zu erzeugen.
- Delete — Eine Kopie einer digitalen Arbeit zu löschen oder zu entfernen.
- Folder — Folder zu erzeugen und zu benennen und Dateien und Folder zwischen Foldern zu bewegen.
- Directory — Einen Folder oder seine Inhalte zu treffen.

[0100] Grammatik-Element **1507 "**Derivative-Works-Code: [Extraxt | Embed | Edit {Process: Process-ID}] {Next-Copy-Rights : Next-Set-of Rights}" listet eine Kategorie von Rechten auf, umfassend die Verwendung einer digitalen Arbeit, um neue Arbeiten zu erzeugen.

- Extract — Einen Teil einer Arbeit zu entfernen, zu Zwecken einer Erzeugung einer neuen Arbeit.
- Embed — Eine Arbeit in eine existierende Arbeit einzuschließen.
- Edit — Eine digitale Arbeit durch Kopieren, Auswählen und Modifizieren von Bereichen einer existierenden, digitalen Arbeit zu ändern.

[0101] Grammatik-Element **1508** ”Configuration-Code: = Install | Uninstall” listet eine Kategorie von Rechten zum Installieren und zum Entfernen von Software an einer Verwahrungsstelle (typischerweise eine gestaltende Verwahrungsstelle) auf. Dies würde typischerweise für die Installation eines neuen Typs eines Abspielgeräts innerhalb der gestaltenden Verwahrungsstelle auftreten.

- Install: Eine neue Software auf einer Verwahrungsstelle installieren
- Uninstall: Eine existierende Software von einer Verwahrungsstelle entfernen.

[0102] Grammatik-Element **1509** ”Next-Set-of-Rights: = {(Add: Set-Of-Rights)} {(Delete: Set-Of-Rights)} {(Replace: Set-Of-Rights)} {(Keep: Set-Of-Rights)}” definiert, wie Rechte nach vorne für eine Kopie einer digitalen Arbeit ausgeführt werden. Falls die Next-Copy-Rights nicht spezifiziert sind, sind die Rechte für die nächste Kopie dieselben wie solche der momentanen Kopie. Ansonsten kann der Satz von Rechten für die nächste Kopie spezifiziert werden. Versionen von Rechten nach Add: werden zu dem momentanen Satz von Rechten hinzufügt. Rechte nach Delete: werden von dem momentanen Satz von Rechten gelöscht. Wenn nur Rechte-Code nach Delete aufgelistet sind: dann werden alle Versionen von Rechten mit solchen Coden gelöscht. Versionen von Rechten nach Replace: subsummiere alle Versionen von Rechten desselben Typs in dem momentanen Satz von Rechten.

[0103] Falls Remaining-Rights nicht spezifiziert ist, dann sind dabei keine Rechte für das Original vorhanden, nachdem alle Loan-Kopien ausgeliehen sind. Falls Remaining-Rights spezifiziert ist, dann das Keep: Token kann verwendet werden, um den Ausdruck zu vereinfachen, welche Rechte dahinter gehalten werden. Eine Liste von Rechte-Coden, die einer Keep-Einrichtung (Beibehaltungs-Einrichtung) folgen, die alle von den Versionen dieser aufgelisteten Rechte sind, werden in der verbleibenden Kopie beibehalten. Diese Spezifikation kann durch ein darauffolgendes Delete: or Replace: specifications überschrieben werden.

Kopie-Zählungs-Spezifikation

[0104] Für verschiedene Transaktionen kann es erwünscht sein, dieselbe Grenze wie die Anzahl von ”Kopien” der Arbeit vorzusehen, die simultan mit dem Recht ausgeübt werden kann. Zum Beispiel kann es erwünscht sein, die Zahl von Kopien einer digitalen Arbeit, die zu einem Zeitpunkt ausgeliehen oder zu einem Zeitpunkt betrachtet werden kann, zu begrenzen.

[0105] Grammatik-Element **1510** ”Copy-Count: = (Copies: positive-integer | 0 | unlimited)” liefert eine Bedingung, die die Zahl von ”Kopien” einer Arbeit, die dem Recht unterworfen ist, definiert. Eine Kopie-Zählung kann 0, eine festgelegte Zahl oder unbegrenzt sein. Die Kopie-Zählung ist jedem Recht zugeordnet, im Gegensatz dazu, dass sie nur eine einzelne Kopie-Zählung für die digitale Arbeit ist. Das Kopie-Count für ein Recht wird zu jedem Zeitpunkt erniedrigt, zu dem ein Recht ausgeübt wird. Wenn das Copy-Count Null gleicht, kann das Recht nicht länger ausgeübt werden. Falls das Copy-Count nicht spezifiziert ist, ist die Voreinstellung eins.

Steuer-Spezifikation

[0106] Rechte und Gebühren hängen allgemein von Rechten, erteilt durch den Urheber, ebenso wie von weiteren Beschränkungen, die späteren Verteilern auferlegt sind, ab. Steuer-Spezifikationen befassen sich mit Interaktionen zwischen den Urhebern und deren Verteilern, die das Auferlegen von weiteren Beschränkungen und Gebühren leiten. Zum Beispiel kann es ein Verteiler einer digitalen Arbeit nicht wünschen, dass ein Endverbraucher einer digitalen Arbeit Gebühren oder einen anderen Profit durch kommerzielles Ausbeuten der erworbenen, digitalen Arbeit hinzufügt.

[0107] Grammatik-Element **1511** ”Control-Spec: = (Control: {Restrictable | Unrestrictable} {Unchargeable | Chargeable})” liefert einen Zustand, den Effekt von Benutzungsrechten und Gebühren von Parents bei der Ausübung des Rechts zu spezifizieren. Eine digitale Arbeit ist einschränkbar, falls d-Blöcke mit einem höheren Level weitere Beschränkungen (Zeitspezifikationen und Zugriffsspezifikationen) auf das Recht auferlegen können. Dies ist uneinschränkbar, falls keine weiteren Beschränkungen auferlegt werden können. Die Vor-

einstellung-Einstellung ist einschränkbar. Ein Recht ist nicht berechenbar, falls keine weiteren Gebühren der Verwendung des Rechts auferlegt werden können. Es ist berechenbar, falls mehr Gebühren auferlegt werden können. Die Voreinstellung ist berechenbar.

Zeit-Spezifikation

[0108] Es ist oftmals erwünscht, ein Start-Datum zuzuordnen oder eine bestimmte Dauer zu spezifizieren, beispielsweise so, wann ein Recht ausgeübt werden kann. Grammatik-Element **1512** "Time-Spec: = ({Fixed-Interval | Sliding-Interval | Meter-Time} Until: Expiration-Date)" dient zur Spezifikation von Zeitzuständen bei der Ausübung eines Rechts. Rechte können für eine spezifizierte Zeit erteilt werden. Unterschiedliche Arten von Zeitspezifikationen sind für unterschiedliche Arten von Rechten geeignet. Einige Rechte können während einer festgelegten und vorbestimmten Dauer ausgeübt werden. Einige Rechte können für ein Intervall ausgeübt werden, das zum ersten Mal startet, zu dem Zeitpunkt, zu dem das Recht durch eine bestimmte Transaktion aufgerufen ist. Einige Rechte können entsprechend einer bestimmten Art einer bestimmten Zeit ausgeübt oder berechnet werden, die in separate Intervalle aufgeteilt ist. Zum Beispiel könnte ein Recht, ein Bild für eine Stunde zu betrachten, in sechs Betrachtungen von jeweils zehn Minuten oder in vier Betrachtungen von jeweils fünfzehn Minuten oder in drei Betrachtungen von jeweils zwanzig Minuten aufgeteilt werden.

[0109] Die Ausdrücke "Zeit" und "Datum" werden synonym dazu verwendet, einen zeitlichen Augenblick zu bezeichnen. Dabei sind drei Arten von Zeitspezifikationen vorhanden. Jede Spezifikation stellt eine bestimmte Beschränkung in Bezug auf die Zeiten dar, während der das Benutzungsrecht gilt. Das Expiration-Date spezifiziert den Augenblick, zu dem das Benutzungsrecht endet. Zum Beispiel endet, falls das Expiration-Date "1. Januar 1995" ist, dann das Recht zu dem ersten Augenblick von 1995. Falls das Expiration-Date als *forever* spezifiziert ist, dann werden die Rechte als fortführend ohne Ende interpretiert. Falls nur ein Ablaufdatum gegeben ist, dann kann das Recht so oft ausgeübt werden, wie dies erwünscht ist, bis zu dem Ablaufdatum.

[0110] Grammatik-Element **1513** "Fixed-Interval: = From: Start-Time" wird dazu verwendet, ein vorbestimmtes Intervall zu definieren, das von der Start-Zeit bis zu dem Ablaufdatum läuft.

[0111] Grammatik-Element **1514** "Sliding-Interval: = Interval: Use-Duration" wird dazu verwendet, eine Zwischen-(oder "offene")-Start-Zeit zu definieren. Sie setzt Grenzen in Bezug auf die fortlaufende Zeitperiode, über die die Inhalte zugänglich sind. Die Periode beginnt mit dem ersten Zugriff und endet, nachdem die Dauer vorbei ist oder das Ablaufdatum erreicht ist, was auch immer zuerst auftritt. Zum Beispiel würde, wenn das Recht 10 Stunden eines fortlaufenden Zugriffs erteilt, die Benutzungsdauer beginnen, als der erste Zugriff vorgenommen wurde, und endet 10 Stunden später.

[0112] Grammatik-Element **1515** "Meter-Time: = Time-Remaining: Remaining-Use" wird dazu verwendet, eine "Mess-Zeit" ("meter time") zu definieren, das bedeutet eine Messung der Zeit, für die das Recht tatsächlich ausgeübt wird. Sie unterscheidet sich von der Sliding-Interval (Gleit-Intervall) Spezifikation, dahingehend, dass die Zeit, für die die digitale Arbeit in Benutzung ist, nicht kontinuierlich sein muss. Zum Beispiel könnten, falls die Rechte drei Tage eines Zugriffs garantieren, diese Tage über einen Monat verteilt werden. Mit dieser Spezifikation können die Rechte ausgeübt werden, bis die Mess-Zeit verbraucht ist oder das Ablaufdatum erreicht ist, was auch immer zuerst auftritt.
Remaining-Use: = Time-Unit
Start-Time: = Time-Unit
Use-Duration: = Time-Unit

[0113] Alle Zeitspezifikationen umfassen Zeit-Einheit-(Time-Unit)-Spezifikationen in deren letztendlichem Fall.

Sicherheits-Klasse und Autorisierungs-Spezifikation

[0114] Die vorliegende Erfindung sieht verschiedene Sicherheits-Mechanismen vor, um sie in ein Verteilungs- oder Benutzungsschema einzufügen. Grammatik-Element **1516** "Access-Spec: = ({SC: Security-Class} {Authorization: Authorization-ID*} {Other-Authorization: Authorization-ID*} {Ticket: Ticket-ID})" liefert eine Einrichtung, um einen Zugriff und eine Übertragung zu beschränken. Zugriffsspezifikationen können eine erforderliche Sicherheits-Klasse für eine Verwahrungsstelle spezifizieren, um ein Recht oder einen erforderlichen Autorisierungs-Test, der erfüllt werden muß, auszuüben.

[0115] Das Schlüsselwort ”SC:” wird dazu verwendet, einen minimalen Sicherheits-Level für die Verwahrungsstellen, die bei dem Zugriff betroffen sind, zu spezifizieren. Falls ”SC:” nicht spezifiziert ist, ist der niedrigste Sicherheits-Level akzeptierbar.

[0116] Das optionale ”Authorization:” Schlüsselwort wird dazu verwendet, erforderliche Autorisierungen an derselben Verwahrungsstelle wie die Arbeit zu spezifizieren. Das optionale ”Other-Authorization:” Schlüsselwort wird dazu verwendet, Autorisierungen an der anderen Verwahrungsstelle in der Transaktion zu spezifizieren.

[0117] Das optionale ”Ticket:” Schlüsselwort spezifiziert die Identität eines Tickets, erforderlich für die Transaktion. Eine Transaktion, die digitale Tickets einsetzt, muß einen geeigneten Digital-Ticket-Agenten lokalisieren, der das Ticket ”stanzen” oder in anderer Weise als gültig erklären kann, bevor die Transaktion fortführen kann. Ticket wird in größerem Detail nachfolgend beschrieben.

[0118] In einer Transaktion, die eine Verwahrungsstelle und einen Dokumenten-Server einsetzt, können bestimmte Benutzungsrechte erfordern, dass die Verwahrungsstelle eine bestimmte Autorisierung besitzt, dass der Server eine bestimmte Autorisierung besitzt oder dass beide Verwahrungsstellen (möglicherweise unterschiedliche) Autorisierungen besitzen. Autorisierungen selbst sind digitale Arbeiten (nachfolgend bezeichnet als ein Autorisierungs-Objekt), die zwischen Verwahrungsstellen in derselben Art und Weise wie andere digitale Arbeiten bewegt werden können. Deren Kopieren und Übertragen wird denselben Rechten und Gebühren wie andere, digitale Arbeiten, unterworfen. Eine Verwahrungsstelle ist eine solche, die eine Autorisierung hat, falls dieses Autorisierungs-Objekt innerhalb der Verwahrungsstelle enthalten ist.

[0119] In einigen Fällen kann eine Autorisierung von einer Quelle, einer anderen als der Dokumenten-Server und die Verwahrungsstelle, erforderlich sein. Ein Autorisierungs-Objekt, auf das durch eine Authorization-ID Bezug genommen ist, kann Digital-Adressen-Informationen enthalten, die verwendet werden sollen, um eine Kommunikations-Verbindung zwischen einer Verwahrungsstelle und einer Autorisierungs-Quelle einzustellen. Diese sind analog zu Telefonnummern. Für solche Zugriffs-Tests müßte die Kommunikation eingerichtet werden und eine Autorisierung erhalten werden, bevor das Recht ausgeübt werden könnte.

[0120] Für einmalige Benutzungsrechte ist eine Variante dieses Schemas diejenige, ein digitales Ticket zu haben. Ein Ticket wird einem Digital-Ticket-Agenten präsentiert, dessen Typ auf dem Ticket spezifiziert ist. In dem einfachsten Fall ist ein zertifizierter, allgemeiner Ticket-Agent, verfügbar an allen Verwahrungsstellen, verfügbar, um das Ticket zu ”stanzen”. In anderen Fällen kann das Ticket Adressier-Informationen enthalten, um einen ”speziellen Ticket-Agenten” zu lokalisieren. Wenn einmal ein Ticket gestanzt worden ist, kann es nicht erneut wieder für dieselbe Art einer Transaktion verwendet werden (ohne dass es nicht gestanzt oder in der anderen Art und Weise, die nachfolgend beschrieben ist, erneuert ist). Ein Stanzen umfasst ein Markieren des Tickets mit einem Zeitstempel des Datums und der Zeit, zu dem es verwendet wurde. Tickets sind digitale Arbeiten und können zwischen Verwahrungsstellen entsprechend den Benutzungsrechten kopiert oder übertragen werden.

[0121] In der derzeit bevorzugten Ausführungsform wird ein ”gestanztes” Ticket ”ungestanzt” oder ”erneuert”, wenn es kopiert oder extrahiert ist. Die Copy und Extract Operationen sichern das Datum und die Zeit als eine Eigenschaft des digitalen Tickets. Wenn einem Ticket-Agent ein Ticket gegeben ist, kann er einfach prüfen, ob die digitale Kopie nach der letzten Zeit, zu der es gestanzt wurde, vorgenommen wurde. Natürlich muß das digitale Ticket die Kopie haben oder Benutzungsrechte, die daran angehängt sind, extrahieren.

[0122] Die Fähigkeit, ein Ticket zu entstanzen, ist in den folgenden Fällen wichtig.

- Eine digitale Arbeit wird unter niedrigen Kosten unter einer Einschränkung zirkuliert, dass sie nur einmal verwendet werden kann.
- Eine digitale Arbeit wird mit einem Ticket zirkuliert, das einmal verwendet werden kann, um Rabatte bzw. Discounts beim Erwerben von anderen Arbeiten zu geben.
- Eine digitale Arbeit wird mit einem Ticket (erhaltend in dem Erwerbspreis und möglicherweise eingebettet in die Arbeit) zirkuliert, das für eine zukünftige Aktualisierung verwendet werden kann.

[0123] In jedem dieser Fälle würde, wenn eine bezahlte Kopie in Bezug auf die digitale Arbeit (umfassend das Ticket) erstellt wird, der neue Besitzer erwarten, ein neues (nicht gestanztes) Ticket zu erhalten, ob nun der Kopie-Verkäufer die Arbeit verwendet hat oder nicht. Im Gegensatz dazu sollte ein Ausleihen einer Arbeit oder ein einfaches Übertragen davon zu einer anderen Verwahrungsstelle nicht das Ticket wieder zum Leben erwecken.

Benutzungsgebühren und Leistungsprämien-Spezifikation

[0124] Die Inrechnungstellung der Verwendung einer digitalen Arbeit dient grundsätzlich für ein kommerzielles Verteilungssystem. Grammatik-Element **1517** "Fee-Spec: {Scheduled-Discount} Regular-Fee-Spec | Scheduled-Fee-Spec | Markup-Spec" liefert einen Bereich von Optionen zum Inrechnungstellen der Benutzung von digitalen Arbeiten.

[0125] Ein Schlüsselmerkmal dieser Maßnahme ist die Entwicklung einer Inrechnungstellung mit niedrigem Overhead für Transaktionen in potentiell kleinen Mengen. Demzufolge wird es möglich, Gebühren von nur ein paar Cent jeweils für Tausende von Transaktionen einzusammeln.

[0126] Die Grammatik differenziert zwischen Verwendungen, bei denen die Berechnung pro Benutzung erfolgt, von denjenigen, wo sie über die Zeiteinheit erfasst wird. Transaktionen können Gebühren unterstützen, die der Benutzer zur Verwendung einer digitalen Arbeit bezahlt, ebenso wie Leistungsprämien, die durch den Geber des Rechts Benutzern gewährt wird, um sie dazu zu veranlassen, die digitale Arbeit zu benutzen und zu verteilen.

[0127] Der optionale, ablaufmäßig geplante Discount bezieht sich auf den Rest der Gebührenspezifikation – Diskontieren von diesem mit einem Prozentsatz über die Zeit. Falls es nicht spezifiziert ist, ist dabei kein Discount geplant. Reguläre Gebührenspezifikationen sind über die Zeit konstant. Ablaufmäßig geplante Gebührenspezifikationen geben einen Ablaufplan von Daten, über die sich die Gebührenspezifikationen ändern. Aufschlagspezifikationen werden in d-Blöcken zum Hinzufügen eines Prozentsatzes zu den Gebühren, die bereits berechnet sind, verwendet werden.

[0128] Grammatik-Element **1518** "Scheduled-Discount: = (Scheduled-Discount: (Time-Spec Percentage)*)" Ein Scheduled-Discount ist im Wesentlichen ein ablaufmäßig geplanter Modifizierer von irgendeiner anderen Gebührenspezifikation für diese Version des Rechts der digitalen Arbeit. (Sie bezieht sich nicht auf Children- oder Parent-Digital-Arbeiten oder auf andere Versionen von Rechten.) Sie ist eine Liste von Paaren von Zeiten und Prozentsätzen. Die am kürzesten vorher liegende Zeit in der Liste, die noch nicht zu dem Zeitpunkt der Transaktion vorüber ist, ist die eine, die gerade auftritt. Der Prozentsatz gibt den Discount-Prozentsatz an. Zum Beispiel bezieht sich die Zahl 10 auf einen Discount von 10%.

[0129] Grammatik-Element **1519** "Regular-Fee-Spec: = ({Fee: | Incentive: } [Per-Use-Spec Metered-Rate-Spec | Best-Price-Spec | Call-For-Price-Spec] {Min: Money-Unit Per: Time-Spec} {Max: Money-Unit Per: Time-Spec} To: Account-ID)" liefert verschiedene Arten von Gebührenspezifikationen.

[0130] Gebühren werden durch den Kopie-Besitzer/Benutzer an den Finanzverwaltungs-Besitzer bezahlt, falls Fee: spezifiziert ist. Leistungsprämien werden durch den Finanzverwaltungs-Besitzer (Revenue-Owner) an den Benutzer gezahlt, falls Incentive: spezifiziert ist. Falls die Min: Spezifikation gegeben ist, dann ist dabei eine minimale Gebühr vorhanden, die pro Zeit-Spec Einheit für deren Verwendung berechnet wird. Falls die Max: Spezifikation gegeben ist, dann ist dabei eine maximale Gebühr vorhanden, die pro Time-Spec für deren Verwendung berechnet wird. Wenn Fee: spezifiziert ist, identifiziert Account-ID das Konto, an das die Gebühr zu bezahlen ist. Wenn Incentive: spezifiziert ist, identifiziert Account-ID das Konto, von dem die Gebühr zu bezahlen ist.

[0131] Grammatik-Element **1520** "Per-Use-Spec: = Per-Use-Money-Unit" definiert eine einfache Gebühr, die zu jedem Zeitpunkt gezahlt werden soll, zu dem das Recht ausgeübt wird, ungeachtet davon, wieviel Zeit die Transaktion benötigt.

[0132] Grammatik-Element **1521** "Metered-Rate-Spec: = Metered: Money-Unit Per: Time-Spec" definiert eine Gebühr basierend auf einer gemessenen bzw. dosierten Rate entsprechend dazu, wie lange das Recht ausgeübt wird. Demzufolge bestimmt die Zeit, die benötigt wird, um die Transaktion abzuschließen, die Gebühr.

[0133] Grammatik-Element **1522** "Best-Price-Spec: = Best-Price: Money-unit Max: Money-unit" wird dazu verwendet, einen besten Preis zu spezifizieren, der bestimmt wird, wenn das Konto eingerichtet wird. Diese Spezifikation dient dazu, spezielle Vereinbarungen, Rabatte und Preise anzupassen, die von Informationen abhängen, die nicht für die Verwahrungsstelle verfügbar sind. Alle Gebührenspezifikationen können mit Tickets oder Autorisierungen kombiniert werden, die anzeigen könnten, dass der Verbraucher ein Großhändler ist oder dass er ein bevorzugter Kunde ist, oder dass der Verkäufer in bestimmter Art und Weise autorisiert ist. Die Menge an Geld in dem Max: Feld ist der maximale Betrag, den die Benutzung kosten wird. Dies ist der Betrag,

der versuchsweise von dem Kredit-Server berechnet wird. Allerdings wird, wenn die Transaktion letztendlich in Einklang gebracht ist, irgendein überschüssiger Betrag zu dem Kunden in einer separaten Transaktion zurückgeführt werden.

[0134] Grammatik-Element **1523** "Call-For-Price-Spec: = Call-For-Price" ist ähnlich zu "Best-Price-Spec" dahingehend, dass vorgesehen ist, Fälle anzupassen, wo Preise dynamisch sind. Eine Call-For-Price Spec erfordert eine Kommunikation mit einem Händler, um den Preis zu bestimmen. Diese Option kann nicht ausgeübt werden, wenn die Verwahrungsstelle nicht mit einem Händler zu der Zeit kommunizieren kann, zu der das Recht ausgeübt wird. Sie basiert auf einer sicheren Transaktion, wobei der Händler einen Preis benennt, um das Recht auszuüben, und zusammen mit einem Handels-Zertifikat weiterleitet, auf das in dem Rechnungsstellungsprozess Bezug genommen oder das darin eingeschlossen wird.

[0135] Grammatik-Element **1524** "Scheduled-Fee-Spec: = (Schedule: (Time-Spec Regular-Fee-Spec)*) wird dazu verwendet, einen Ablaufplan von Daten zu liefern, über die sich die Gebührenspezifikationen ändern. Die Gebührenspezifikation mit dem am kürzesten vorher liegenden Datum, nicht in der Zukunft, ist die eine, die vorgenommen wird. Dies ist ähnlich, allerdings viel allgemeiner, als der ablaufmäßig geplante Discount. Es ist allgemeiner, da dies ein Mittel schafft, um eine Gebührenaufstellung für jede Zeitperiode zu variieren.

[0136] Grammatik-Element **1525** "Markup-Spec: = Markup: percentage To: Account-ID" ist zum Hinzufügen eines Prozentsatzes zu den Gebühren, die bereits berechnet sind, vorgesehen. Zum Beispiel bedeutet ein Zuschlag von 5% (5% Markup), dass eine Gebühr von 5% einer kumulativen Gebühr bis jetzt dem Verteiler zugeordnet wird. Eine Zuschlagspezifikation kann bei allen anderen Arten von Gebührenspezifikationen angewandt werden. Dies wird typischerweise in einem Mantel verwendet, der durch einen Verteiler geliefert wird. Sie bezieht sich auf Gebühren, die d-Blöcken zugeordnet sind, die Teile des momentanen d-Blocks sind. Dies könnte eine passende Spezifikation für die Verwendung bei Steuern oder in einem Distributor-Overhead sein.

VERWAHRUNGSSTELLEN-TRANSAKTIONEN

[0137] Wenn ein Benutzer einen Zugriff auf eine digitale Arbeit anfordert, wird die Verwahrungsstelle verschiedene Transaktionen initiieren. Die Kombination von Transaktionen, die aufgerufen sind, hängt von den Spezifikationen ab, die einem Benutzungsrecht zugeordnet sind. Dabei sind drei grundsätzliche Typen von Transaktionen vorhanden, Session Initiation Transactions, Financial Transactions und Usage Transactions. Allgemein werden Session Initiation Transactions (Sitzungs-Initiierungs-Transaktionen) zuerst initiiert, um eine gültige Sitzung einzurichten. Wenn eine gültige Sitzung eingerichtet ist, werden Transaktionen entsprechend zu den verschiedenen Nutzungsrechten aufgerufen. Schließlich werden anforderungs-spezifische Transaktionen durchgeführt.

[0138] Transaktionen treten zwischen zwei Verwahrungsstellen (wobei eine als ein Server arbeitet), zwischen einer Verwahrungsstelle und einer Dokumenten-Abspiel-Plattform (z. B. zum Ausführen oder zum Betrachten), zwischen einer Verwahrungsstelle und einem Kredit-Server oder zwischen einer Verwahrungsstelle und einem Autorisierungs-Server, auf. Wenn Transaktionen zwischen mehr als einer Verwahrungsstelle auftreten, wird angenommen, dass dort ein zuverlässiger Kommunikationskanal zwischen den Verwahrungsstellen vorhanden ist. Zum Beispiel könnte dies ein TCP/IP-Kanal oder irgendein anderer, kommerziell verfügbarer Kanal sein, der eingebaute Fähigkeiten zum Erfassen und zum Korrigieren von Übertragungsfehlern besitzt. Allerdings wird nicht angenommen, dass der Kommunikationskanal sicher ist. Vorsehungen für eine Sicherheit und eine Privatsphäre sind Teil der Erfordernisse zum Spezifizieren und Ausführen von Verwahrungsstellen und bilden so das Erfordernis für verschiedene Transaktionen.

Nachrichten-Übertragung

[0139] Transaktionen erfordern, dass dabei eine bestimmte Kommunikation zwischen Verwahrungsstellen vorhanden ist. Eine Kommunikation zwischen Verwahrungsstellen tritt in Einheiten auf, die als Nachrichten bezeichnet sind. Da die Kommunikationsleitung dahingehend angenommen wird, dass sie nicht sicher ist, werden alle Kommunikationen mit Verwahrungsstellen, die von der vorstehend angegebenen niedrigsten Sicherheitsklasse sind, verschlüsselt, unter Verwendung einer Öffentlich-Schlüssel-Verschlüsselungstechnik. Eine Öffentlich-Schlüssel-Verschlüsselung ist eine ausreichend bekannte Technik auf dem Gebiet der Verschlüsselung. Der Ausdruck Schlüssel bezieht sich auf einen numerischen Code, der in Verbindung mit Verschlüsselungs- und Entschlüsselungs-Algorithmen verwendet wird. Schlüssel kommen in Paaren an, wobei "schreibende Schlüssel" dazu verwendet werden, Daten zu verschlüsseln, und "prüfende Schlüssel" dazu verwendet werden, Daten zu entschlüsseln. Sowohl schreibende als auch prüfende Schlüssel können öffentlich oder

privat sein. Öffentliche Schlüssel sind solche, die zu anderen hin verteilt werden. Privatschlüssel werden vertraulich gehalten.

[0140] Ein Schlüssel-Management und eine -Sicherheit ist ein Instrumentarium aufgrund eines Öffentlich-Schlüssel-Verschlüsselungs-Systems. In der derzeit bevorzugten Ausführungsform behalten eine oder mehrere Master-Verwahrungsstellen die Schlüssel bei und erzeugen die Identifikations-Zertifikate, die durch die Verwahrungsstellen verwendet werden.

[0141] Wenn eine sendende Verwahrungsstelle eine Nachricht zu einer empfangenden Verwahrungsstelle überträgt, verschlüsselt die sendende Verwahrungsstelle alle deren Daten unter Verwendung des öffentlichen, schreibenden Schlüssels der empfangenen Verwahrungsstelle. Die sendende Verwahrungsstelle schließt deren Namen, den Namen der empfangenden Verwahrungsstelle, einen Sessions-Identifizierer, wie beispielsweise einen einmaligen (nonce) (der nachfolgend beschrieben wird) und einen Nachrichten-Zähler in jeder Nachricht ein.

[0142] Auf diese Art und Weise kann die Kommunikation nur durch die empfangende Verwahrungsstelle gelesen werden (mit einer hohen Wahrscheinlichkeit), die den privaten, prüfenden Schlüssel für die Entschlüsselung hält. Die Hilfs-Daten werden dazu verwendet, gegen verschiedene Angriffe auf die Sicherheit zu schützen. Wenn Nachrichten mit dem falschen Zähler oder einem alten Adhoc-Wort ankommen, können die Verwahrungsstellen annehmen, dass irgendjemand mit einer Kommunikation und der Transaktion, die beendet ist, in Wechselwirkung tritt.

[0143] Die jeweiligen, öffentlichen Schlüssel für die Verwahrungsstellen, die für eine Verschlüsselung verwendet werden sollen, werden in der Registrierungs-Transaktion, die nachfolgend beschrieben ist, erhalten.

Sitzungs-Initiierungs-Transaktionen

[0144] Eine Benutzungs-Transaktion wird in einer Sitzung zwischen Verwahrungsstellen ausgeführt. Für Benutzungs-Transaktionen, die mehr als eine Verwahrungsstelle einsetzen, oder für Finanztransaktionen zwischen einer Verwahrungsstelle und einem Kredit-Server, wird eine Registrierungs-Transaktion durchgeführt. Eine zweite Transaktion, bezeichnet als Log-in-Transaktion, kann auch benötigt werden, um die Sitzung zu initiieren. Das Ziel der Registrierungs-Transaktion ist dasjenige, einen sicheren Kanal zwischen zwei Verwahrungsstellen einzurichten, die zueinander die Identitäten kennen. Da angenommen wird, dass der Kommunikationskanal zwischen den Verwahrungsstellen zuverlässig, allerdings nicht sicher, ist, ist ein Risiko vorhanden, dass eine Nicht-Verwahrungsstelle das Protokoll nachahmen kann, um einen nicht legalen Zugriff zu einer Verwahrungsstelle zu erhalten.

[0145] Die Registrierungs-Transaktion zwischen zwei Verwahrungsstellen wird unter Bezugnahme auf die **Fig.** 16 und **Fig.** 17 beschrieben. Die Schritte, die beschrieben sind, erfolgen von der Perspektive einer ”Verwahrungsstelle-1”, die ihre Identität mit einer ”Verwahrungsstelle-2” registriert, aus. Die Registrierung muß symmetrisch sein, so dass derselbe Satz von Schritten für die Verwahrungsstelle-2 wiederholt werden wird, die deren Identität zu der Verwahrungsstelle-1 registriert. Wie **Fig.** 16 zeigt, erzeugt die Verwahrungsstelle-1 zuerst einen verschlüsselten Registrierungs-Identifizierer, Schritt **1601**, und erzeugt dann eine Registrierungs-Nachricht, Schritt **1602**. Eine Registrierungs-Nachricht ist auf einem Identifizierer einer Master-Verwahrungsstelle, dem Identifikations-Zertifikat für die Verwahrungsstelle-1 und einem verschlüsselten Zufalls-Registrierungs-Identifizierer aufgebaut. Das Identifikations-Zertifikat ist durch die Master-Verwahrungsstelle in deren Privat-Schlüssel verschlüsselt, und bescheinigt die Tatsache, dass die Verwahrungsstelle (hier Verwahrungsstelle-1) eine gutgläubige Verwahrungsstelle ist. Das Identifikations-Zertifikat enthält auch einen öffentlichen Schlüssel für die Verwahrungsstelle, den Verwahrungsstellen-Sicherheits-Level und einen Zeitstempel (eine Zeit anzeigend, nach der das Zertifikat nicht länger gültig ist). Der Registrierungs-Identifizierer ist eine Zahl, erzeugt durch die Verwahrungsstelle für diese Registrierung. Der Registrierungs-Identifizierer ist eindeutig für die Sitzung und ist in dem Privat-Schlüssel der Verwahrungsstelle-1 verschlüsselt. Der Registrierungs-Identifizierer wird dazu verwendet, eine Sicherheit einer Autentifikation durch Erfassen bestimmter Arten von auf Kommunikationen basierenden Angriffen zu verbessern. Die Verwahrungsstelle-1 überträgt dann die Registrierungs-Nachricht zu der Verwahrungsstelle-2, Schritt **1603**.

[0146] Unter Empfangen der Registrierungs-Nachricht bestimmt die Verwahrungsstelle-2, ob sie den öffentlichen Schlüssel für die Master-Verwahrungsstelle benötigt hat, Schritt **1604**. Falls die Verwahrungsstelle-2 nicht den benötigten, öffentlichen Schlüssel besitzt, um das Identifikations-Zertifikat zu entschlüsseln, endet die Registrierungs-Transaktion in einem Fehler, Schritt **1618**.

[0147] Es wird angenommen, dass die Verwahrungsstelle-2 den geeigneten, öffentlichen Schlüssel hat, wobei das Identifikations-Zertifikat entschlüsselt wird, Schritt **1605**. Die Verwahrungsstelle-2 sichert den verschlüsselten Registrierungs-Identifizierer, Schritt **1606**, und extrahiert den Verwahrungsstellen-Identifizierer, Schritt **1607**. Der extrahierte Verwahrungsstellen-Identifizierer wird gegen eine ”hotlist” von betroffenen Dokumenten-Verwahrungsstellen geprüft, Schritt **1608**. In der derzeit bevorzugten Ausführungsform wird jede Verwahrungsstelle ”hotlist” von betroffenen Verwahrungsstellen enthalten. Falls die Verwahrungsstelle auf der ”hotlist” vorhanden ist, endet die Registrierungs-Transaktion in einem Fehler mit Schritt **1618**. Verwahrungsstellen können von der hotlist entfernt werden, wenn deren Zertifikate ablaufen, so dass die Liste nicht anwachsen muß. Auch kann, durch Beibehalten einer kurzen Liste von Hotlist-Zertifikaten, die sie zuvor empfangen hat, eine Verwahrungsstelle die Arbeit vermeiden, tatsächlich durch die Liste hindurchzugehen. Diese Listen würden durch eine Master-Verwahrungsstelle verschlüsselt sein. Eine kleine Variation in Bezug auf die Maßnahme, eine Effektivität zu verbessern, würde die Verwahrungsstellen zuerst Listen von Namen von Hotlist-Zertifikaten ändern lassen, was letztendlich nur solche Listen austauscht, die sie nicht zuvor empfangen hatten. Die ”hotlists” werden beibehalten und durch Master-Verwahrungsstellen verteilt.

[0148] Es ist anzumerken, dass, im Gegensatz dazu, in einem Fehler zu enden, die Transaktion fordern könnte, dass eine andere Registrierungs-Nachricht gesendet wird, und zwar basierend auf einem Identifikations-Zertifikat, das durch eine andere Master-Verwahrungsstelle erzeugt ist. Dies kann wiederholt werden, bis ein zufriedenstellendes Identifikations-Zertifikat gefunden ist, oder bestimmt ist, dass ein Vertrauen nicht eingerichtet werden kann.

[0149] Unter der Annahme, dass die Verwahrungsstelle nicht auf der hotlist vorhanden ist, muß die Verwahrungsstellen-Identifikation verifiziert werden. Mit anderen Worten muß die Verwahrungsstelle-2 für gültig erklären, dass die Verwahrungsstelle an dem anderen Ende tatsächlich Verwahrungsstelle-1 ist. Dies wird als ein Performance-Testen bezeichnet und wird durchgeführt, um einen ungültigen Zugriff auf die Verwahrungsstelle über eine nachgeahmte Verwahrungsstelle zu vermeiden, die eine Aufzeichnung einer früheren Sitzungs-Initiierung zwischen Verwahrungsstelle-1 und Verwahrungsstelle-2 erneut abspielt. Ein Performance- bzw. Funktions-Testen wird durch Verwahrungsstelle-2 initiiert, was eine Funktionsnachricht erzeugt, Schritt **1609**. Die Funktionsnachricht besteht aus einem ”Nonce”, den Namen der jeweiligen Verwahrungsstellen, der Zeit und dem Registrierungs-Identifizierer, empfangen von Verwahrungsstelle-1. Ein ”Nonce” ist eine erzeugte Nachricht basierend auf bestimmten Zufalls- und variablen Informationen (z. B. die Zeit oder die Temperatur). Das Nonce wird dazu verwendet, zu prüfen, ob Verwahrungsstelle-1 tatsächlich eine korrekte Verschlüsselung einer Nachricht unter Verwendung der privaten Schlüssel, die sie beansprucht zu haben, in Bezug auf eine Nachricht zeigen kann, die niemals zuvor gesehen worden ist. Die Funktionsnachricht wird unter Verwendung des öffentlichen Schlüssels, spezifiziert in der Registrierungs-Nachricht der Verwahrungsstelle-1, verschlüsselt. Die Funktionsnachricht wird zu der Verwahrungsstelle-1, Schritt **1610**, übertragen, wo sie durch die Verwahrungsstelle-1 unter Verwendung deren privaten Schlüssels entschlüsselt wird, Schritt **1611**. Die Verwahrungsstelle-1 prüft dann, um sicherzustellen, dass die Namen der zwei Verwahrungsstellen korrekt sind, Schritt **1612**, dass die Zeit akkurat ist, Schritt **1613**, und dass der Registrierungs-Identifizierer dem einen entspricht, den sie schickt, Schritt **1614**. Falls irgendwelche dieser Tests fehlschlagen, wird die Transaktion mit Schritt **1616** beendet. Unter der Annahme, dass die Tests durchgelaufen sind, überträgt die Verwahrungsstelle-1 das Nonce zu der Verwahrungsstelle-2 klar und deutlich, Schritt **1615**. Die Verwahrungsstelle-2 vergleicht dann das empfangene Nonce mit dem originalen Nonce, Schritt **1617**. Falls sie nicht identisch sind, endet die Registrierungs-Transaktion in einem Fehler mit Schritt **1618**. Falls sie dieselben sind, ist die Registrierungs-Transaktion erfolgreich abgeschlossen worden.

[0150] An diesem Punkt tauschen, unter der Annahme, dass die Transaktion nicht beendet ist, die Verwahrungsstellen Nachrichten aus, die Sitzungs-Schlüssel enthalten, die in allen Kommunikationen während der Sitzung verwendet werden sollen, und Synchronisieren deren Takte. **Fig.** 17 stellt den Sitzungs-Informations-Austausch und die Takt-Synchronisations-Schritte dar (wiederum von der Perspektive der Verwahrungsstelle-1 aus gesehen). Wie **Fig.** 17 zeigt, erzeugt Verwahrungsstelle-1 ein Sitzungs-Schlüssel-Paar, Schritt **1701**. Ein erster Schlüssel wird privat gehalten und wird durch Verwahrungsstelle-1 verwendet, um Nachrichten zu verschlüsseln. Der zweite Schlüssel ist ein öffentlicher Schlüssel, verwendet durch Verwahrungsstelle-2, um Nachrichten zu entschlüsseln. Der zweite Schlüssel ist unter Verwendung des öffentlichen Schlüssels von Verwahrungsstelle-2 verschlüsselt, Schritt **1702**, und wird zu der Verwahrungsstelle-2 geschickt, Schritt **1703**. Unter Empfang entschlüsselt die Verwahrungsstelle-2 den zweiten Schlüssel, Schritt **1704**. Der zweite Schlüssel wird dazu verwendet, Nachrichten in darauffolgenden Kommunikationen zu entschlüsseln. Wenn jede Verwahrungsstelle diesen Schritt abgeschlossen hat, sind sie beide übereingekommen, dass die andere Verwahrungsstelle ehrlich bzw. vertrauenswürdig ist und dass sie mit dem Original kommunizieren. Jede Verwahrungsstelle hat der anderen einen Schlüssel gegeben, der beim Entschlüsseln weiterer Kommunikationen während der

Sitzung verwendet werden soll. Da dieser Schlüssel selbst in dem öffentlichen Schlüssel der empfangenden Verwahrungsstelle übertragen ist, wird nur sie in der Lage sein, den Schlüssel zu entschlüsseln, der dazu verwendet ist, darauffolgende Nachrichten zu entschlüsseln.

[0151] Nachdem die Sitzungs-Informationen ausgetauscht sind, müssen die Verwahrungsstellen deren Takte synchronisieren. Eine Takt-Synchronisation wird durch die Verwahrungsstellen verwendet, um eine gemeinsam vereinbarte Zeit-Basis für die finanziellen Aufzeichnungen deren gegenseitiger Transaktionen einzurichten. Wie wiederum **Fig.** 17 zeigt, initiiert die Verwahrungsstelle-2 eine Takt-Synchronisation durch Erzeugen einer Zeit-Stempel-Austausch-Nachricht, Schritt **1705**, und überträgt sie zu der Verwahrungsstelle-1, Schritt **1706**. Unter Empfang erzeugt die Verwahrungsstelle-1 deren eigene Zeit-Stempel-Nachricht, Schritt **1707**, und überträgt sie zurück zu Verwahrungsstelle-2, Schritt **1708**. Die Verwahrungsstelle-2 erfasst die momentane Zeit, Schritt **1709**, und speichert die Zeit, empfangen von der Verwahrungsteile-1, Schritt **1710**. Die momentane Zeit wird mit der Zeit, empfangen von der Verwahrungsstelle-1, verglichen, Schritt **1711**. Der Unterschied wird dann geprüft, um zu sehen, ob er eine vorbestimmte Toleranz übersteigt (z. B. eine Minute), Schritt **1712**. Falls dies der Fall ist, beendet die Verwahrungsstelle-2 die Transaktion, da dies einen manipulierenden bzw. unberechtigten Eingriff mit der Verwahrungsstelle anzeigen kann, Schritt **1713**. Falls dies nicht der Fall ist, berechnet die Verwahrungsstelle-2 ein eingestelltes Zeit-Delta, Schritt **1714**. Das eingestellte Zeit-Delta ist die Differenz zwischen der Takt-Zeit von Verwahrungsstelle-2 und dem Durchschnitt der Zeiten von Verwahrungsstelle-1 und Verwahrungsstelle-2.

[0152] Um eine größere Genauigkeit zu erreichen, kann die Verwahrungsstelle-2 die Zeit erneut anfordern, bis zu einer festgelegten Anzahl von Malen (z. B. fünf Mal), die Takt-Synchronisations-Schritte wiederholen und die Ergebnisse mitteln.

[0153] Eine zweite Sitzungs-Initiierungs-Transaktion ist eine Log-in-Transaktion. Die Log-in-Transaktion wird dazu verwendet, die Authentizität eines Benutzers, der eine Transaktion anfordert, zu prüfen. Eine Log-in-Transaktion ist besonders für die Autorisierung von finanziellen Transaktionen vernünftig, die an einen Kredit-Server in Rechnung gestellt werden werden. Die Log-in-Transaktion setzt eine Interaktion zwischen dem Benutzer an einer Benutzerschnittstelle und dem Kredit-Server, zugeordnet einer Verwahrungsstelle, ein. Die Informationen, die hier ausgetauscht sind, sind eine Log-in-Folge, zugeführt durch den Verwahrungsstellen/Kredit-Server, um sich selbst dem Benutzer zu identifizieren und einer Personal-Identifikations-Nummer (Personal Identification Number – PIN), geliefert durch den Benutzer, um ihn selbst zu dem Kredit-Server zu identifizieren. In dem Fall, dass der Benutzer auf einen Kredit-Server in einer Verwahrungsstelle, unterschiedlich zu der einen, auf der die Benutzerschnittstelle vorhanden ist, zugreift, würde ein Austausch der Informationen unter Verwendung der öffentlichen und privaten Schlüssel für die jeweiligen Verwahrungsstellen verschlüsselt werden.

Rechnungsstellungs-Transaktionen

[0154] Rechnungsstellungs-Transaktionen (Billing Transactions) sind auf Finanztransaktionen mit einem Kredit-Server gerichtet. Rechnungsstellungs-Transaktionen werden ausgeführt, wenn alle Bedingungen erfüllt sind und eine Benutzungsgebühr zum Gewähren der Anforderung erforderlich ist. Für den größten Teil werden Rechnungsstellungs-Transaktionen aufgrund des Stands der Technik verstanden. Diese Transaktionen erfolgen zwischen einer Verwahrungsstelle und einem Kredit-Server oder zwischen einem Kredit-Server und einer Zahlstelle. Kurz gesagt umfassen die erforderlichen Transaktionen die folgenden:

- Registrierung und LOGIN Transaktionen, durch die die Verwahrungsstelle und ein Benutzer deren Vertrauenswürdigkeit zu einem Kredit-Server hin einrichten. Diese Transaktionen würden vollständig intern in Fällen sein, wo die Verwahrungsstelle und der Kredit-Server als ein einzelnes System ausgeführt sind.
- Registrierung und LOGIN Transaktionen, durch die ein Kredit-Server seine Vertrauenswürdigkeit zu einer Zahlstelle hin einrichtet.
- Eine Assign-Fee Transaktion, um eine Berechnung zuzuordnen. Die Informationen in dieser Transaktion würden einen Transaktions-Identifizierer, die Identitäten der Verwahrungsstellen in der Transaktion und eine Liste von Gebühren für die Teile der digitalen Arbeit umfassen. Falls dabei irgendein ungewöhnliches Ereignis in der Transaktion vorhanden gewesen ist, wie beispielsweise eine Unterbrechung von Kommunikationen, werden diese Informationen ebenso eingeschlossen werden.
- Eine Beginn-Gebühren-Transaktion, um eine Gebühr zuzuordnen. Diese Transaktion ist im Wesentlichen dieselbe wie eine Zuordnungs- bzw. Einschreibe-Gebühr-Transaktion, mit der Ausnahme, dass sie für eine dosierte bzw. erfasste Benutzung verwendet wird. Sie umfasst dieselben Informationen wie die Assign-Fee Transaktion ebenso wie die Benutzungs-Gebühren-Information. Der Kredit-Server ist dann für ein Laufenlassen eines Taktes verantwortlich.

• Eine End-Gebühren-Transaktion, um eine Gebühr für eine dosierte bzw. gemessene Benutzung zu beenden. (In einer Variation dieser Maßnahme würden die Verwahrungsstellen periodisch Informationen für jeden Zeitblock austauschen.)
• Eine Report-Gebühren-Transaktion zwischen einem Personal-Kredit-Server und einer Zahlstelle. Diese Transaktion wird mindestens einmal pro Zahlperiode aufgerufen. Sie wird dazu verwendet, Informationen über Gebühren weiterzuleiten. Auf Debit- und Kredit-Karten würde diese Transaktion auch dazu verwendet werden, Balance-Informationen und Kreditgrenzen zu aktualisieren, wie dies benötigt wird.

[0155] Allen Zahlungstransaktionen wird eine Transaktions-ID gegeben und sie werden zu den Kredit-Servern durch sowohl den Server als auch den Client berichtet. Dies verringert einen möglichen Verlust von Zahlungs-Informationen, wenn eine der Parteien in Bezug auf eine Transaktion eine Bankkarte verliert und eine Prüfung gegenüber einem unberechtigten Eingriff in das System vornimmt.

Benutzungs-Transaktionen

[0156] Nachdem die Sitzungs-Initiierungs-Transaktionen abgeschlossen worden sind, dann kann die Benutzungsanforderung bearbeitet werden. Um die Beschreibung der Schritte, die bei der Verarbeitung einer Benutzungsanforderung ausgeführt werden, zu vereinfachen, wird der Ausdruck ”Anforderer” hier dazu verwendet, auf eine Verwahrungsstelle in dem Anforderer-Modus Bezug zu nehmen, der eine Anforderung einleitet, und der Ausdruck ”Server” wird dazu verwendet, auf eine Verwahrungsstelle in einem Server-Modus Bezug zu nehmen, und der die erwünschte, digitale Arbeit enthält. In vielen Fällen, wie beispielsweise Anforderungen, eine Arbeit zu drucken oder anzusehen, können der Anforderer und der Server dieselbe Vorrichtung sein und die Transaktionen, die nachfolgend beschrieben sind, würden vollständig intern ablaufen. In solchen Fällen müssen bestimmte Transaktions-Schritte, wie beispielsweise die Registrierungs-Transaktion, nicht durchgeführt werden.

[0157] Dabei sind einige gemeinsame Schritte vorhanden, die Teil der Semantiken aller Benutzungsrechte-Transaktionen sind. Diese Schritte werden als die gemeinsamen Transaktions-Schritte bezeichnet. Dabei sind zwei Sätze vorhanden – die ”Öffnungs”Schritte und die ”Schließ-”Schritte. Zur Vereinfachung werden diese hier aufgelistet, im Gegensatz dazu, sie in den Beschreibungen aller Benutzungsrechte-Transaktionen zu wiederholen.

[0158] Transaktionen können sich auf einen Teil einer digitalen Arbeit, eine vollständige, digitale Arbeit oder eine digitale Arbeit, die andere digitale Arbeiten enthält, beziehen. Obwohl es hier nicht im Detail beschrieben ist, kann sich eine Transaktion sogar auf einen Folder beziehen, der aus einer Vielzahl von digitalen Arbeiten aufgebaut ist. Der Ausdruck ”Arbeit” wird dazu verwendet, auf das Bezug zu nehmen, was auch immer ein Teil oder ein Satz von digitalen Arbeiten, auf die zugegriffen werden soll, ist.

[0159] Viele der Schritte hier umfassen ein Bestimmen, ob bestimmte Bedingungen erfüllt sind. Es wird daran erinnert, dass jedes Benutzungsrecht eine oder mehrere Zustände bzw. Bedingungen haben kann, die erfüllt werden müssen, bevor das Recht ausgeübt werden kann. Digitale Arbeiten haben Teile und Teile haben Teile. Unterschiedliche Teile können unterschiedliche Rechte und Gebühren haben. Demzufolge ist es notwendig, zu verifizieren, dass die Erfordernisse für ALLE der Teile erfüllt sind und dass sie in einer Transaktion umfasst sind. Kurz gesagt bedeutet, wenn Bezug auf eine Prüfung genommen wird, ob die Rechte existieren und die Bedingungen für eine Ausübung erfüllt sind, dies, dass eine solche gesamte Prüfung für jeden der relevanten Teile der Arbeit stattfindet.

[0160] **Fig.** 18 stellt die anfänglichen, üblichen Öffnungs- und Schließschritte für eine Transaktion dar. An diesem Punkt wird angenommen, dass hier eine Registrierung aufgetreten ist und dass eine ”vertrauenswürdige” Sitzung stattfindet. Allgemeine Tests sind Tests über Benutzungsrechte, die dem Folder zugeordnet sind, der die Arbeit enthält, oder einigen, die einen Folder höher in der Datei-System-Hierarchie enthalten. Diese Tests entsprechen Erfordernissen, die der Arbeit als Folge auferlegt sind, dass sie an der bestimmten Verwahrungsstelle vorliegt, im Gegensatz dazu, dass sie an die Arbeit selbst angehängt sind. Wie **Fig.** 18 zeigt, führt, vor einer Initiierung einer Benutzungs-Transaktion, der Anforderer irgendwelche allgemeinen Tests durch, die erforderlich sind, bevor das Recht, zugeordnet der Transaktion, ausgeübt werden kann, Schritt **1801**. Zum Beispiel können ein Installieren, ein Deinstallieren und ein Löschen von Rechten ausgeführt werden, um zu fordern, dass ein Anforderer ein Autorisierungs-Zertifikat besitzt, bevor das Recht ausgeübt werden kann. Ein anderes Beispiel ist das Erfordernis, dass ein digitales Ticket vorhanden ist und gestanzt wird, bevor eine digitale Arbeit zu einem Anforderer hin kopiert werden kann. Falls irgendwelche der allgemeinen Tests fehlschlagen, wird die Transaktion nicht initiiert, Schritt **1802**. Es wird angenommen, dass solche erforderlichen Tests durchge-

laufen sind, und zwar unter Empfang der Benutzungsanforderung, wobei dann der Server einen Transaktions-Identifizierer erzeugt, der in Aufzeichnungen oder Berichten der Transaktion verwendet wird, Schritt **1803**. Der Server prüft dann, ob der digitalen Arbeit das Recht erteilt worden ist, entsprechend der angeforderten Transaktion, Schritt **1804**. Falls die digitale Arbeit nicht das Recht entsprechend der Anforderung erteilt worden ist, endet die Transaktion, Schritt **1805**. Falls der digitalen Arbeit das angeforderte Recht erteilt worden ist, dann bestimmt der Server, ob die verschiedenen Bedingungen zum Ausüben des Rechts erfüllt worden sind. Auf der Zeit basierende Bedingungen werden geprüft, Schritt **1806**. Diese Bedingungen werden durch Prüfen der Zeit-Spezifikation für die Version des Rechts geprüft. Falls irgendwelche der Bedingungen nicht erfüllt sind, endet die Transaktion mit Schritt **1805**.

[0161] Unter der Annahme, dass die auf der Zeit basierenden Bedingungen erfüllt sind, prüft der Server Sicherheits- und Zugriffs-Bedingungen, Schritt **1807**. Solche Sicherheits- und Zugriffs-Bedingungen sind erfüllt, falls: 1) der Anforderer sich bei der spezifizierten Sicherheitsklasse befindet, oder einer höheren Sicherheitsklasse, 2) der Server irgendeinen spezifizierten Autorisierungs-Test erfüllt, und 3) der Anforderer irgendwelche spezifizierten Autorisierungs-Tests erfüllt und irgendwelche erforderlichen, digitalen Tickets besitzt. Falls irgendeine der Bedingungen nicht erfüllt ist, endet die Transaktion mit Schritt **1805**.

[0162] Unter der Annahme, dass die Sicherheits- und Zugriffs-Bedingungen alle erfüllt sind, prüft der Server die Kopie-Zählungs-Bedingung, Schritt **1808**. Falls die Kopie-Zählung Null gleicht, dann kann die Transaktion nicht abgeschlossen werden und die Transaktion endet mit Schritt **1805**.

[0163] Unter der Annahme, dass die Kopie-Zählung nicht gleich Null ist, prüft der Server, ob die Kopien, die für das angeforderte Recht in Benutzung sind größer als oder gleich zu irgendeiner Kopie-Zählung für das angeforderte Recht (oder relevante Teile) ist, Schritt **1809**. Falls die Kopien, die in Verwendung sind, größer als oder gleich zu der Kopie-Zählung sind, zeigt dies an, dass Benutzungsrechte für die Version der Transaktion ausgesondert worden sind. Dementsprechend beendet der Server die Transaktion, Schritt **1805**. Falls die Kopie-Zählung geringer als die Kopien, die in Benutzung für die Transaktionen sind, ist, kann die Transaktion nicht fortfahren, und die Kopien, die in Benutzung sind, würden um die Zahl von digitalen Arbeiten, angefordert in der Transaktion, erhöht werden, Schritt **1810**.

[0164] Der Server prüft dann, ob die digitale Arbeit ein ”Loan” (”Ausleih-”) Zugriffs-Recht besitzt, Schritt **1811**. Das ”Ausleih-” Zugriffs-Recht ist ein spezieller Fall, da verbleibende Rechte vorhanden sein können, obwohl alle Kopien ausgeliehen sind. Falls die digitale Arbeit das ”Ausleih” Zugriffs-Recht hat, wird eine Prüfung vorgenommen, um zu sehen, ob alle Kopien ausgeliehen worden sind, Schritt **1812**. Die Anzahl von Kopien, die ausgeliehen werden könnten, ist die Summe der Kopie-Zählungen für alle die Versionen des Ausleih-Rechts der digitalen Arbeit. Für eine Komposit-Arbeit ist die relevante Figur das Minimum einer solchen Summe jeder der Komponenten der Komposit-Arbeit. Falls alle Kopien ausgeliehen worden sind, werden die verbleibenden Rechte bestimmt, Schritt **1813**. Die verbleibenden Rechte werden aus den Spezifikationen der verbleibenden Rechte aus den Versionen des Ausleih-Rechts bestimmt. Falls dort nur eine Version des Ausleih-Rechts vorhanden ist, dann ist die Bestimmung einfach. Die verbleibenden Rechte sind solche, die in dieser Version des Ausleih-Rechts spezifiziert sind, oder keine, falls Remaining-Rights: ist nicht spezifiziert. Falls dort mehrere Versionen des Ausleih-Rechts vorhanden sind und alle Kopien aller der Versionen ausgeliehen sind, dann werden die verbleibenden Rechte als der minimale Satz (Schnittmenge) der verbleibenden Rechte über alle der Versionen des Ausleih-Rechts genommen. Der Server bestimmt dann, ob das angeforderte Recht in dem Satz der verbleibenden Rechte vorhanden ist, Schritt **1814**. Falls das angeforderte Recht nicht in dem Satz der verbleibenden Rechte vorhanden ist, beendet der Server die Transaktion, Schritt **1805**.

[0165] Falls ein Ausleihen nicht ein Benutzungsrecht für die digitale Arbeit ist oder falls alle Kopien nicht ausgeliehen worden sind oder das angeforderte Recht in dem Satz von verbleibenden Rechten vorhanden ist, werden die Gebührenbedingungen für das Recht dann geprüft, Schritt **1815**. Dies wird verschiedene finanzielle Transaktionen zwischen der Verwahrungsstelle und dem zugeordneten Kredit-Server einleiten. Weiterhin wird irgendeine dosierte bzw. gemessene Benutzung einer digitalen Arbeit beginnen. Falls irgendeine finanzielle Transaktion fehlschlägt, endet die Transaktion mit Schritt **1805**.

[0166] Es sollte angemerkt werden, dass die Transaktion, in der die Zustände geprüft werden, nicht der Reihenfolge der Schritte **1806**–**1815** folgen muß.

[0167] An diesem Punkt werden nur Rechte-spezifischen Schritte durchgeführt und sind hier als Schritt **1816** dargestellt. Die Rechte-spezifischen Schritte werden in größerem Detail nachfolgend beschrieben.

[0168] Die üblichen Schließ-Transaktions-Schritte werden nun durchgeführt. Jeder dieser Schließ-Transaktions-Schritte wird durch den Server nach einem erfolgreichen Abschluß einer Transaktion durchgeführt. Wie wiederum **Fig.** 18 zeigt, werden die Kopien, die in Benutzung sind, der Wert für das angeforderte Recht, um die Anzahl von Kopien, die in die Transaktion eingeflossen sind, verringert, Schritt **1817**. Als nächstes subtrahiert, falls das Recht eine gemessene Benutzungs-Gebühr-Spezifikation besaß, der Server die abgelaufene Zeit von der verbleibenden Benutzungszeit, die dem Recht zugeordnet ist, für jeden Teil, der in die Transaktion eingeschlossen ist, Schritt **1818**. Schließlich initiiert, falls dort Gebührenspezifikationen vorhanden sind, die dem Recht zugeordnet sind, der Server eine End-Gebühren-Finanz-Transaktion, um eine Rechnungsstellung zu bestätigen, Schritt **1819**.

Übertragungs-Protokoll

[0169] Ein wichtiger Bereich, der zu berücksichtigen ist, ist die Übertragung der digitalen Arbeit von dem Server zu dem Anforderer. Das Übertragungsprotokoll, das hier beschrieben ist, bezieht sich auf Ereignisse, die auftreten, nachdem eine gültige Sitzung erzeugt worden ist. Das Übertragungsprotokoll muß den Fall einer Unterbrechung in den Kommunikationen zwischen den Verwahrungsstellen handhaben. Es wird angenommen, dass eine Störung, wie beispielsweise ein eintretendes Rauschen in den Kommunikationskanal, durch die Integritäts-Prüfungen (z. B. Parität, Prüfsumme, usw.) geprüft werden kann, die in das Transport-Protokoll eingebaut sind und hier nicht im Detail diskutiert werden.

[0170] Das Ziel in dem Übertragungsprotokoll ist hierbei, bestimmte Fehler-Moden auszuschließen, wie beispielsweise eine fehlerhafte oder ungewollte Interferenz auf dem Kommunikationskanal. Es wird zum Beispiel angenommen, dass der Benutzer eine Karte an dem Kredit-Server zu einer spezifischen Zeit nahe dem Ende einer Transaktion zieht. Dabei sollte keine ungeschützte Zeit vorhanden sein, zu der ein ”Ziehen der Karte” bewirkt, dass die Verwahrungsstellen fehlschlagen, korrekt die Zahl von Kopien der Arbeit, die erzeugt worden ist, zu berechnen. Anders ausgedrückt sollte dort keine Zeit vorhanden sein, zu der eine Partei eine Verbindung als eine Maßnahme unterbrechen kann, um eine Bezahlung, nach Verwendung einer digitalen Arbeit, zu vermeiden.

[0171] Wenn eine Transaktion unterbrochen ist (oder fehlerhaft ist), stellen beide Verwahrungsstellen die digitalen Arbeiten wieder her und berechnen deren Zustand vor dem Fehler, Modulo-Aufzeichnungen des Fehlers selbst.

[0172] **Fig.** 19 ist ein Zustands-Diagramm, das Schritte in dem Prozess einer Übertragung von Informationen während einer Transaktion darstellt. Jeder Kasten stellt einen Zustand einer Verwahrungsstelle in entweder dem Server-Modus (oberhalb der zentralen, punktierten Linie **1901**) oder in dem Anforderer-Modus (unterhalb der punktierten Linie **1901**) dar. Durchgezogene Pfeile stehen für Transaktionen zwischen Zuständen. Unterbrochene Pfeile stehen für Nachrichten-Kommunikationen zwischen den Verwahrungsstellen. Ein unterbrochener Nachrichtenpfeil, der auf einen durchgehenden Übergangspfeil hinweist, wird so interpretiert, dass er bedeutet, dass die Transaktion stattfindet, wenn die Nachricht empfangen ist. Nicht bezeichnete Übergangspfeile finden nicht konditionell statt. Andere Ettiketten an den Zustandspfeilen beschreiben Zustände, die die Übergänge triggern.

[0173] Wie nun **Fig.** 19 zeigt, befindet sich der Server in einem Zustand **1902**, wo eine neue Transaktion über eine Start-Nachricht **1903** initiiert wird. Diese Nachricht umfasst Transaktions-Informationen, umfassend einen Transaktions-Identifizierer, und eine Zählung der Blöcken von Daten, die übertragen werden sollen. Der Anforderer befindet sich zu Anfang in einem Wartezustand **1904**, wobei er dann in einen Daten-Wartezustand **1905** eintritt.

[0174] Der Server tritt in einen Daten-Übertragungszustand **1906** ein und überträgt einen Block von Daten **1907** und tritt in ein Warten für einen Kenntnis-Zustand **1908** ein. Wenn die Daten empfangen sind, tritt der Anforderer in einen Daten-Empfangszustand **1909** ein, und wenn die Datenblöcke vollständig empfangen sind, tritt er nicht in einen Kenntniszustand **1910** ein und überträgt eine Kenntnis-Nachricht **1911** zu dem Server.

[0175] Wenn dabei mehr Blöcke zu verschicken sind, wartet der Server bis zu dem Empfang einer Kenntnis-Nachricht von dem Anforderer. Wenn eine Kenntnis-Nachricht empfangen ist, schickt er den nächsten Block zu dem Anforderer und wartet erneut auf die Kenntnis. Der Anforderer wiederholt auch denselben Zyklus von Zuständen.

[0176] Wenn der Server erfasst, dass eine Kommunikation fehlschlägt, bevor der letzte Block gesendet wird, tritt er in einen Aufhebungszustand **1912** ein, wo die Transaktion aufgehoben wird. Ähnlich tritt, wenn der Anforderer einen Kommunikations-Ausfall vor Empfangen des letzten Blocks erfasst, er in einen Aufhebungs-Zustand **1913** ein.

[0177] Falls dabei keine weiteren Blöcke vorhanden sind, die verschickt werden, beendet er die Transaktion und wartet auf die abschließende Kenntnisnahme im Zustand **1914**. Falls dabei ein Kommunikations-Ausfall auftritt, bevor der Server die abschließende Kenntnis-Nachricht empfängt, überträgt er noch die Transaktion, allerdings schließt er einen Bericht über das Ereignis zu seinem Kredit-Server im Zustand **1915** ein. Dieser Bericht dient zu zwei Zwecken. Er wird dabei helfen, irgendwelche Ansprüche durch einen Benutzer, dass er für empfangene, digitale Arbeiten gezahlt hat, die nicht vollständig empfangen wurden, zu legitimieren. Auch hilft er dabei, Verwahrungsstellen und Kommunikationsleitungen zu identifizieren, die verdächtige Benutzungsmuster und eine Unterbrechung haben. Der Server tritt dann in seinen Abschluß-Zustand **1916** ein.

[0178] Auf der Anforderer-Seite übergibt, wenn dort nicht mehr Blöcke vorhanden sind, die zu empfangen sind, der Anforderer zu der Transaktion im Zustand **1917**. Wenn der Anforderer einen Kommunkations-Fehler bei diesem Zustand erfasst, berichtet er den Fehler zu seinem Kredit-Server in dem Zustand **1918**, allerdings übergibt er zu der Transaktion. Wenn er übergeben hat, sendet er eine Bestätigungs-Nachricht zu dem Server.

[0179] Der Server tritt dann in seinen Vervollständigungs-Zustand **1919** ein.

[0180] Die Schlüssel-Eigenschaft ist diejenige, dass sowohl der Server als auch der Anforderer eine Transaktion aufheben, wenn sie unterbrochen wird, bevor alle Datenblöcke zugeführt sind, und zu ihr übergibt, wenn alle Datenblöcke geliefert worden sind.

[0181] Dabei ist eine Möglichkeit vorhanden, dass der Server alle Datenblöcke gesendet haben muß (und übergeben haben muß), allerdings wird der Anforderer nicht alle davon empfangen haben und wird die Transaktion aufheben. In diesem Fall werden beide Verwahrungsstellen wahrscheinlich einen Kommunikations-Fehler erfasssen und ihn zu deren Kredit-Server berichten. Dieser Fall wird wahrscheinlich selten sein, da er von einer sehr präzisen Zeitabstimmung des Kommunikations-Fehlers abhängt. Die einzige Folge wird die sein, dass der Benutzer an der Verwahrungsstelle des Anforderers es wünschen kann, eine Rückerstattung von den Kredit-Service-Diensten anzufordern – und der Fall für diese Rückerstattung wird durch Berichte durch beide Verwahrungsstellen dokumentiert werden.

[0182] Um einen Verlust von Daten zu verhindern, sollte der Server nicht irgendeine übertragene, digitale Arbeit löschen, bis die Endbestätigung von dem Anforderer empfangen ist. Allerdings soll er auch nicht die Datei verwenden. Eine ausreichend bekannte Art und Weise, um sich dieser Situation zuzuwenden, wird als ”Zwei-Phasen-Übergabe” oder 2PC bezeichnet.

[0183] Eine Zwei-Phasen-Übergabe arbeitet wie folgt. Die erste Phase arbeitet entsprechend dem Verfahren, das vorstehend beschrieben ist. Der Server schickt alle Daten zu dem Anforderer. Beide Verwahrungsstellen markieren die Transaktion (und geeignete Dateien) als nicht übergeben. Der Server schickt eine Nachricht, bereit zur Übergabe, zu dem Anforderer. Der Anforderer schickt eine Bestätigung zurück. Der Server übergibt dann und schickt dem Anforderer eine Übergabe-Nachricht. Wenn der Anforderer die Übergabenachricht empfängt, übergibt er die Datei.

[0184] Wenn dabei ein Kommunikations-Fehler oder ein anderer Crash bzw. Zusammenbruch vorhanden ist, muß der Anforderer mit dem Server zurückprüfen, um den Status der Transaktion zu bestimmen. Der Server hat das letzte Wort hierüber. Der Anforderer kann alle Daten empfangen haben, falls allerdings er nicht die abschließende Nachricht erhalten hat, hat er nicht übergeben. Der Server kann weitergehen und Dateien löschen (mit der Ausnahme der Transaktions-Aufzeichnung), wenn er einmal übergibt, da die Dateien dahingehend bekannt sind, dass sie vollständig übertragen worden sind, bevor der 2PC Zyklus gestartet wird.

[0185] Dabei sind Variationen im Stand der Technik bekannt, die dazu verwendet werden können, denselben Effekt zu erreichen. Zum Beispiel könnte der Server einen zusätzlichen Level einer Verschlüsselung verwenden, wenn eine Arbeit zu einem Client übertragen wird. Nur nachdem der Client eine Nachricht geschickt hat, die einen Empfang bestätigt, schickt er den Schlüssel. Der Client stimmt dann einer Bezahlung für die digitale Arbeit zu. Der Punkt dieser Variation ist derjenige, dass sie einen klaren Audit-Trail liefert, dass der Client die Arbeit empfangen hat. Für vertrauliche Systeme fügt allerdings diese Variation einen Level einer Verschlüsselung für keinen realen Zugang zu einer Zahlungsfähigkeit hinzu.

[0186] Die Transaktion für spezifische Benutzungsrechte wird nun diskutiert.

Die Kopie-Transaktion

[0187] Eine Kopie-Transaktion ist eine Anforderung, eine oder mehrere unabhängige Kopien der Arbeit mit denselben oder geringeren Benutzungsrechten vorzunehmen. Eine Kopie unterscheidet sich von dem Extraktions-Recht, das später diskutiert wird, dahingehend, dass es sich auf gesamte, digitale Arbeiten oder gesamte Folder, die digitale Arbeiten enthalten, bezieht. Eine Kopie-Operation kann nicht verwendet werden, um einen Teil einer digitalen Arbeit zu entfernen.

- Der Anforderer schickt dem Server eine Nachricht, um die Kopie-Transaktion zu initiieren. Diese Nachricht zeigt die Arbeit an, die kopiert werden soll, die Version des Kopierrechts, das für die Transaktion verwendet werden soll, die Bestimmungs-Adressen-Informationen (Stelle in einem Folder) zum Platzieren der Arbeit, die Datei-Daten für die Arbeit (umfassend deren Größe) und die Anzahl von Kopien, die angefordert sind.
- Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktionsschritte durch.
- Der Server überträgt die angeforderten Inhalte und Daten zu dem Client entsprechend dem Übertragungsprotokoll. Falls ein nächster Satz von Rechten (Next-Set-Of-Rights) in der Version des Rechts vorgesehen worden ist, werden solche Rechte als die Rechte für die Arbeit übertragen. Ansonsten werden die Rechte des Originals übertragen. In jedem Fall wird das Kopie-Zählungs-Feld für die Kopie der digitalen Arbeit, die rechtens gesendet ist, auf die Zahl von Kopien, die angefordert sind, eingestellt.
- Der Anforderer zeichnet die Arbeits-Inhalte, Daten und Benutzungsrechte auf und speichert die Arbeit. Er zeichnet die Daten und die Zeit, zu der die Kopie vorgenommen wurde, in den Eigenschaften der digitalen Arbeit auf.
- Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

Die Übertragungs-Transaktion

[0188] Eine Übertragungs-Transaktion ist eine Anforderung, Kopien der Arbeit mit denselben oder geringeren Benutzungsrechten zu einer anderen Verwahrungsstelle zu bewegen. Im Gegensatz zu einer Kopie-Transaktion führt dies zu einem Entfernen der Arbeits-Kopien von dem Server.

- Der Anforderer schickt dem Server eine Nachricht, um die Übertragungs-Transaktion zu initiieren. Diese Nachricht zeigt die Arbeit an, die übertragen werden soll, und die Version des Übertragungsrechts, das bei der Transaktion verwendet werden soll, die Bestimmungs-Adressen-Informationen zum Platzieren der Arbeit, die Datei-Daten für die Arbeit und die Anzahl von Kopien, die umfasst sind.
- Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktions-Schritte durch.
- Der Server überträgt die angeforderten Inhalte und die Daten zu dem Anforderer entsprechend dem Übertragungs-Protokoll. Falls ein nächster Satz von Rechten (Next-Set-Of-Rights) vorgesehen worden ist, werden solche Rechte als die Rechte für die Arbeit übertragen. Ansonsten werden die Rechte des Originals übertragen. In jedem Fall wird das Kopie-Zählungs-Feld für die übertragenen Rechte auf die Zahl von Kopien, die angefordert sind, eingestellt.
- Der Anforderer zeichnet die Arbeits-Inhalte, Daten und Benutzungsrechte auf und speichert die Arbeit.
- Der Server erniedrigt seine Kopie-Zählung um die Zahl von Kopien, die in der Transaktion umfasst sind.
- Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.
- Falls die Anzahl von Kopien, die in dem Server verbleiben, nun Null ist, löscht er die digitale Arbeit von seinem Speicher.

Die Leih-Transaktion

[0189] Eine Leih-Transaktion ist ein Mechanismus zum Leihen von Kopien einer digitalen Arbeit. Die maximale Dauer des Ausleihens wird durch einen internen Parameter der digitalen Arbeit bestimmt. Arbeiten werden automatisch nach einer vorbestimmten Zeitperiode zurückgeführt.

- Der Anforderer schickt dem Server eine Nachricht, die Übertragungs-Transaktion zu initiieren. Diese Nachricht zeigt die Arbeit, die ausgeliehen wird, die Version des Leih-Rechts, die in der Transaktion verwendet werden soll, die Bestimmungs-Adressen-Information zum Platzieren der Arbeit, die Anzahl von Kopien, die umfasst sind, die Datei-Daten für die Arbeit, und die Periode des Ausleihens, an.
- Der Server prüft die Gültigkeit der angeforderten Leih-Periode und endet mit einem Fehler, wenn die Periode nicht gültig ist. Ein Ausleihen für eine ausgeliehene Kopie kann nicht über die Periode der originalen Ausleihung an den Server hinaus verlängert werden. Die Verwahrungsstellen führen gemeinsame Transaktionsschritte durch.
- Der Server überträgt die angeforderten Inhalte und Daten zu dem Anforderer. Falls ein nächster Satz von Rechten (Next-Set-Of-Rights) geliefert worden ist, werden solche Rechte als die Rechte für die Arbeit

übertragen. Ansonsten werden die Rechte des Originals übertragen, wie modifiziert ist, um die Leih-Periode wiederzugeben.

• Der Anforderer zeichnet die digitalen Arbeitsinhalte, Daten, Benutzungsrechte und Leih-Periode auf und speichert die Arbeit.

• Der Server aktualisiert die Benutzungsrechte-Information in der digitalen Arbeit, um die Zahl von Kopien, die ausgeliehen ist, wiederzugeben.

• Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

• Der Server aktualisiert die Benutzungsrechte-Daten für die digitale Arbeit. Dies kann eine Benutzung der Arbeit ausschließen, bis sie von dem Ausleihen zurückgeführt ist. Der Benutzer auf der Anforderer-Plattform kann nun die übertragenen Kopien der digitalen Arbeit verwenden. Ein Benutzer, der auf die originale Verwahrungsstelle zugreift, kann nicht die digitale Arbeit verwenden, ohne dass dort Kopien verbleiben. Dasjenige, was als nächstes auftritt, hängt von der Reihenfolge der Ereignisse über die Zeit ab.

Fall 1.

[0190] Falls die Zeit der Ausleihperiode noch nicht abgelaufen ist und der Anforderer die Anforderung einer Rückführ-Nachricht schickt.

• Die Rückführ-Nachricht umfasst die Anforderer-Identifikation, und die Transaktions-ID.

• Der Server erniedrigt das Feld der Kopien, die in Benutzung sind, um die Zahl der Kopien, die zurückgeführt wurden (falls die Anzahl von digitalen Arbeiten zurückgeführt sind, größer als die Zahl ist, die tatsächlich betroffen ist, wird dies als ein Fehler betrachtet.) Dieser Schritt kann nun die Arbeit an dem Server für andere Benutzer verfügbar machen.

• Der Anforderer deaktiviert seine Kopien und entfernt die Inhalte von seinem Speicher.

Fall 2.

[0191] Falls die Zeit der Ausleihperiode erschöpft ist und der Anforderer noch nicht bis jetzt eine Rückführ-Nachricht geschickt hat.

• Der Server erniedrigt das Feld der Kopien, die in Benutzung sind, um die Zahl von digitalen Arbeiten, die betroffen waren.

• Der Anforderer deaktiviert automatisch seine Kopien der digitalen Arbeit. Er bestimmt alle momentanen Benutzungen und löscht die digitalen Arbeitskopien von dem Speicher. Eine Frage ist diejenige, warum ein Anforderer immer eine Arbeit früher als die Periode des Ausleihens zurückführen würde, da sie automatisch immer zurückgeführt werden würde. Ein Grund für eine frühe Rückführung ist diejenige, dass eine berechnete Gebühr vorhanden ist, die die Kosten des Ausleihens bestimmt. Ein frühes Zurückführen kann diese Gebühr verringern.

Die Abspiel-Transaktion

[0192] Eine Abspiel-Transaktion ist eine Anforderung, die Inhalte einer Anforderung zu verwenden. Typischerweise ist es, eine Arbeit ”abzuspielen”, dasjenige, die digitale Arbeit über dieselbe Art eines Wandlers, wie beispielsweise eines Lautsprechers oder einer Anzeigevorrichtung, zu schicken. Die Anforderung bringt die Absicht mit sich, dass die Inhalte nicht digital zu irgendeinem anderen System kommuniziert werden. Zum Beispiel werden sie nicht zu einem Drucker geschickt werden, auf irgendeinem digitalen Medium aufgezeichnet werden, nach der Transaktion beibehalten werden oder zu einer anderen Verwahrungsstelle geschickt werden.

[0193] Dieser Ausdruck ”Abspielen” (”play”) steht natürlich für Bespiele ähnlich Abspielen einer Musik, Abspielen eines Films oder Abspielen eines Videospiels. Die allgemeine Form einer Abspieleinrichtung, das bedeutet ein ”Abspielgerät” (”Player”), wird dazu verwendet, die digitale Arbeit zu benutzen. Allerdings umfasst der Ausdruck ”abspielen” alle Medien und Arten von Aufzeichnungen. Demzufolge bedeutet, wenn jemand eine digitale Arbeit ”abspielen” würde, dies, sie für ein Lesen zu gestalten, oder ein Computerprogramm abzuspielen, was bedeutet, es auszuführen. Für ein digitales Ticket würde das Abspielgerät ein Digital-Ticket-Agent sein.

• Der Anforderer schickt dem Server eine Nachricht, die Abspiel-Transaktion zu initiieren. Diese Nachricht zeigt die Arbeit an, die abgespielt werden soll, die Version des Abspielrechts, die in der Transaktion verwendet werden soll, die Identität des Abspielgeräts, das verwendet werden soll, und die Datei-Daten für die Arbeit.

• Der Server prüft die Gültigkeit der Abspielgeräte-Identifikation und die Kompatibilität der Abspielgeräte-Identifikation mit der Abspielgeräte-Spezifikation in dem Recht. Sie endet mit einem Fehler, falls diese nicht erfüllt sind.

• Die Verwahrungsstellen führen die gemeinsamen Öffnungs-Transaktions-Schritte durch.

- Der Server und der Anforderer lesen und schreiben die Blöcke der Daten, wie sie durch das Abspielgerät angefordert sind, entsprechend dem Übertragungs-Protokoll. Der Anforderer spielt die Arbeitsinhalte, unter Verwendung des Abspielgeräts, ab.
- Wenn das Abspielgerät fertig ist, entfernen das Abspielgerät und der Anforderer die Inhalte von deren Speicher.
- Die Verwahrungsstellen führen gemeinsame, schließende Transaktions-Schritte durch.

Die Druck-Transaktion

[0194] Eine Druck-Transaktion ist eine Anforderung, die Inhalte der Arbeit für den Zweck, diese auf einem ”Drucker” zu gestalten, zu erhalten. Hier wird der Ausdruck ”Drucker” dazu verwendet, den üblichen Fall eines Schreibens mit Tinte auf Papier zu umfassen. Allerdings ist der Schlüssel-Aspekt eines ”Druckens” in der Benutzung hier des Ausdrucks derjenige, dass er eine Kopie der digitalen Arbeit an einer Stelle außerhalb des Schutzes von Benutzungsrechten herstellt. Wie bei allen Rechten kann dies bestimmte Autorisierungs-Zertifikate erfordern.

[0195] Wenn einmal eine digitale Arbeit gedruckt ist, werden der Herausgeber und der Benutzer durch das gebunden, was auch immer Copyright-Rechte tatsächlich sind. Allerdings bewegt ein Drucken die Inhalte außerhalb der Kontrolle von Verwahrungsstellen. Zum Beispiel kann, ohne irgendwelche anderen Zwangsmechanismen, wenn einmal eine digitale Arbeit auf Papier gedruckt ist, sie auf gewöhnlichen Fotokopiermaschinen ohne eine Intervention durch eine Verwahrungsstelle, um Benutzungsgebühren einzusammeln, kopiert werden. Wenn der Drucker zu einer digitalen Platte bzw. Disk zugelassen wird, dann befindet sich diese digitale Kopie außerhalb der Kontrolle von Benutzungsrechten. Sowohl der Erzeuger als auch der Benutzer kennen dies, obwohl der Erzeuger bzw. Urheber nicht notwendigerweise seine stillschweigende Zustimmung zu einem solchen Kopieren gibt, was Copyright-Gesetze verletzen kann.

- Der Anforderer schickt dem Server eine Nachricht, um eine Druck-Transaktion zu initiieren. Diese Nachricht zeigt die Arbeit an, die abgespielt werden soll, die Identität des Druckers, der verwendet werden soll, die Datei-Dateien für die Arbeit und die Zahl von Kopien in der Anforderung.
- Der Server prüft die Gültigkeit der Drucker-Identifikation und die Kompatibilität der Drucker-Identifikation mit der Drucker-Spezifikation in dem Recht. Sie endet mit einem Fehler, falls diese nicht erfüllt sind.
- Die Verwahrungsstellen führen die gemeinsamen Öffnungs-Transaktions-Schritte durch.
- Der Server überträgt Blöcke von Daten entsprechend dem Übertragungs-Protokoll.
- Der Anforderer druckt die Inhalte der Arbeit, unter Verwendung des Druckers.
- Wenn der Drucker fertig ist, entfernen der Drucker und der Anforderer die Inhalte von deren Speicher.
- Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

Die Backup-Transaktion (die Sicherungs-Transaktion)

[0196] Eine Backup- bzw. Sicherungs-Transaktion ist eine Anforderung, eine Backup- bzw. Sicherungskopie einer digitalen Arbeit, als Schutz gegen einen Fehler des Mediums, herzustellen. In dem Zusammenhang mit den Verwahrungsstellen unterscheiden sich Sicherungs-Kopien von anderen Kopien auf drei Arten und Weisen: (1) sie werden unter der Steuerung einer Backup-Transaktion im Gegensatz zu einer Kopie-Transaktion erstellt, (2) sie zählen nicht als reguläre Kopien, und (3) sie sind nicht als reguläre Kopien verwendbar. Allgemein sind Backup-Kopien verschlüsselt.

[0197] Obwohl Backup-Kopien übertragen oder kopiert werden können, in Abhängigkeit von deren zugeordneten Rechten, ist die einzige Art und Weise, um sie zum Abspielen, Drucken oder zum Einfügen verwendbar zu machen, sie wiederherzustellen.

[0198] Die Ausgabe einer Backup-Operation ist sowohl eine verschlüsselte Daten-Datei, die die Inhalte und die Beschreibung einer Arbeit enthält, als auch eine Wiederherstellungs-Datei mit einem Verschlüsselungs-Schlüssel zum Wiederherstellen der verschlüsselten Inhalte. In vielen Fällen würde die verschlüsselte Daten-Datei Rechte zum ”Drucken” auf eine Disk außerhalb des Schutzsystems haben, was nur auf deren Verschlüsselung für eine Sicherheit beruht. Solche Dateien könnten irgendwo, wo es physikalisch sicher und passend ist, gespeichert werden. Die Wiederherstellungs-Datei würde in der Verwahrungsstelle gehalten werden. Diese Datei ist für de Wiederherstellung einer Backup-Kopie notwendig. Sie kann Rechte zum Übertragen zwischen Verwahrungsstellen haben.

• Der Anforderer schickt dem Server eine Nachricht, um eine Backup-Transaktion zu initiieren. Diese Nachricht zeigt die Arbeit an, die gesichert werden soll, die Version des Sicherungs- bzw. Backup-Rechts, das in der Transaktion verwendet werden soll, die Bestimmungs-Adressen-Information zum Platzieren der Backup-Kopie, die Datei-Daten für die Arbeit an.
• Die Verwahrungsstellen führen die gemeinsamen Öffnungs-Transaktions-Schritte durch.
• Der Server überträgt die angeforderten Inhalte und die Daten zu dem Anforderer. Falls ein Next-Set-Of-Rights (nächster Satz von Rechten) geliefert worden ist, werden diese Rechte als die Rechte für die Arbeit übertragen. Ansonsten wird ein Satz von Voreinstellungs-Rechten für Backup-Dateien des Originals durch den Server übertragen.
• Der Anforderer zeichnet die Arbeits-Inhalte, Daten und Benutzungsrechte auf. Er erzeugt dann einen einmaligen Schlüssel und verschlüsselt die Inhalts-Datei. Er sichert die Schlüssel-Informationen in einer Wiederherstellungs-Datei.
• Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

[0199] In einigen Fällen ist es passend, in der Lage zu sein, die große, verschlüsselte Inhalts-Datei in einem Off-Line-Speicher zu sichern, wie beispielsweise einem magneto-optischen Speichersystem oder einem magnetischen Band. Diese Erzeugung einer Nicht-Verwahrungsstellen-Archiv-Datei ist so sicher wie der Verschlüsselungsprozess. Ein solcher Nicht-Verwahrungsstellen-Archiv-Speicher wird als eine Form eines ”Druckens” angesehen und wird durch ein Druckrecht mit einem spezifizierten ”Archiv-Drucker” (”archive-printer”) gesteuert. Eine Archiv-Drucker-Vorrichtung wird so programmiert, um die Datei mit den verschlüsselten Inhalten (allerdings nicht die Entschlüsselungs-Datei) Offline in einer solchen Art und Weise zu sichern, dass sie aufgesucht werden kann.

Die Wiederherstellungs-Transaktion

[0200] Eine Wiederherstellungs-Transaktion ist eine Anforderung, eine verschlüsselte Backup-Kopie einer digitalen Arbeit in eine verwendbare Kopie umzuwandeln. Eine Wiederherstellungs-Operation ist dazu vorgesehen, verwendet zu werden, um einen katastrophalen Medien-Fehler zu kompensieren. Ähnlich aller Benutzungsrechte können Wiederherstellungs-Rechte Gebühren und Zugriffs-Tests, umfassend Autorisierungs-Prüfungen, umfassen.
• Der Anforderer schickt dem Server eine Nachricht, um eine Wiederherstellungs-Transaktion zu initiieren. Die Nachricht die Arbeit, die hergestellt werden soll, die Version des Wiederherstellungs-Rechts für die Transaktion, die Bestimmung-Adressen-Informationen zum Platzieren der Arbeit und die Datei-Daten für die Arbeit an.
• Der Server verifiziert, dass die Inhalts-Datei verfügbar ist (d. h. eine digitale Arbeit entsprechend der Anforderung ist gesichert worden). Falls dies nicht der Fall ist, beendet er die Transaktion mit einem Fehler.
• Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktionsschritte durch.
• Der Server sucht den Schlüssel von der Wiederherstellungs-Datei auf. Er entschlüsselt die Arbeits-Inhalte, die Daten und die Benutzungsrechte.
• Der Server überträgt die angeforderten Inhalte und die Daten zu dem Anforderer entsprechend dem Übertragungs-Protokoll. Falls ein nächster Satz von Rechten (Next-Set-Of-Rights) geliefert worden ist, werden solche Rechte als die Rechte für die Arbeit übertragen. Ansonsten wird ein Satz von Voreinstellungs-Rechten für Backup-Dateien des Originals durch den Server übertragen.
• Der Anforderer speichert die digitale Arbeit.
• Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

Die Lösch-Transaktion

[0201] Eine Lösch- bzw. Delete-Transaktion löscht eine digitale Arbeit oder eine Anzahl von digitalen Kopien einer Arbeit von einer Verwahrungsstelle. Praktisch würden alle digitalen Arbeiten Löschungs-Rechte haben.

[0202] • Der Anforderer schickt dem Server eine Nachricht, um eine Löschungs-Transaktion zu initiieren. Diese Nachricht zeigt die Arbeit, die gelöscht werden soll, die Version des Löschungs-Rechts für die Transaktion, an.

[0203] • Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktions-Schritte durch.

[0204] • Der Server löscht die Datei, wobei er sie von dem Datei-System löscht.

[0205] • Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

Die Directory-Transaktion

[0206] Eine Directory-Transaktion ist eine Anforderung nach Informationen über Folder, digitale Arbeiten und deren Teilen. Dies entspricht grob derselben Idee wie Schutz-Code in einem herkömmlichen Datei-System ähnlich TENEX, mit der Ausnahme, dass sie zu der vollen Leistung der Zugriffs-Spezifikation der Verwendungs-Rechte-Sprache generalisiert ist.

[0207] Die Directory-Transaktion besitzt die wichtige Rolle, Beschreibungen der Rechte und der Gebühren, die einer digitalen Arbeit zugeordnet sind, weiterzuführen. Wenn es ein Benutzer wünscht, ein Recht auszuüben, nimmt die Benutzer-Schnittstelle seiner Verwahrungsstelle implizit eine Directory-Anforderung vor, um die Versionen des Rechts, die verfügbar sind, zu bestimmen. Typischerweise werden diese dem Benutzer präsentiert – wie beispielsweise unterschiedliche Auswahlen einer Zahlung zum Ausüben eines Rechts. Demzufolge sind viele Directory-Transaktionen zu dem Benutzer hin denkbar und werden als Teil des normalen Prozesses einer Ausübung aller Rechte ausgeübt.

- Der Anforderer schickt dem Server eine Nachricht, um eine Directory-Transaktion zu initiieren. Diese Nachricht zeigt die Datei oder den Folder an, das bedeutet die Wurzel (root) der Directory-Anforderung und die Version des Directory-Rechts, das für die Transaktion verwendet wird.
- Der Server verifiziert, dass die Information für den Anforderer zugänglich sind. Insbesondere führt er die Namen irgendwelcher Dateien zurück, die einen HIDE-NAME Status in deren Directory-Spezifikationen haben und führt nicht die Teile irgendwelcher Folder oder Dateien zurück, die HIDE-PARTS in deren Spezifikation haben. Falls die Informationen nicht zugänglich sind, beendet der Server die Transaktion mit einem Fehler.
- Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktions-Schritte durch.
- Der Server schickt die angeforderten Daten zu dem Anforderer entsprechend dem Übertragungs-Protokoll.
- Der Anforderer zeichnet die Daten auf.
- Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

Die Folder-Transaktion

[0208] Eine Folder-Transaktion ist eine Anforderung, einen Folder zu erzeugen oder umzubenennen, oder eine Arbeit zwischen Foldern zu bewegen. Zusammen mit Directory-Rights, steuern Folder-Rights den Grad, indem auf eine Organisation einer Verwahrungsstelle zugegriffen oder von einer anderen Verwahrungsstelle modifiziert werden kann.

- Der Anforderer schickt dem Server eine Nachricht, um eine Folder-Transaktion zu initiieren. Diese Nachricht zeigt dem Folder an, das bedeutet den Ursprung der Folder-Anforderung, die Version des Holder-Rechts für die Transaktion, eine Operation und Daten. Die Operation kann eine einer erzeugenden, umbenennenden und bewegenden Datei sein. Die Daten sind die Spezifikationen, die für die Operationen erforderlich sind, wie beispielsweise eine Spezifikation eines Folders oder einer digitalen Arbeit und eines Namens.
- Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktions-Schritte durch.
- Der Server führt die angeforderte Operation durch – Erzeugen eines Folders, Umbenennung eines Folders oder Bewegen einer Arbeit zwischen Foldern.
- Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

Die Extrahier-Transaktion

[0209] Eine Extrahier-Transaktion ist eine Anforderung, einen Teil einer digitalen Arbeit zu kopieren und eine neue Arbeit, die sie enthält, zu erzeugen. Die Extraktions-Operation unterscheidet sich von einem Kopieren dahingehend, dass sie dazu verwendet werden kann, einen Teil einer digitalen Arbeit von d-Blöcken oder Mänteln, die zusätzliche Restriktionen oder Gebühren darauf auferlegen, zu separieren. Die Extrahier-Operation unterscheidet sich von der Editier-Operation dahingehend, dass sie nicht die Inhalte einer Arbeit ändert, sondern sie nur d-Blöcke einbettet. Eine Fraktion erzeugt eine neue, digitale Arbeit.

- Der Anforderer schickt dem Server eine Nachricht, um eine Extrahier-Transaktion zu initiieren. Diese Nachricht zeigt den Teil der Arbeit, der extrahiert werden soll, die Version des Extrahier-Rechts, das in der Transaktion verwendet werden soll, die Bestimmungs-Adressen-Informationen zum Platzieren des Teils als eine neue Arbeit, die Datei-Daten für die Arbeit und die Zahl von Kopien, die betroffen sind, an.
- Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktions-Schritte durch.
- Der Server überträgt die angeforderten Inhalte und die Daten zu dem Anforderer entsprechend dem Übertragungs-Protokoll. Falls ein nächster Satz von Rechten (Next-Set-Of-Rights) geliefert worden ist, werden solche Rechte als die Rechte für die neue Arbeit übertragen. Ansonsten werden die Rechte des Originals

übertragen. Das Kopie-Zähl-Feld für dieses Recht wird auf die Zahl von Kopien, die angefordert sind, gesetzt.

• Der Anforderer zeichnet die Inhalte, Daten und Benutzungsrechte auf und speichert die Arbeit. Er zeichnet die Daten und die Zeit, zu der die neue Arbeit vorgenommen wurde, in den Eigenschaften der Arbeit auf.

• Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

Die eingebettete Transaktion

[0210] Eine eingebettete Transaktion ist eine Anforderung, eine Maßnahme vorzunehmen, dass eine digitale Arbeit ein Teil einer anderen digitalen Arbeit wird, oder einen Mantel-d-Block hinzuzufügen, um das Hinzufügen von Gebühren durch einen Distributor der Arbeit zu ermöglichen.

• Der Anforderer schickt dem Server eine Nachricht, um eine eingebettete Transaktion zu initiieren. Diese Nachricht zeigt die Arbeit, die eingebettet werden soll, die Version des eingebetteten Rechts, das in der Transaktion verwendet werden soll, die Bestimungs-Adressen-Informationen zum Platzieren des Teils als eine Arbeit, die Datei-Daten für die Arbeit und die Zahl von Kopien, die umfasst sind, an.

• Der Server prüft die Steuer-Spezifikation für alle Rechte in dem Teil und der Bestimmung. Falls sie nicht kompatibel sind, beendet der Server die Transaktion mit einem Fehler.

• Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktions-Schritte durch.

• Der Server überträgt die angeforderten Inhalte und die Daten zu dem Anforderer entsprechend dem Übertragungs-Protokoll. Falls ein nächster Satz von Rechten (Next-Set-Of-Rights) geliefert worden ist, werden solche Rechte als die Rechte für die neue Arbeit übertragen. Ansonsten werden die Rechte des Originals übertragen. Das Kopie-Zählungs-Feld für dieses Recht wird auf die Zahl von Kopien, die angefordert sind, eingestellt.

• Der Anforderer zeichnet die Inhalte, die Daten und die Benutzungsrechte auf und bettet die Arbeit in die Bestimmungs-Datei ein.

• Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

Die Editier-Transaktion

[0211] Die Editier-Transaktion ist eine Anforderung, eine neue, digitale Arbeit durch Kopieren, Auswählen und Modifizieren von Teilen einer existierenden, digitalen Arbeit zu erstellen. Diese Operation kann tatsächlich die Inhalte einer digitalen Arbeit ändern.

[0212] Die Arten von Änderungen, die zugelassen sind, hängen von dem Prozess ab, der verwendet wird. Ähnlich der Extraktions-Operation arbeitet ein Editieren in Bezug auf Teile einer digitalen Arbeit. Im Gegensatz zu der Extrahier-Operation beeinflußt ein Editieren nicht die Rechte oder die Stelle der Arbeit. Sie ändert nur die Inhalte. Die Arten von Änderungen, die zugelassen sind, werden durch den Typ einer Spezifikation des Prozessors, spezifiziert in den Rechten, bestimmt. In der derzeit bevorzugten Ausführungsform ändert eine Editier-Transaktion die Arbeit selbst und erstellt keine neue Arbeit. Allerdings würde es eine annehmbare Variation sein, um zu bewirken, dass eine neue Kopie der Arbeit erstellt wird.

• Der Anforderer schickt dem Server eine Nachricht, um eine Editier-Transaktion zu initiieren. Diese Nachricht zeigt die Arbeit, die editiert werden soll, die Version des Editier-Rechts, die in der Transaktion verwendet werden soll, die Datei von Daten für die Arbeit (umfassend deren Größe), die Prozess-ID für den Prozess und die Zahl von Kopien, die betroffen sind, an.

• Der Server prüft die Kompatibilität der Prozess-ID, die durch den Anforderer verwendet werden soll, gegenüber irgendeiner Prozess-ID-Spezifikation in dem Recht. Falls sie nicht kompatibel sind, endet die Transaktion mit einem Fehler.

• Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktionsschritte durch.

• Der Anforderer verwendet den Prozess, um die Inhalte der digitalen Arbeit so zu ändern, wie dies erwünscht ist. (Zum Beispiel kann er Teile davon auswählen und duplizieren; er kann sie mit anderen Informationen kombinieren; oder kann Funktionen basierend auf den Informationen berechnen. Dies kann zum Editieren eines Textes, von Musik oder von Bildern führen oder irgendwelche anderen Schritte vornehmen, die beim Erzeugen einer abgeleiteten Arbeit nützlich sind.)

• Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

[0213] Die Editier-Transaktion wird dazu verwendet, einen weiten Bereich von Arten von Arbeiten abzudecken. Die Kategorie beschreibt einen Prozess, der als seine Eingabe irgendeinen Teil einer digitalen Arbeit heranzieht und dann die Eingabe in einer bestimmten Art und Weise modifiziert. Zum Beispiel würde für einen Text ein Prozess zum Editieren des Textes Editier-Rechte fordern. Ein Prozess zum ”Summieren” oder Zählen von Worten in dem Text würde auch als Editieren angesehen werden. Für eine Musik-Datei könnte

eine Verarbeitung ein Ändern des Pitch bzw. der Teilung oder des Tempos, oder Hinzufügen von Nachhall, oder igendeinen anderen Audio-Effekt, umfassen. Für digitale Video-Arbeiten würde irgendetwas, was das Bild ändert, Editier-Rechte erfordern. Beispiele würden ein Colorieren, ein Skalieren, ein Extrahieren von Standbildern bzw. -fotos, Auswählen und Kombinieren von Einzelbildern in Geschichtstafeln, Schärfermachen mit einer Signalverarbeitung, usw., sein.

[0214] Einige Erzeuger bzw. Urheber können es wünschen, die Authentizität deren Arbeit durch Einschränken der Arten von Prozessen, die in Bezug darauf durchgeführt werden können, zu schützen. Falls dort keine Editier-Rechte vorhanden sind, wird insgesamt keine Verarbeitung zugelassen. Ein Prozessor-Identifizierer kann eingeschlossen werden, um zu spezifizieren, welche Art eines Prozesses erlaubt ist. Falls kein Prozess-Identifizierer spezifiziert ist, dann können wahlweise Prozessoren verwendet werden. Zum Beispiel kann, für einen spezifischen Prozess, es ein Fotografierer wünschen, dass erlaubt wird, dass seine Fotografie verwendet wird, allerdings wünschen, dass sie nicht coloriert wird. Ein Musiker kann wünschen, eine Extrahierung von Bereichen seiner Arbeit zuzulassen, allerdings keine Änderungen in der Tonlage bzw. -folge.

Autorisierungs-Transaktionen

[0215] Es können hierbei Arten und Weisen vorhanden sein, mit denen Autorisierungs-Transaktionen definiert werden können. Nachfolgend ist die bevorzugte Weise hier diejenige, einfach sie im Hinblick auf andere Transaktionen zu definieren, die hier bereits für Verwahrungsstellen verwendet wurden. Demzufolge ist es manchmal einfach, von ”Autorisierungs-Transaktionen” zu sprechen, allerdings sind sie tatsächlich aus anderen Transaktionen aufgebaut, die die Verwahrungstellen bereits haben.

[0216] Ein Benutzungsrecht kann eine Autorisierungs-ID spezifizieren, die ein Autorisierungs-Objekt (eine digitale Arbeit in einer Datei eines Standard-Formats) identifiziert, das die Verwahrungsstelle haben muß und das sie verarbeiten muß. Die Autorisierung wird zu dem generischen Autorisierungs-(oder Ticket)Server der Verwahrungsstelle hin gegeben, die beginnt, die Autorisierung zu interpretieren.

[0217] Wie früher beschrieben ist, enthält die Autorisierung einen Server-Identifizierer, der nur der generische Autorisierungs-Server sein kann oder irgendein anderer Server sein kann. Wenn ein entfernter Autorisierungs-Server erforderlich ist, muß er eine digitale Adresse enthalten. Er kann auch ein digitales Zertifikat enthalten.

[0218] Wenn ein entfernter Autorisierungs-Server erforderlich ist, dann führt der Autorisierungs-Prozess zuerst die folgenden Schritte durch:

- Der generische Autorisierungs-Server versucht, den Kommunikationskanal einzustellen. (Falls der Kanal nicht eingestellt werden kann, dann schlägt die Autorisierung mit einem Fehler fehl.)
- Wenn der Kanal eingestellt ist, führt er einen Registrierungs-Prozess mit der entfernen Verwahrungsstelle durch. (Falls eine Registrierung fehlschlägt, dann schlägt die Autorisierung mit einem Fehler fehl.)
- Wenn eine Registrierung abgeschlossen ist, ruft der generische Autorisierungs-Server eine ”Abspiel” (”Play”) Transaktion mit der entfernten Verwahrungsstelle auf, was das Autorisierungs-Moment als die digitale Arbeit, die abgespielt werden soll, zuführt, und den entfernten Autorisierungs-Server (ein Programm) als die ”Abspieleinrichtung” (”Player”) aufruft. (Falls das Abspielgerät nicht gefunden werden kann oder einen bestimmten anderen Fehler besitzt, dann schlägt die Autorisierung mit einem Fehler fehl.)
- Der Autorisierungs-Server ”spielt” dann die Autorisierung ab. Diese umfasst eine Entschlüsselung davon unter Verwendung entweder des öffentlichen Schlüssels der Master-Verwahrungsstelle, die das Zertifikat herausgegeben hat, oder des Sitzungs-Schlüssels von der Verwahrungsstelle, die sie übertragen hat. Der Autorisierungs-Server führt dann verschiedene Tests durch. Diese Tests variieren entsprechend dem Autorisierungs-Server. Sie umfassen solche Schritte wie eine prüfende Maßnahme und Gültigkeits-Daten der Autorisierung und prüfen irgendwelche Hot-Lists von bekannten, ungültigen Autorisierungen. Der Autorisierungs-Server kann ein Ausführen irgendwelcher anderer Transaktionen an der Verwahrungsstelle ebenso erfordern, wie beispielsweise Prüfen von Directories, Veranlassen, dass eine bestimmte Person ein Passwort übermittelt, oder Abspielen einer bestimmten, anderen digitalen Arbeit. Sie kann auch einen bestimmten, speziellen Prozess zum Prüfen von Informationen über die Stellen oder derzeitige Ereignisse aufrufen. Das ”Script” für solche Schritte ist innerhalb des Autorisierungs-Servers enthalten.
- Falls alle erforderlichen Schritte zufriedenstellend vorgenommen sind, schließt der Autorisierungs-Server die Transaktion normalerweise ab, signalisierend, dass die Autorisierung erteilt ist.

Die Installierungs-Transaktion

[0219] Eine Installierungs-Transaktion ist eine Anforderung, eine digitale Arbeit als laufbare Software auf einer Verwahrungsstelle zu installieren. In einem typischen Fall ist die Verwahrungsstelle des Anforderers eine gestaltende Verwahrungsstelle und die Software würde eine neue Art oder eine neue Version eines Abspielers sein. Auch würde in einem typischen Fall die Software zu dem Datei-System der Verwahrungsstelle des Anforderers hin kopiert werden, bevor sie installiert wird.

- Der Anforderer schickt dem Server eine Installier-Nachricht. Diese Nachricht zeigt die Arbeit an, die installiert werden muß, die Version des Installier-Rechts, das aufgerufen wird, und die Datei-Daten für die Arbeit (umfassend deren Größe).
- Die Verwahrungsstellen führen gemeinsame, öffnende Transaktions-Schritte durch.
- Der Anforderer extrahiert eine Kopie des digitalen Zertifikats für die Software. Falls das Zertifikat nicht gefunden werden kann oder die Master-Verwahrungsstelle für das Zertifikat nicht dem Anforderer bekannt ist, endet die Transaktion mit einem Fehler.
- Der Anforderer entschlüsselt das digitale Zertifikat unter Verwendung des öffentlichen Schlüssels der Master-Verwahrungsstelle, die Identität des Lieferanten und des Urhebers, einen Schlüssel zum Entschlüsseln der Software, die Kompatibilitäts-Formationen und einen Manipulier-Prüf-Code. (Dieser Schritt zertifiziert die Software.)
- Der Anforderer entschlüsselt die Software unter Verwendung des Schlüssels von dem Zertifikat und berechnet einen Prüf-Code darauf unter Verwendung einer Ein-Wege-Kontroll-Funktion. Falls der Prüf-Code den Manipulier-Prüf-Code von dem Zertifkat anpasst, endet die Installations-Transaktion mit einem Fehler. (Dieser Schritt stellt sicher, dass die Inhalte der Software, umfassend die verschiedenen Skript, nicht manipuliert worden sind.)
- Der Anforderer sucht die Instruktionen in dem Kompatibilitäts-Prüf-Skript auf und folgt diesen. Falls die Software nicht mit der Verwahrungsstelle kompatibel ist, endet die Installations-Transaktion mit einem Fehler. (Dieser Schritt prüft eine Plattform-Kompatibilität.)
- Der Anforderer sucht die Instruktionen in dem Installations-Schritt auf und folgt diesem. Falls dort ein Fehler in diesem Prozess vorhanden ist (wie beispielsweise unzureichende Ressourcen), dann endet die Transaktion mit einem Fehler. Es ist anzumerken, dass der Installations-Prozess die lauffähige Software in einer Stelle in der Verwahrungsstelle platziert, wo sie nicht länger als eine Arbeit zum Ausüben irgendwelcher Benutzungsrechte, andere als die Ausführung der Software als Teil von Verwahrungsstellen-Operationen beim Ausführen anderer Transaktionen, zugänglich ist.
- Die Verwahrungsteilen führen die gemeinsamen, schließenden Transaktions-Schritte durch.

Die Deinstallierungs-Transaktion

[0220] Eine Deinstallierungs-Transaktion ist eine Anforderung, Software von einer Verwahrungsstelle zu entfernen. Da ein nicht kontrolliertes und ein nicht korrektes Entfernen einer Software von einer Verwahrungsstelle deren verhaltensmäßige Integrität beeinflussen könnte, wird dieser Schritt kontrolliert.

- Der Anforderer schickt dem Server eine Deinstallierungs-Nachricht. Diese Nachricht zeigt die Arbeit an, die deinstalliert werden soll, die Version des Deinstallierungs-Rechts, das aufgerufen werden soll, und die Datei-Daten für die Arbeit (umfassend deren Größe).
- Die Verwahrungsstellen führen die gemeinsamen, öffnenden Transaktions-Schritte durch.
- Der Anforderer extrahiert eine Kopie des digitalen Zertifikats für die Software. Falls das Zertifikat nicht gefunden werden kann oder die Master-Verwahrungsstelle für das Zertifikat nicht dem Anforderer bekannt ist, endet die Transaktion mit einem Fehler.
- Der Anforderer prüft, ob die Software installiert ist. Falls die Software nicht installiert ist, endet die Transaktion mit einem Fehler.
- Der Anforderer entschlüsselt das digitale Zertifikat unter Verwendung des öffentlichen Schlüssels der Master-Verwahrungsstelle, zeichnet die Identität des Lieferanten und des Urhebers, einen Schlüssel zum Entschlüsseln der Software, die Kompatibilitäts-Informationen und einen Manipulier-Prüf-Code auf. (Dieser Schritt authentisiert die Zertfikation der Software, umfassend das Skript für ein Deinstallieren davon.)
- Der Anforderer entschlüsselt die Software unter Verwendung des Schlüssels von dem Zertifikat und berechnet einen Prüf-Code darauf unter Verwendung einer Ein-Wege-Prüf-Funktion. Falls der Prüf-Code nicht den Manipulier-Prüf-Code von dem Zertifikat anpasst, endet die Installations-Transaktion mit einem Fehler. (Dieser Schritt stellt sicher, dass die Inhalte der Software, umfassend die verschlüsselten Skripte, nicht manipuliert worden sind.)

• Der Anforderer sucht die Instruktionen in dem Deinstallations-Skript auf und folgt ihnen. Falls dort ein Fehler in dem Prozess vorhanden ist (wie zum Beispiel nicht ausreichende Ressourcen), dann endet die Transaktion mit einem Fehler.
• Die Verwahrungsstellen führen die gemeinsamen, schließenden Transaktionsschritte durch.

[0221] Gemäß eines weiteren Aspektes der vorliegenden Erfindung, ein Verteilungssystem zum Verbreiten von digitalen Werken, wobei die digitalen Werke eine oder mehrere Nutzungsrechte beigefügt haben, wobei das Verteilungssystem umfasst:
eine Grammatik zum Erzeugen von Instanzen (instances) von Nutzungsrechten, welche eine Art anzeigen, gemäß der ein Besitzer eines zugeordneten digitalen Werkes das zugeordnete digitale Werk übermitteln kann;
Mittel zum Erzeugen von Nutzungsrechten aus der Grammatik;
Mittel zum Hinzufügen von erzeugten Nutzungsrechten zu einem digitalen Werk;
ein Anforderungsverwahrungsort zum Zugreifen auf digitale Werke, wobei der Anforderungsverwahrungsort ein Mittel zum Erzeugen von Nutzungsrechtetransaktionen hat, wobei jeder der Nutzungstransaktionen ein Nutzungsrecht angibt;
ein Server-Verwahrungsort zum Speichern digitaler Werke mit zugeordneten erzeugten Nutzungsrechten, wobei der Server-Verwahrungsort Mittel zum Verarbeiten von Nutzungstransaktionen von dem Anforderungsverwahrungsort hat, um zu bestimmen, ob Zugriff auf ein digitales Werk gewährt werden kann.

[0222] Gemäß eines weiteren Aspektes des Verteilungssystems, wobei die Grammatik des Weiteren eine Vielzahl von Default-Bedingungen (default plurality of conditions) für eine Instanz eines Nutzungsrechtes angibt, wobei die eine oder mehrere Bedingungen erfüllt sein müssen, bevor das Nutzungsrecht ausgeführt werden kann.

[0223] Gemäß eines weiteren Aspektes des Verteilungssystems, wobei das Mittel zum Erzeugen von Nutzungsrechten aus der Grammatik des Weiteren Mittel zum Verändern der Vielzahl von Default-Bedingungen für eine Instanz eines Nutzungsrechtes umfasst.

[0224] Gemäß eines weiteren Aspektes des Verteilungssystems, wobei das digitale Werk ein Softwareprogramm ist.

[0225] Gemäß eines weiteren Aspektes des Verteilungssystems, wobei die Grammatik des Weiteren zum Erzeugen einer ersten Version eines Nutzungsrechtes und einer zweiten Version eines Nutzungsrechtes ist, wobei die erste Version einen ersten Satz von Bedingungen und die zweite Version einen zweiten Satz von Bedingungen umfasst.

[0226] Gemäß eines weiteren Aspektes der vorliegenden Erfindung, ein computerbasiertes System zum Steuern der Verbreitung und Benutzung von digitalen Werken, welches umfasst:
eine Nutzungsrechtegrammatik zum Erzeugen von Instanzen (instances) von Nutzungsrechten, welche definieren, wie ein digitales Werk genutzt oder verbreitet werden kann, wobei die Nutzungsrechtegrammatik eine erste Vielzahl von Grammatikelementen zum Definieren von Übermittlungsnutzungsrechten und eine zweite Vielzahl von Grammatikelementen zum Definieren von Wiedergabenutzungsrechten (rendering usage rights) umfasst;
Mittel zum Hinzufügen von Nutzungsrechten zu digitalen Werken;
eine Vielzahl von Verwahrungsorten zum Speichern und Austauschen von digitalen Werken, wobei jedes der Vielzahl von Verwahrungsorten umfasst:
Mittel zum Speichern von digitalen Werken und deren hinzugefügten Nutzungsrechten;
Transaktionsverarbeitungsmittel, welches eine Anforderungsbetriebsart und eine Server-Betriebsart hat, wobei die Anforderungsbetriebsart zum Anfordern von Zugriff auf ein angefragtes digitales Werk ist, wobei die Anfrage ein Nutzungsrecht angibt, und wobei die Server-Betriebsart zum Verarbeiten von Zugriffsanfragen auf das angefragte digitale Werk ist, basierend auf dem Nutzungsrecht, welches in der Anfrage angegeben ist und den Nutzungsrechten, welche zu dem angefragten digitalen Werk hinzugefügt sind; und
ein Verbindungsmittel zum Verbinden zu einem anderen aus der Vielzahl von Verwahrungsorten über ein Kommunikationsmedium.

[0227] Gemäß eines weiteren Aspektes des computerbasierten Systems zum Steuern der Verbreitung und Benutzung von digitalen Werken, wobei die erste Vielzahl von Grammatikelementen umfasst:
ein Leih-Grammatikelement (loan grammar element) zum Ermöglichen, dass ein digitales Werk zu einem anderen Verwahrungsort ausgeliehen werden kann;

ein Kopier-Grammatikelement zum Ermöglichen, dass eine Kopie eines digitalen Werkes gemacht und zu einem anderen Verwahrungsort übermittelt werden kann; und
ein Übermittlungs-Grammatikelement zum Ermöglichen, dass ein digitales Werk zu einem anderen Verwahrungsort übermittelt werden kann.

[0228] Gemäß eines weiteren Aspektes des computerbasierten Systems zum Steuern der Verbreitung und Benutzung von digitalen Werken, wobei die zweite Vielzahl von Grammatikelementen umfasst:
ein Wiedergabe-Grammatikelement (play grammar element) zum Ermöglichen, dass ein digitales Werk mit einer angegebenen Klasse von Wiedergabegeräten wiedergegeben werden kann; und
ein Druck-Grammatikelement zum Ermöglichen, dass ein digitales Werk mit einer angegebenen Klasse von Druckergeräten gedruckt werden kann.

[0229] Gemäß eines weiteren Aspektes des computerbasierten Systems zum Steuern der Verbreitung und Benutzung von digitalen Werken, wobei die Grammatik eine oder mehrere weiterer Vielzahlen von Grammatikelementen umfasst, welche zum Definieren von Dateiverwaltungsnutzungsrechten, zum Ermöglichen, dass ein digitales Werk in der Erstellung eines neuen digitalen Werkes benutzt werden kann, zum Ermöglichen einer sicheren Installation und Deinstallation von digitalen Werken, welche Softwareprogramme umfassen, oder zum Bereitstellen eines Satzes von Bedingungen, welche von einem Erzeuger angegeben sind und für jede Instanziierung eines durch ein Grammatikelement definiertes Nutzungsrechtes erfüllt sein müssen, sind.

[0230] Gemäß eines weiteren Aspektes der vorliegenden Erfindung, ein Verfahren zum Steuern der Verbreitung und Benutzung von digitalen Werken, welches die folgenden Schritte umfasst:

a) Erzeugen eines Satzes von Nutzungsrechten aus einer Nutzungsrechtegrammatik, wobei jedes der Nutzungsrechte eine bestimmte Instanz (instance) angibt, wie ein digitales Werk benutzt oder verbreitet werden kann, und wobei jedes der Nutzungsrechte eine oder mehrere Bedingungen angibt, welche erfüllt sein müssen, um das Nutzungsrecht auszuführen;
b) Hinzufügen des Satzes von Nutzungsrechten zu einem digitalen Werk;
c) Speichern eines digitalen Werkes und seines hinzugefügten Nutzungsrechte in einem ersten Verwahrungsort;
d) Initiieren, durch einen zweiten Verwahrungsort, einer Zugriffsanfrage auf das digitale Werk in dem ersten Verwahrungsort, wobei die Anfrage ein Nutzungsrecht angibt;
e) Empfangen der Anfrage von dem zweiten Verwahrungsort bei dem ersten Verwahrungsort;
f) Bestimmen, durch den ersten Verwahrungsort, ob das angegebene Nutzungsrecht zu dem digitalen Werk hinzugefügt ist;
g) Verweigern, durch den ersten Verwahrungsort, von Zugriff auf das digitale Werk, falls das angegebene Nutzungsrecht nicht zu dem digitalen Werk hinzugefügt ist;
h) Bestimmen, durch den ersten Verwahrungsort, ob durch das Nutzungsrecht angegebene Bedingungen erfüllt sind, falls das angegebene Nutzungsrecht zu dem digitalen Werk hinzugefügt ist;
i) Verweigern von Zugriff auf das digitale Werk durch den ersten Verwahrungsort, falls die Bedingungen nicht erfüllt sind;
j) Übermitteln des digitalen Werks zu dem zweiten Verwahrungsort, durch den ersten Verwahrungsort, falls die Bedingungen erfüllt sind.

Patentansprüche

1. Verfahren zum Steuern der Verbreitung und der Benutzung von digitalen Werken, wobei das Verfahren die folgenden Schritte umfasst:
a) Erzeugen von Nutzungsrechten aus einer Nutzungsrechtegrammatik, wobei jedes der Nutzungsrechte eine bestimmte Instanz angibt, wie ein digitales Werk benutzt oder verbreitet werden kann;
b) Zuordnen der Nutzungsrechte zu einem digitalen Werk;
c) Speichern des digitalen Werkes und seiner zugehörigen Nutzungsrechte in einem ersten Verwahrungsort, wobei der erste Verwahrungsort eine Server-Betriebsart besitzt, um dem ersten Verwahrungsort zu ermöglichen, Zugangsanfragen von anderen Verwahrungsorten zu digitalen Werken in Übereinstimmung mit Nutzungsrechten zu gewähren oder zu verweigern und wobei der erste Verwahrungsort eine Anforderungsbetriebsart besitzt, die dem ersten Verwahrungsort ermöglicht, Zugang zu digitalen Werken anzufordern;
d) initiieren einer Zugangsanfrage für ein digitales Werk in dem ersten Verwahrungsort, durch einen zweiten Verwahrungsort, welcher eine Anforderungsbetriebsart besitzt, die dem zweiten Verwahrungsort ermöglicht, Zugang zu digitalen Werken anzufordern, wobei die Anforderung ein Übermittlungsnutzungsrecht angibt und wobei das Übermittlungsnutzungsrecht ein Recht zum Kopieren, ein Recht zum Übertragen oder ein Recht zum Ausleihen ist;

e) Bestimmen, durch den ersten Verwahrungsort, ob das angegebene Übermittlungsbenutzungsrecht dem digitalen Werk zugeordnet ist;
f) Verweigern, durch den ersten Verwahrungsort, von Zugang zu dem digitalen Werk, falls das angegebene Übermittlungsnutzungsrecht nicht dem digitalen Werk zugeordnet ist;
g) Gewähren, durch den ersten Verwahrungsort, von Zugang zu dem digitalen Werk, falls das angegebene Übermittlungsnutzungsrecht dem digitalen Werk zugeordnet ist;
h) Übermitteln des digitalen Werkes und dessen zugeordneter Nutzungsrechte von dem ersten Verwahrungsort zu dem zweiten Verwahrungsort, wobei die Übermittlungsnutzungsrechte angeben, wie das digitale Werk benutzt werden kann und ob das digitale Werk, nachdem es zu dem zweiten Verwahrungsort übermittelt wurde, weiter verbreitet werden kann;
i) Speichern des digitalen Werkes und dessen zugehöriger Nutzungsrechte in dem zweiten Verwahrungsort;
j) der zweite Verwahrungsort des Weiteren eine Serverbetriebsart besitzt, welche dem zweiten Verwahrungsort ermöglicht, Zugangsanfragen von anderen Verwahrungsorten zu digitalen Werken in Übereinstimmung mit Nutzungsrechten zu gewähren oder zu verweigern;
k) Initiieren einer Zugangsanfrage zu dem digitalen Werk in dem zweiten Verwahrungsort, durch einen dritten Verwahrungsort, welcher eine Anforderungsbetriebsart besitzt, die dem dritten Verwahrungsort ermöglicht, Zugang zu digitalen Werken anzufordern, wobei die Anforderung ein weiteres Nutzungsrecht angibt und das weitere Nutzungsrecht eine Recht zum Rendern ist;
wobei der dritte Verwahrungsort ein Wiedergabeverwahrungsort (Rendering Repository) ist, der von einem Wiedergabesystem umfasst ist, wobei das Wiedergabesystem des Weiteren ein Renderingsystem (Rendering Engine) zum Rendern des angefragten digitalen Werkes umfasst;
wobei sich der dritte Verwahrungsort und das Renderingsystem innerhalb einer sicheren Abgrenzung befinden, innerhalb der Kommunikationen sicher sind;
l) Bestimmen, durch den zweiten Verwahrungsort, ob das angegebene weitere Nutzungsrecht dem digitalen Werk zugeordnet ist;
m) Verweigern von Zugang zu dem digitalen Werk, durch den zweiten Verwahrungsort, falls das angegebene weitere Nutzungsrecht nicht dem digitalen Werk zugeordnet ist;
n) Gewähren von Zugang zu dem digitalen Werk, durch den zweiten Verwahrungsort, und Übermitteln des digitalen Werkes an den dritten Verwahrungsort, falls das angegebene weitere Nutzungsrecht dem digitalen Werk zugeordnet ist,
wobei das digitale Werk von dem dritten Verwahrungsort nicht an einen anderen Verwahrungsort oder ein anderes System kommuniziert wird, und nachdem das Recht zum Rendern ausgeführt wurde, der digitale Inhalt nicht in dem dritten Verwahrungsort und dem Renderingsystem verwahrt wird.

2. Verfahren gemäß Anspruch 1, wobei der zweite Verwahrungsort, welcher eine Anfrage empfängt, und der dritte Verwahrungsort, welcher die Anfrage initiiert, verschiedene physikalische Geräte sind.

3. Verfahren gemäß Anspruch 1, wobei das Verfahren des Weiteren die folgenden Schritte umfasst:
a) Bestimmen, durch den zweiten Verwahrungsort, ob Bedingungen, die erfüllt sein müssen, um das Nutzungsrecht auszuführen, durch das Nutzungsrecht angegeben sind, falls das ermittelte Nutzungsrecht dem digitalen Werk zugeordnet ist;
b) Bestimmen, durch den zweiten Verwahrungsort, ob die Bedingungen erfüllt sind, falls die Bedingungen durch das Nutzungsrecht angegeben sind;
c) Verweigern von Zugang zu dem digitalen Werk, durch den zweiten Verwahrungsort, falls die Bedingungen nicht erfüllt sind;
d) Gewähren, durch den zweiten Verwahrungsort, von Zugang zu dem digitalen Werk basierend auf dem Nutzungsrecht, welches dem angeforderten digitalen Werk zugeordnet ist, falls die Bedingungen erfüllt sind.

4. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei das Nutzungsrecht in demselben physikalischen Gerät gespeichert ist, in dem das zugeordnete digitale Werk gespeichert ist.

5. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei das Nutzungsrecht und das zugehörige digitale Werk in verschiedenen physikalischen Geräten gespeichert sind.

6. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei der dritte Anforderungsverwahrungsort und der zweite Verwahrungsort, in dem ein digitales Werk gespeichert ist, verschiedene physikalische Geräte sind.

7. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei die Verwahrungsorte vertrauenswürdig sind.

8. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei mindestens einer der Verwahrungsorte ein Wiedergabeverwahrungsort (Rendering Repository) ist.

9. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei die Verwahrungsorte eine Vielzahl von Sicherheitsstufen bereitstellen.

10. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei eine Bedingung zum Ausführen eines Rechtes ist, dass der Anforderungsverwahrungsort ein Sicherheitskriterium erfüllen muss.

11. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei die Nutzungsrechte Verzeichnistransaktionen angeben.

12. Verfahren gemäß Anspruch 11, wobei Versionen von verfügbaren Rechten bestimmt werden.

13. Verfahren gemäß Anspruch 12, wobei Versionen von Rechten dem Benutzer angezeigt werden.

14. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei das digitale Werk ein Softwareprogramm ist.

15. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei das Nutzungsrecht angibt, wie ein digitales Werk, welches ein Softwareprogramm ist, ausgeführt werden kann.

16. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei das digitale Werk ein Video-Werk ist.

17. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei das digitale Werk ein Audio-Werk ist.

18. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei das digitale Werk ein Multimedia-Werk ist.

19. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei das digitale Werk ein Aktienzertifikat (Stock Certificate) ist.

20. Verfahren gemäß einem der Ansprüche 1 bis 3, wobei das digitale Werk ein Inhaberbond (Bearer Bond) ist.

21. System zum Steuern der Verbreitung und der Benutzung von digitalen Werken, welche zugeordnete Nutzungsrechte haben, wobei das System umfasst:
eine Vielzahl von Verwahrungsorten zum Speichern und Austauschen von digitalen Werken, wobei mindestens einer der Verwahrungsorte ein Anforderungsverwahrungsort, mindestens einer der Verwahrungsorte ein Server-Verwahrungsort und mindestens einer der Verwahrungsorte ein Server- und Anforderungsverwahrungsort ist,
wobei der mindestens eine Server-Verwahrungsort umfasst:
Mittel zum Speichern von digitalen Werken und deren zugeordneter Nutzungsrechte;
Transaktionsverarbeitungsmittel, welches eine Server-Betriebsart hat, die dem Verwahrungsort ermöglicht, als ein Server-Verwahrungsort zum Verarbeiten von Zugangsanfragen zu digitalen Werken zu agieren;
das Transaktionsverarbeitungsmittel des Weiteren eine Anforderungsbetriebsart besitzt, die es dem Verwahrungsort ermöglicht, als ein Anforderungsverwahrungsort zum Anfordern von Zugang zu digitalen Werken zu agieren;
Verbindungsmittel zum Verbinden mit einem anderen aus der Vielzahl von Verwahrungsorten über ein Kommunikationsmedium,
wobei der mindestens eine Anforderungsverwahrungsort umfasst:
Mittel zum Speichern von digitalen Werken;
Transaktionsverarbeitungsmittel, welche eine Anforderungsbetriebsart besitzt, die es dem Verwahrungsort ermöglicht, als ein Anforderungsverwahrungsort zum Anfordern von Zugang zu digitalen Werken zu agieren;
Verbindungsmittel zum Verbinden mit einem anderen aus der Vielzahl von Verwahrungsorten über ein Kommunikationsmedium,
wobei der mindestens eine Server- und Anforderungsverwahrungsort umfasst:
Mittel zum Speichern von digitalen Werken und deren zugeordneter Nutzungsrechte;
Transaktionsverarbeitungsmittel, welches eine Server-Betriebsart besitzt, die es dem Verwahrungsort ermöglicht, als ein Server-Verwahrungsort zum Bearbeiten von Zugangsanfragen zu digitalen Werken zu agieren;
Transaktionsverarbeitungsmittel, welches eine Anforderungsbetriebsart besitzt, die es dem Verwahrungsort ermöglicht, als ein Anforderungsverwahrungsort zum Anfordern von Zugang zu digitalen Werken zu agieren;

Verbindungsmittel zum Verbinden zu einem anderen aus der Vielzahl von Verwahrungsorten über ein Kommunikationsmedium,
wobei das System des Weiteren umfasst:
Mittel zum Erzeugen von Nutzungsrechten aus einer Grammatik, die zum Definieren von Instanzen von Nutzungsrechten geeignet ist, welche angeben, wie ein digitales Werk benutzt oder verbreitet werden kann;
Mittel zum Speichern der digitalen Werke und der Nutzungsrechte in einem Verwahrungsort;
Mittel zum Zuordnen von einem oder mehr als einem der Nutzungsrechte, welche basierend auf der Grammatik erzeugt wurden, zu digitalen Werken, wobei die Nutzungsrechte und die digitalen Werke in demselben Verwahrungsort gespeichert werden;
wobei
das System angepasst ist die Verfahrensschritte gemäß Anspruch 1 zu implementieren, wobei der mindestens eine Server-Verwahrungsort der erste Verwahrungsort ist, der mindestens eine Server- und Anforderungsverwahrungsort der zweite Verwahrungsort ist und der mindestens eine Anforderungsverwahrungsort der dritte Verwahrungsort ist;
wobei der mindestens eine Anforderungsverwahrungsort ein Wiedergabeverwahrungsort (Rendering Repository) ist, der von einem Wiedergabesystem umfasst ist, wobei das Wiedergabesystem des Weiteren ein Renderingsystem (Rendering Engine) zum Rendern des angefragten digitalen Werkes umfasst;
wobei sich der mindestens eine Anforderungsverwahrungsort und das Renderingsystem innerhalb einer sicheren Abgrenzung befinden, innerhalb der Kommunikationen sicher sind.

22. System gemäß Anspruch 21, wobei der mindestens eine Server- und Anforderungsverwahrungsort, welcher eine Anfrage von dem mindestens einen Anforderungsverwahrungsort empfängt und der mindestens eine Anforderungsverwahrungsort, welcher die Anfrage initiiert, verschiedene physikalische Geräte sind.

23. System gemäß Anspruch 21, wobei die Nutzungsrechtegrammatik (**1501**–**1525**) eine erste Vielzahl von Grammatikelementen und eine zweite Vielzahl von Grammatikelementen umfasst, wobei die erste Vielzahl von Grammatikelementen zum Definieren von Übermittlungsnutzungsrechten und die zweite Vielzahl von Grammatikelementen zum Definieren von Wiedergabenutzungsrechten (Rendering Usage Rights) ist.

24. System gemäß einem der Ansprüche 21 bis 23, wobei die Grammatik (**1501**–**1525**) des Weiteren eine Default Vielzahl von Bedingungen für eine Instanz eines Nutzungsrechtes angibt, wobei die eine oder mehreren Bedingungen erfüllt sein müssen, bevor das Nutzungsrecht ausgeführt werden kann.

25. System gemäß Anspruch 24, wobei das Mittel zum Erzeugen von Nutzungsrechten aus der Grammatik (**1501**–**1525**) des Weiteren ein Mittel zum Verändern der Default-Vielzahl von Bedingungen für eine Instanz eines Nutzungsrechtes umfasst.

26. System gemäß Anspruch 21, wobei das digitale Werk ein Softwareprogramm ist.

27. System gemäß Anspruch 21, wobei das Nutzungsrecht angibt, wie ein digitales Werk, welches ein Softwareprogramm ist, ausgeführt werden kann.

28. System gemäß Anspruch 21, wobei das digitale Werk ein Video-Werk ist.

29. System gemäß Anspruch 21, wobei das digitale Werke in Audio-Werk ist.

30. System gemäß Anspruch 21, wobei das digitale Werk ein Multimedia-Werk ist.

31. System gemäß Anspruch 21, wobei das digitale Werk ein Aktienzertifikat (Stock Certificate) ist.

32. System gemäß Anspruch 21, wobei das digitale Werk ein Inhaberbond (Bearer Bond) ist.

33. System gemäß Anspruch 21, wobei die Grammatik (**1501**–**1525**) des Weiteren zum Erzeugen einer ersten Version eines Nutzungsrechtes ist, welche einen ersten Satz von Bedingungen besitzt und zum Erzeugen einer zweiten Version des Nutzungsrechtes ist, welche einen zweiten Satz von Bedingungen besitzt.

34. System zum Steuern der Verbreitung und Benutzung von digitalen Werken gemäß Anspruch 21, wobei die erste Vielzahl von Grammatikelementen umfasst:
Leih-Grammatikelement (Loan Grammar Element) zum Ermöglichen, dass ein digitales Werk an einen anderen Verwahrungsort ausgeliehen werden kann;

ein Kopier-Grammatikelement zum Ermöglichen, dass eine Kopie eines digitalen Werkes gemacht werden kann und zu einem anderen Verwahrungsort übermittelt werden kann; und
ein Übermittlungs-Grammatikelement zum Ermöglichen, dass ein digitales Werk zu einem anderen Verwahrungsort übermittelt werden kann.

35. System zum Steuern der Verbreitung und der Benutzung von digitalen Werken gemäß Anspruch 21 oder 12, wobei die zweite Vielzahl von Grammatikelementen umfasst:
ein Wiedergabe-Grammatikelement (Play Grammar Element) zum Ermöglichen, dass ein digitales Werk mit einer bestimmten Klasse von Wiedergabegeräten wiedergegeben (gerendered) werden kann; und
ein Druck-Grammatikelement zum Ermöglichen, dass ein digitales Werk mit einer bestimmten Klasse von Druckergeräten gedruckt werden kann.

36. System zum Steuern der Verbreitung und der Benutzung von digitalen Werken gemäß einem der Ansprüche 21 und 32 bis 33, wobei die Grammatik (**1501**–**1525**) eine oder mehrere weiterer Vielzahlen von Grammatikelementen umfasst, welche zum Definieren von Dateiverwaltungsnutzungsrechten (File Management Usage Rights), zum Ermöglichen, dass ein digitales Werk zur Erzeugung eines neuen digitalen Werkes benutzt werden kann, zum Ermöglichen, dass digitale Werke, welche Softwareprogramme umfassen, sicher installiert und deinstalliert werden können, und zum Bereitstellen eines Satzes von Bedingungen, welche von einem Erzeuger angegeben sind und welche für jede Instanziierung eines Nutzungsrechtes, welches durch ein Grammatikelement definiert ist, erfüllt sein müssen, sind.

37. System gemäß Anspruch 21, wobei das Nutzungsrecht in demselben physikalischen Gerät gespeichert ist, in dem das zugeordnete digitale Werk gespeichert ist.

38. System gemäß Anspruch 21, wobei das Nutzungsrecht und das zugeordnete digitale Werk in verschiedenen physikalischen Geräten gespeichert sind.

39. Verwahrungsorte gemäß Anspruch 21, wobei der mindestens eine Anforderungsverwahrungsort und der Verwahrungsort, in dem ein digitales Werk gespeichert ist, verschiedene physikalische Geräte sind.

40. System gemäß Anspruch 21, wobei die Verwahrungsorte vertrauenswürdig sind.

41. System gemäß Anspruch 21, wobei mindestens einer der Verwahrungsorte ein Wiedergabeverwahrungsort (Rendering Repository) ist.

42. System gemäß Anspruch 21, wobei die Verwahrungsorte eine Vielzahl von Sicherheitsstufen bereitstellen.

43. System gemäß Anspruch 21, wobei eine Bedingung zum Ausführen eines Rechtes ist, dass ein Anforderungsverwahrungsort ein Sicherheitskriterium erfüllen muss.

44. System gemäß Anspruch 21, wobei die Nutzungsrechte Verzeichnistransaktionen angeben.

45. System gemäß Anspruch 44, wobei Versionen von verfügbaren Rechten bestimmt werden.

46. System gemäß Anspruch 45, wobei Versionen von Rechten dem Benutzer angezeigt werden.

Es folgen 13 Seiten Zeichnungen

Anhängende Zeichnungen

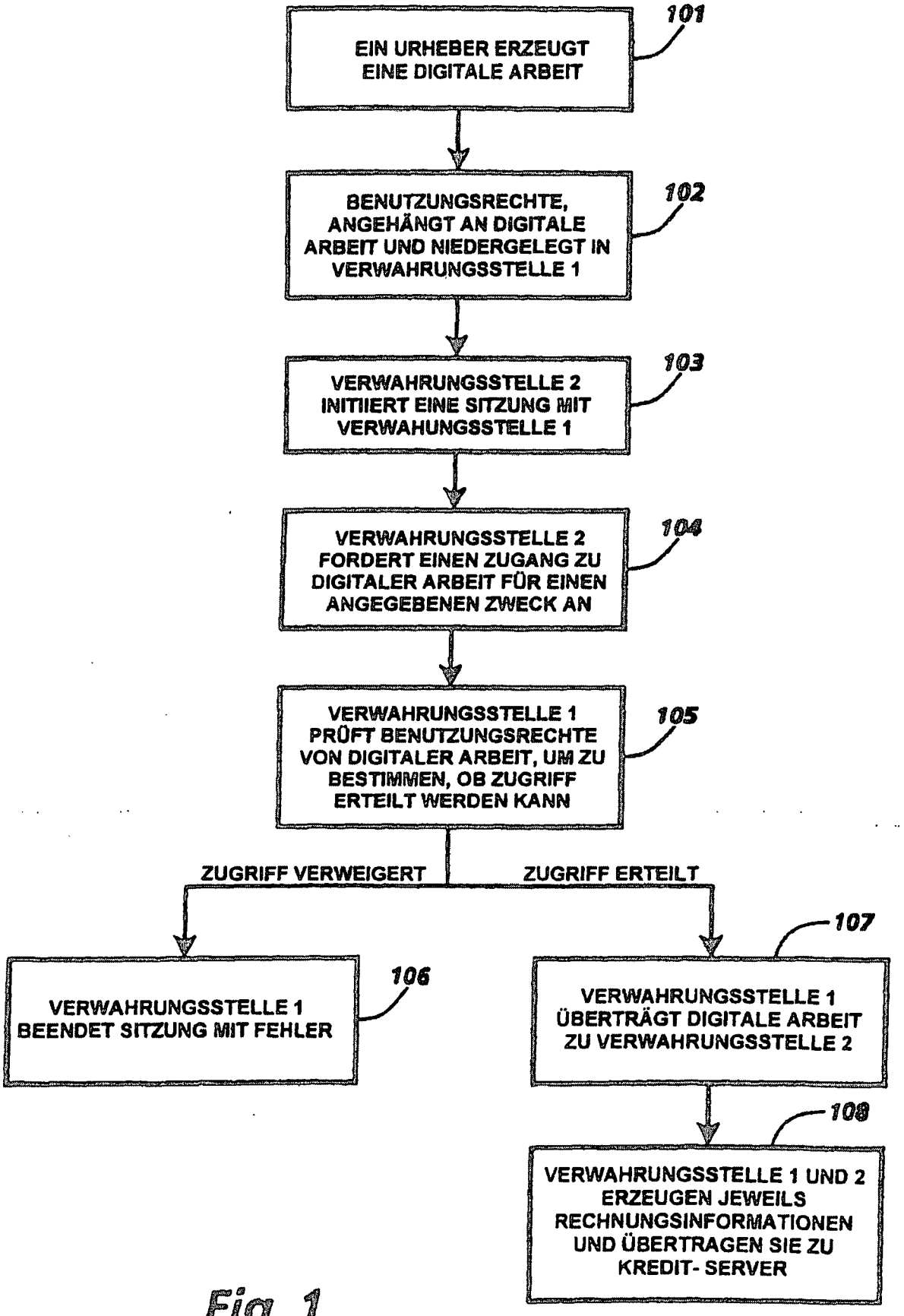

Fig. 1

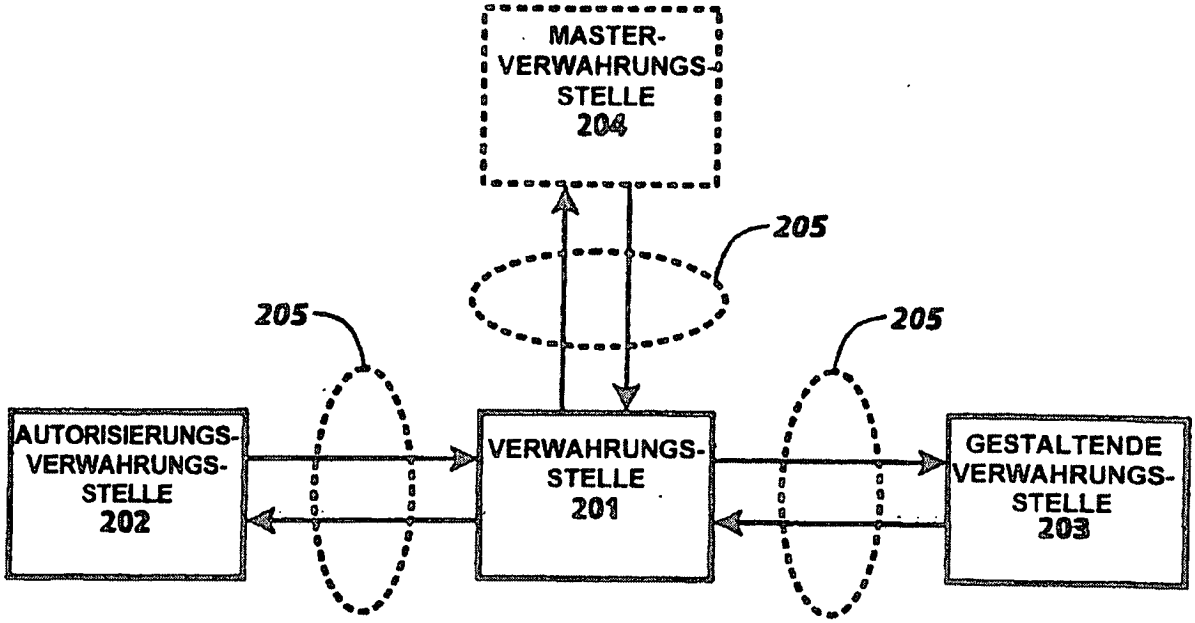
MASTER-
VERWAHRUNGS-
STELLE
204
205
205
205
AUTORISIERUNGS-
VERWAHRUNGS-
STELLE
202
VERWAHRUNGS-
STELLE
201
GESTALTENDE
VERWAHRUNGS-
STELLE
203

Fig. 2

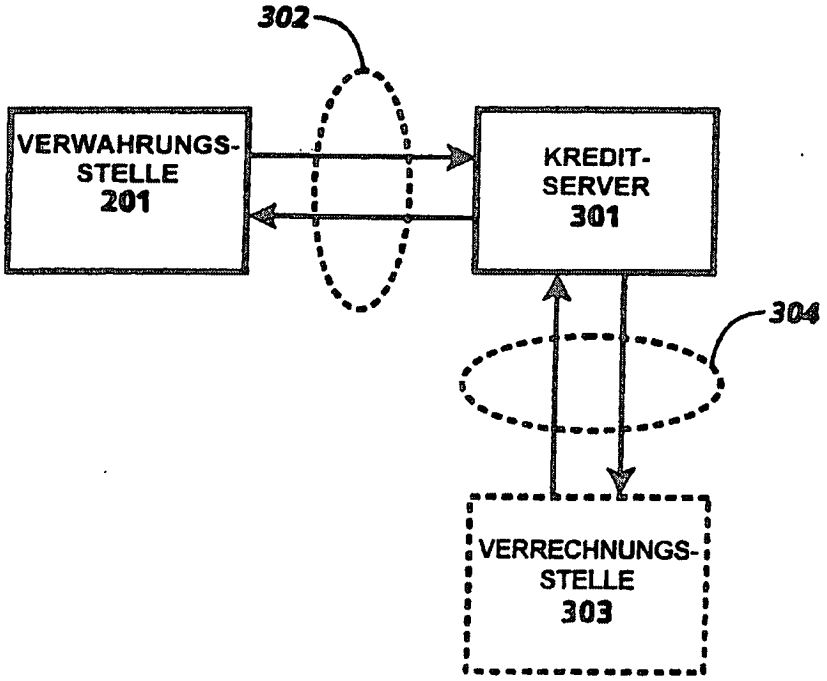
302
VERWAHRUNGS-
STELLE
201
KREDIT-
SERVER
301
304
VERRECHNUNGS-
STELLE
303

Fig. 3

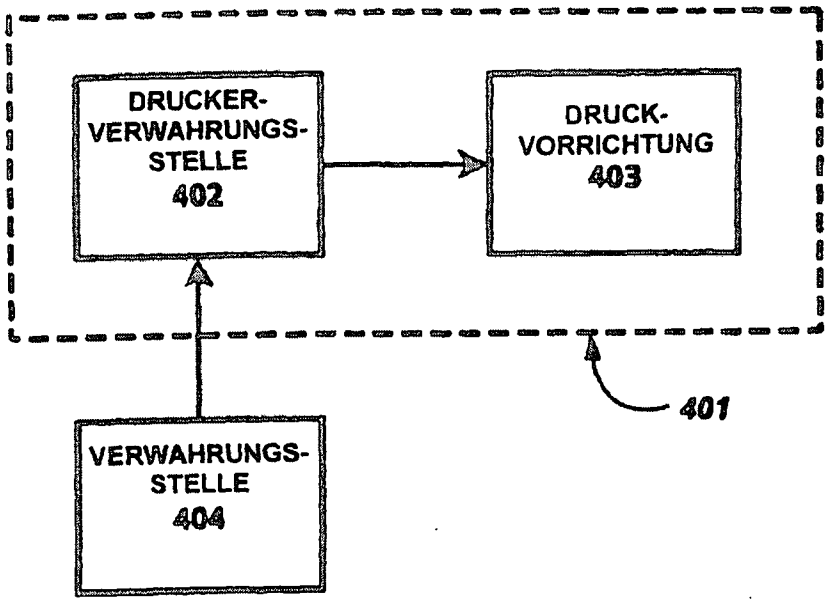
DRUCKER-VERWAHRUNGS-STELLE 402
DRUCK-VORRICHTUNG 403
401
VERWAHRUNGS-STELLE 404

Fig. 4a

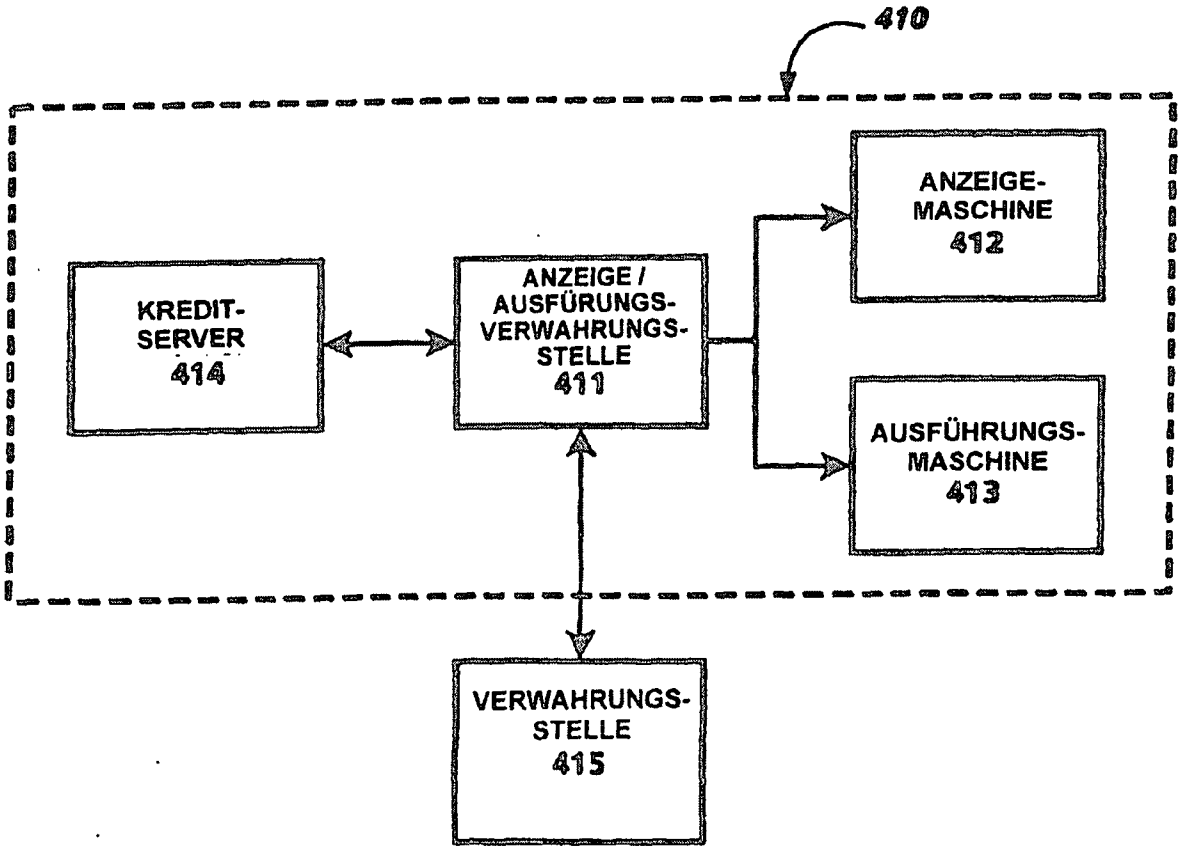
410
KREDIT-SERVER 414
ANZEIGE / AUSFÜRUNGS-VERWAHRUNGS-STELLE 411
ANZEIGE-MASCHINE 412
AUSFÜHRUNGS-MASCHINE 413
VERWAHRUNGS-STELLE 415

Fig. 4b

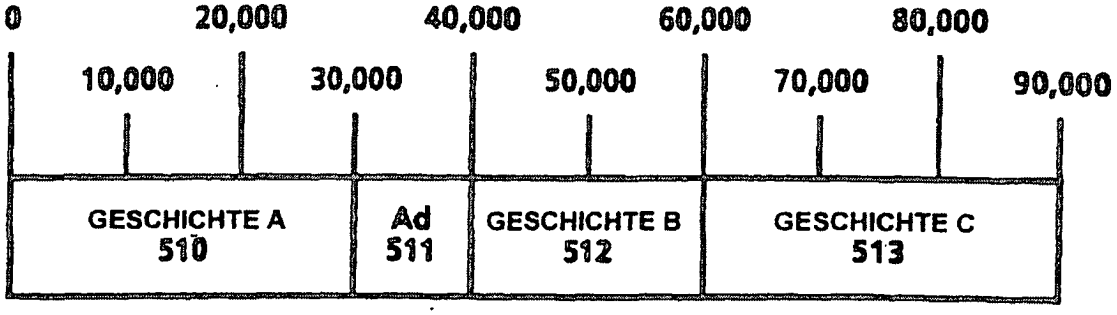
0
20,000
40,000
60,000
80,000
10,000
30,000
50,000
70,000
90,000
GESCHICHTE A
510
Ad
511
GESCHICHTE B
512
GESCHICHTE C
513

Fig. 5

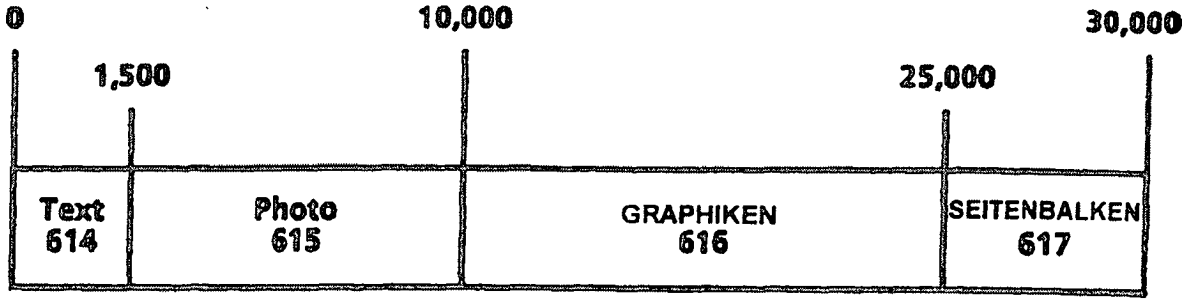
0
10,000
30,000
1,500
25,000
Text
614
Photo
615
GRAPHIKEN
616
SEITENBALKEN
617

Fig. 6

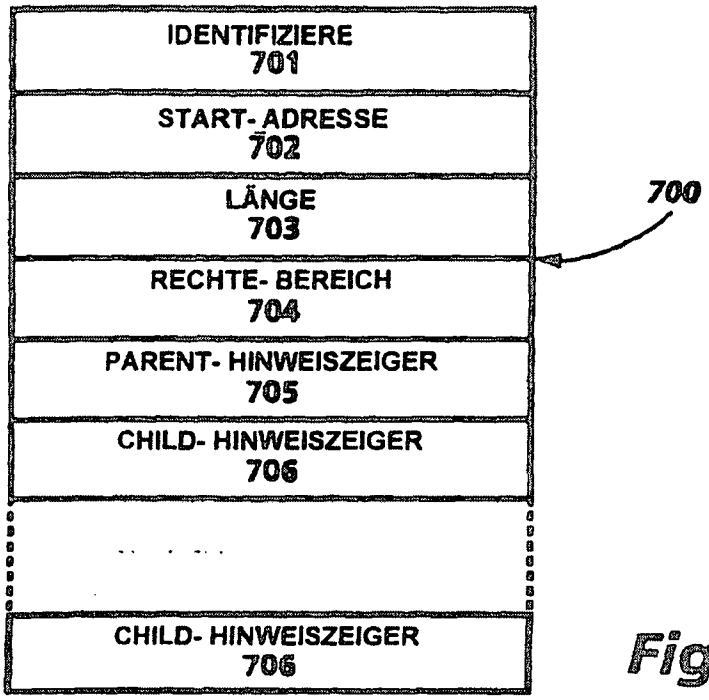

Fig. 7

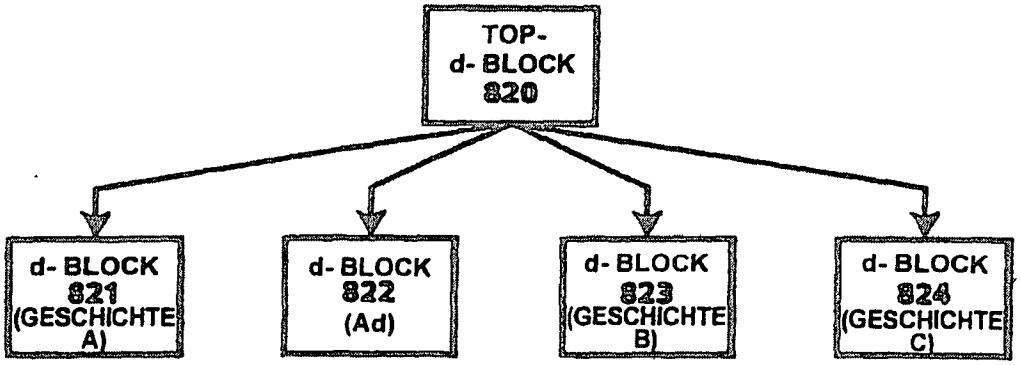

Fig. 8

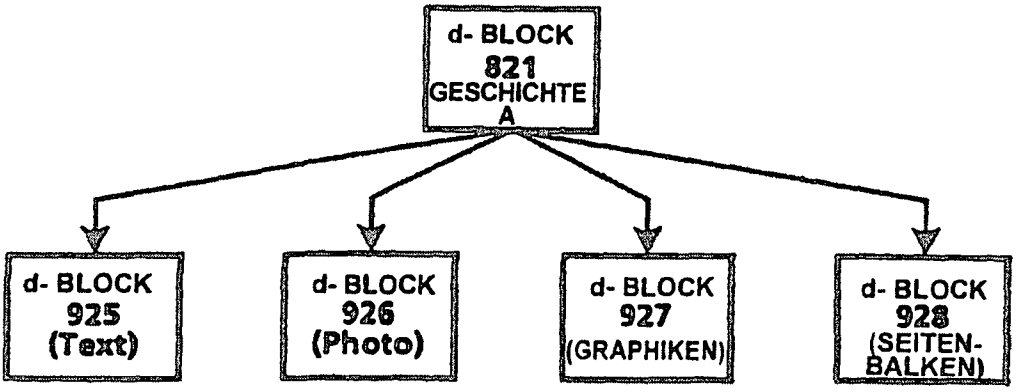

Fig. 9

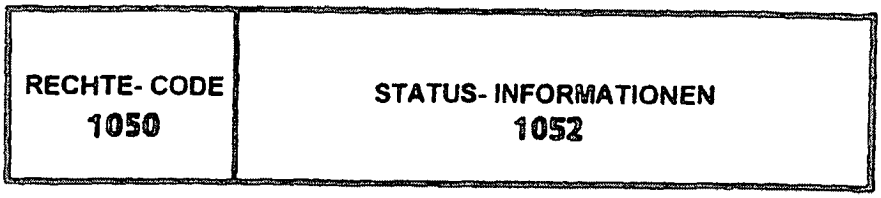
RECHTE- CODE
1050
STATUS- INFORMATIONEN
1052

Fig.10

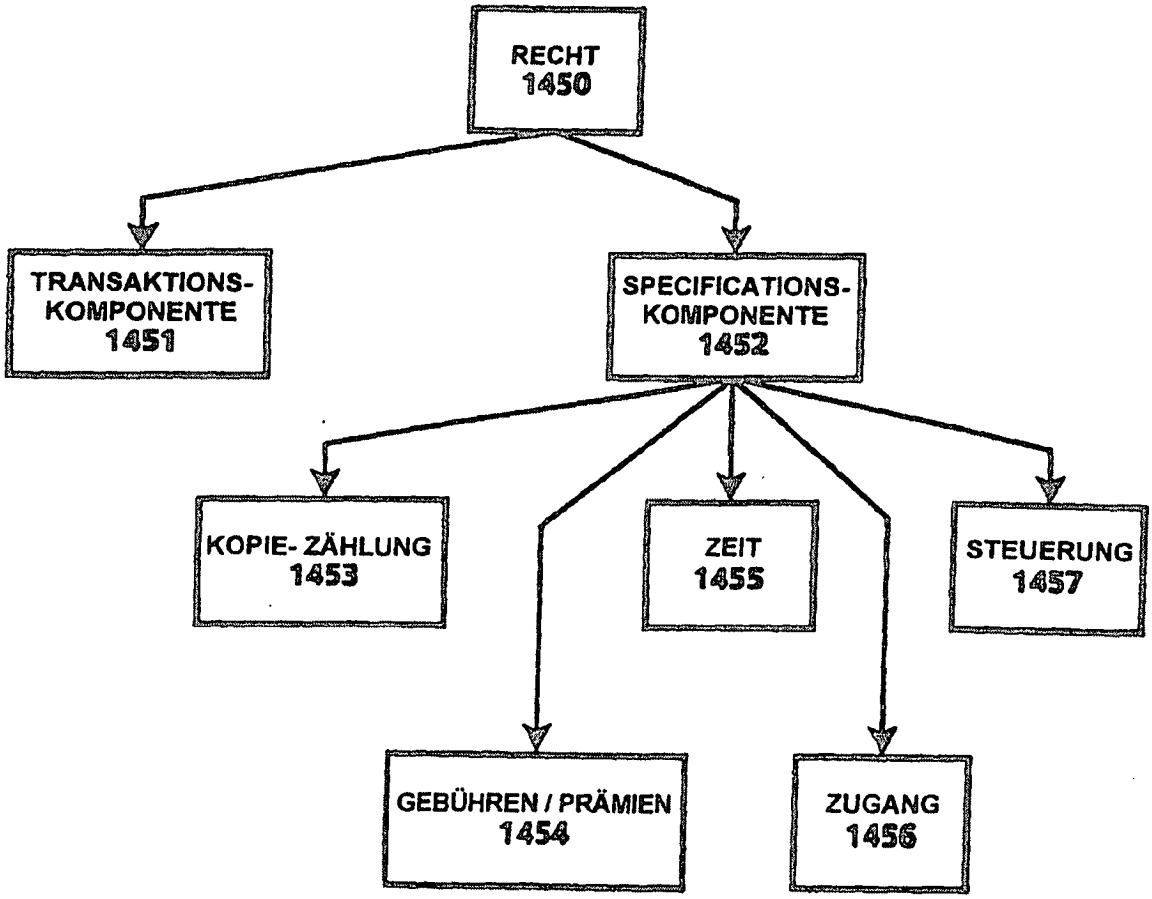
RECHT
1450
TRANSAKTIONS-
KOMPONENTE
1451
SPECIFICATIONS-
KOMPONENTE
1452
KOPIE- ZÄHLUNG
1453
GEBÜHREN / PRÄMIEN
1454
ZEIT
1455
ZUGANG
1456
STEUERUNG
1457

Fig.14

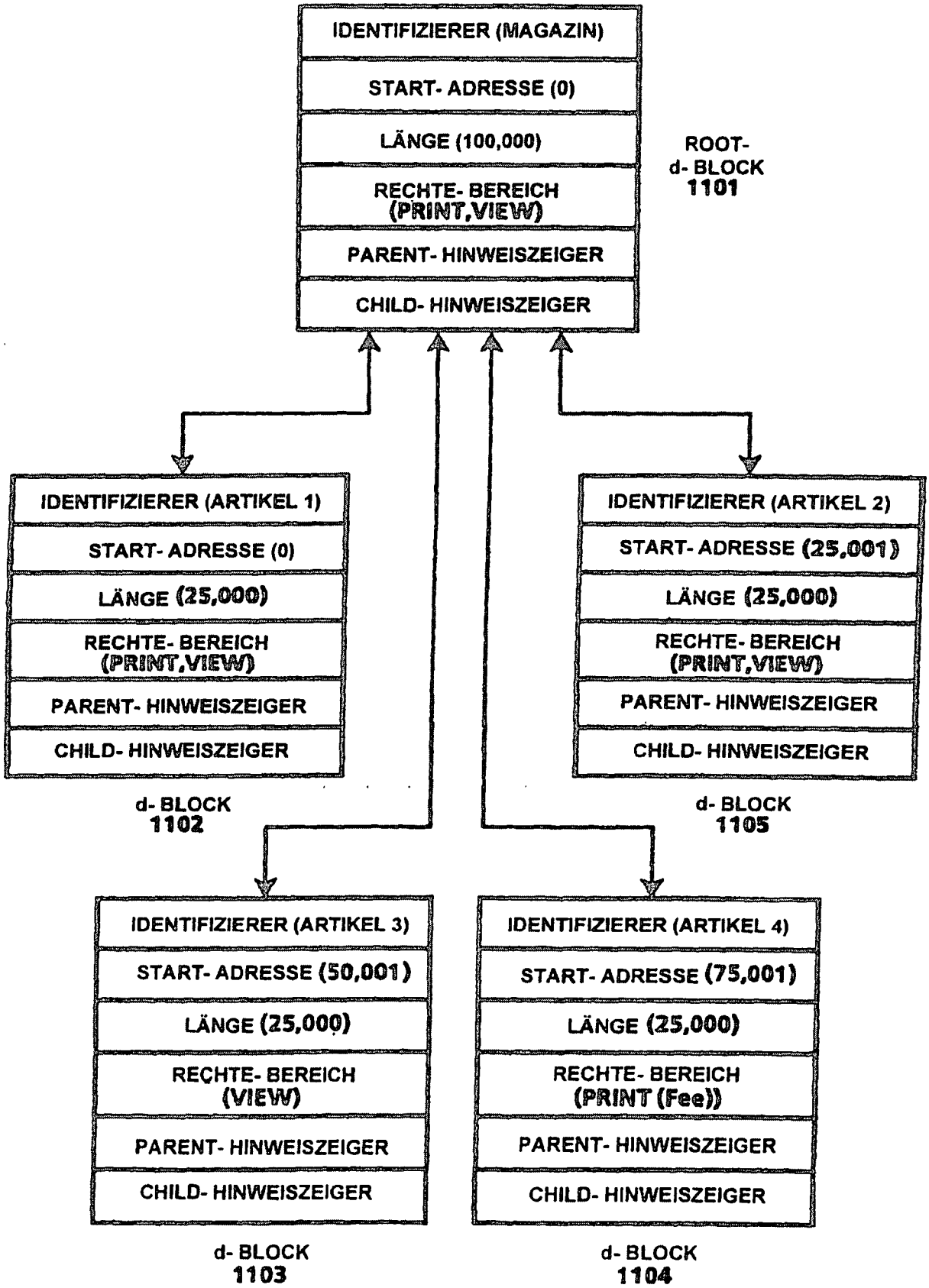
IDENTIFIZIERER (MAGAZIN)
START- ADRESSE (0)
LÄNGE (100,000)
RECHTE- BEREICH (PRINT,VIEW)
PARENT- HINWEISZEIGER
CHILD- HINWEISZEIGER
ROOT- d- BLOCK 1101
IDENTIFIZIERER (ARTIKEL 1)
START- ADRESSE (0)
LÄNGE (25,000)
RECHTE- BEREICH (PRINT,VIEW)
PARENT- HINWEISZEIGER
CHILD- HINWEISZEIGER
d- BLOCK 1102
IDENTIFIZIERER (ARTIKEL 2)
START- ADRESSE (25,001)
LÄNGE (25,000)
RECHTE- BEREICH (PRINT,VIEW)
PARENT- HINWEISZEIGER
CHILD- HINWEISZEIGER
d- BLOCK 1105
IDENTIFIZIERER (ARTIKEL 3)
START- ADRESSE (50,001)
LÄNGE (25,000)
RECHTE- BEREICH (VIEW)
PARENT- HINWEISZEIGER
CHILD- HINWEISZEIGER
d- BLOCK 1103
IDENTIFIZIERER (ARTIKEL 4)
START- ADRESSE (75,001)
LÄNGE (25,000)
RECHTE- BEREICH (PRINT (Fee))
PARENT- HINWEISZEIGER
CHILD- HINWEISZEIGER
d- BLOCK 1104

Fig.11

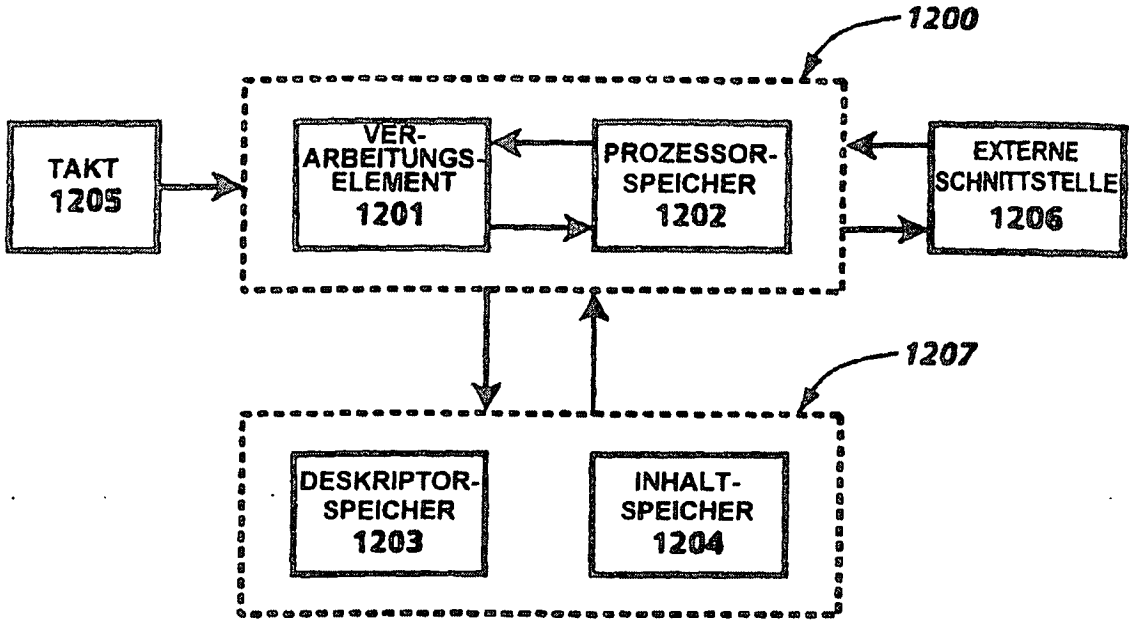
1200
TAKT
1205
VER-
ARBEITUNGS-
ELEMENT
1201
PROZESSOR-
SPEICHER
1202
EXTERNE
SCHNITTSTELLE
1206
1207
DESKRIPTOR-
SPEICHER
1203
INHALT-
SPEICHER
1204

Fig.12

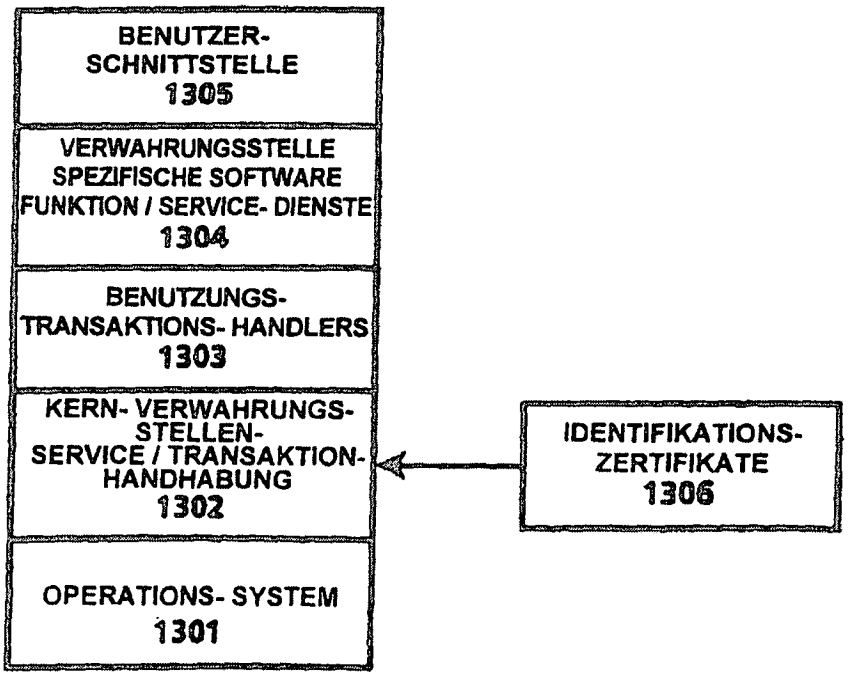
BENUTZER-
SCHNITTSTELLE
1305
VERWAHRUNGSSTELLE
SPEZIFISCHE SOFTWARE
FUNKTION / SERVICE- DIENSTE
1304
BENUTZUNGS-
TRANSAKTIONS- HANDLERS
1303
KERN- VERWAHRUNGS-
STELLEN-
SERVICE / TRANSAKTION-
HANDHABUNG
1302
OPERATIONS- SYSTEM
1301
IDENTIFIKATIONS-
ZERTIFIKATE
1306

Fig.13

1501 ~ Digital Work Rights:= (Rights*)
1502 ~ Right : = (Right-Code {Copy-Count} {Control-Spec} {Time-Spec }
{Access-Spec} {Fee-Spec})
1503 ~ Right-Code : = Render-Code | Transport-Code | File-Management-
Code| Derivative-Works- Code | Configuration-Code
1504 ~ Render-Code : = [Play : {Player: Player-ID} | Print: {Printer: Printer-ID}]
1505 ~ Transport-Code : = [Copy | Transfer | Loan {Remaining-Rights:
Next-Set-of-Rights}]{(Next-Copy-Rights: Next-Set-of-Rights)}
1506 ~ File-Management-Code := Backup {Back-Up-Copy-Rights:
Next-Set-of-Rights} | Restore | Delete | Folder
| Directory {Name: Hide-Local | Hide-Remote}
{Parts: Hide-Local | Hide-Remote}
1507 ~ Derivative-Works-Code : = [Extract | Embed | Edit{Process:
Process-ID}] {Next-Copy-Rights :
Next-Set-of Rights}
1508 ~ Configuration-Code : = Install | Uninstall
1509 ~ Next-Set-of-Rights : = {(Add: Set-Of-Rights)} {(Delete:
Set-Of-Rights)} {(Replace: Set-Of-Rights)}{(Keep: Set-Of-Rights)}
1510 ~ Copy-Count : = (Copies:positive-integer | 0 | Unlimited)
1511 ~ Control-Spec : = (Control: {Restrictable | Unrestrictable}
{Unchargeable | Chargeable})
1512 ~ Time-Spec : = ({Fixed-Interval | Sliding-Interval | Meter-Time}
Until: Expiration-Date)
1513 ~ Fixed-Interval : = From: Start-Time
1514 ~ Sliding-Interval : = Interval: Use-Duration
1515 ~ Meter-Time: = Time-Remaining: Remaining-Use
1516 ~ Access-Spec : = ({SC: Security-Class} {Authorization: Authorization-ID*}
{Other-Authorization: Authorization-ID*} {Ticket: Ticket-ID})
1517 ~ Fee-Spec: = {Scheduled-Discount} Regular-Fee-Spec | Scheduled-Fee-Spec |
Markup-Spec
1518 ~ Scheduled-Discount: = Scheduled-Discount: (Scheduled-Discount:
(Time-Spec Percentage)*)
1519 ~ Regular-Fee-Spec : = ({Fee: | Incentive: } [Per-Use-Spec | Metered-Rate-
Spec | Best-Price-Spec | Call-For-Price-Spec]
{Min: Money-Unit Per: Time-Spec}{Max:
Money-Unit Per: Time-Spec} To: Account-ID)
1520 ~ Per-Use-Spec: = Per-Use: Money-unit
1521 ~ Metered-Rate-Spec : = Metered: Money-Unit Per: Time-Spec
1522 ~ Best-Price-Spec : = Best-Price: Money-unit Max: Money-unit
1523 ~ Call-For-Price-Spec : = Call-For -Price
1524 ~ Scheduled-Fee-Spec: = (Schedule: (Time-Spec Regular-Fee-Spec)*)
1525 ~ Markup-Spec: = Markup: percentage To: Account-ID

Fig. 15

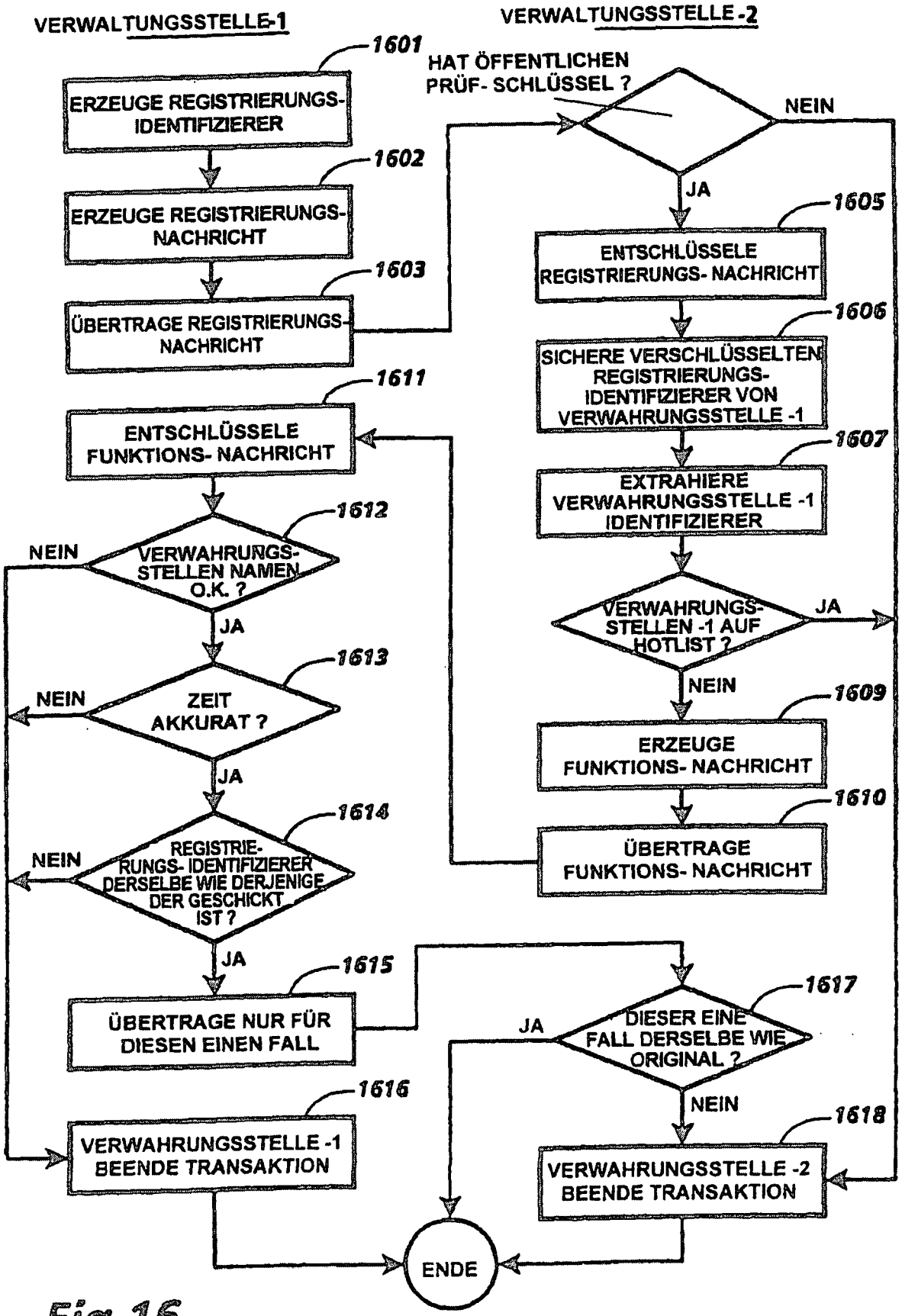
VERWALTUNGSSTELLE-1
VERWALTUNGSSTELLE-2
1601
ERZEUGE REGISTRIERUNGS-IDENTIFIZIERER
1602
ERZEUGE REGISTRIERUNGS-NACHRICHT
1603
ÜBERTRAGE REGISTRIERUNGS-NACHRICHT
HAT ÖFFENTLICHEN PRÜF- SCHLÜSSEL ?
NEIN
JA
1605
ENTSCHLÜSSELE REGISTRIERUNGS- NACHRICHT
1606
SICHERE VERSCHLÜSSELTEN REGISTRIERUNGS-IDENTIFIZIERER VON VERWAHRUNGSSTELLE -1
1607
EXTRAHIERE VERWAHRUNGSSTELLE -1 IDENTIFIZIERER
VERWAHRUNGS-STELLEN -1 AUF HOTLIST ?
JA
NEIN
1609
ERZEUGE FUNKTIONS- NACHRICHT
1610
ÜBERTRAGE FUNKTIONS- NACHRICHT
1611
ENTSCHLÜSSELE FUNKTIONS- NACHRICHT
1612
VERWAHRUNGS-STELLEN NAMEN O.K. ?
NEIN
JA
1613
ZEIT AKKURAT ?
NEIN
JA
1614
REGISTRIE-RUNGS- IDENTIFIZIERER DERSELBE WIE DERJENIGE DER GESCHICKT IST ?
NEIN
JA
1615
ÜBERTRAGE NUR FÜR DIESEN EINEN FALL
1617
DIESER EINE FALL DERSELBE WIE ORIGINAL ?
JA
NEIN
1616
VERWAHRUNGSSTELLE -1 BEENDE TRANSAKTION
1618
VERWAHRUNGSSTELLE -2 BEENDE TRANSAKTION
ENDE

Fig.16

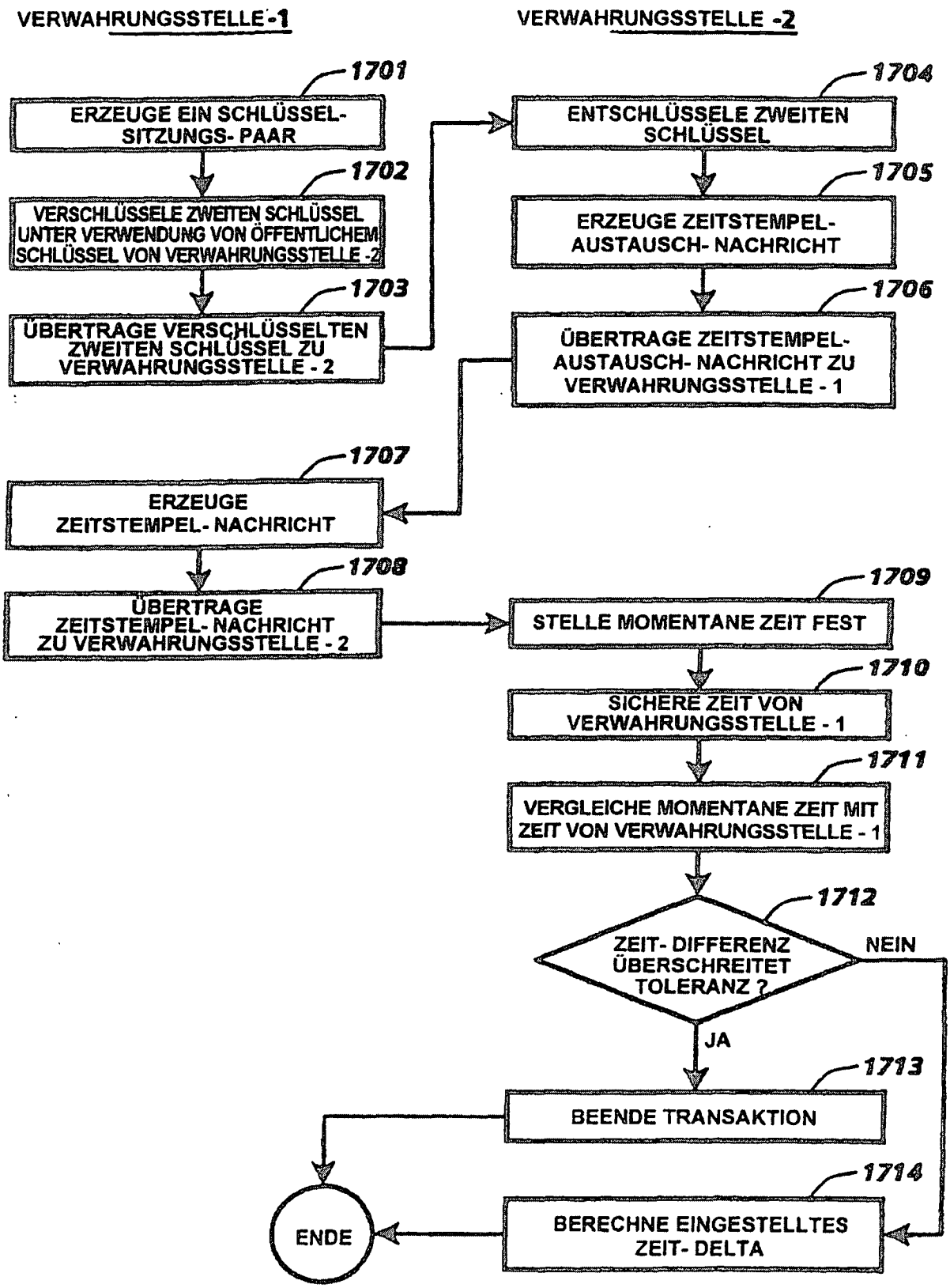
VERWAHRUNGSSTELLE -1
VERWAHRUNGSSTELLE -2
1701
ERZEUGE EIN SCHLÜSSEL-SITZUNGS- PAAR
1702
VERSCHLÜSSELE ZWEITEN SCHLÜSSEL UNTER VERWENDUNG VON ÖFFENTLICHEM SCHLÜSSEL VON VERWAHRUNGSSTELLE -2
1703
ÜBERTRAGE VERSCHLÜSSELTEN ZWEITEN SCHLÜSSEL ZU VERWAHRUNGSSTELLE - 2
1704
ENTSCHLÜSSELE ZWEITEN SCHLÜSSEL
1705
ERZEUGE ZEITSTEMPEL-AUSTAUSCH- NACHRICHT
1706
ÜBERTRAGE ZEITSTEMPEL-AUSTAUSCH- NACHRICHT ZU VERWAHRUNGSSTELLE - 1
1707
ERZEUGE ZEITSTEMPEL- NACHRICHT
1708
ÜBERTRAGE ZEITSTEMPEL- NACHRICHT ZU VERWAHRUNGSSTELLE - 2
1709
STELLE MOMENTANE ZEIT FEST
1710
SICHERE ZEIT VON VERWAHRUNGSSTELLE - 1
1711
VERGLEICHE MOMENTANE ZEIT MIT ZEIT VON VERWAHRUNGSSTELLE - 1
1712
ZEIT- DIFFERENZ ÜBERSCHREITET TOLERANZ ?
NEIN
JA
1713
BEENDE TRANSAKTION
1714
BERECHNE EINGESTELLTES ZEIT- DELTA
ENDE

Fig.17

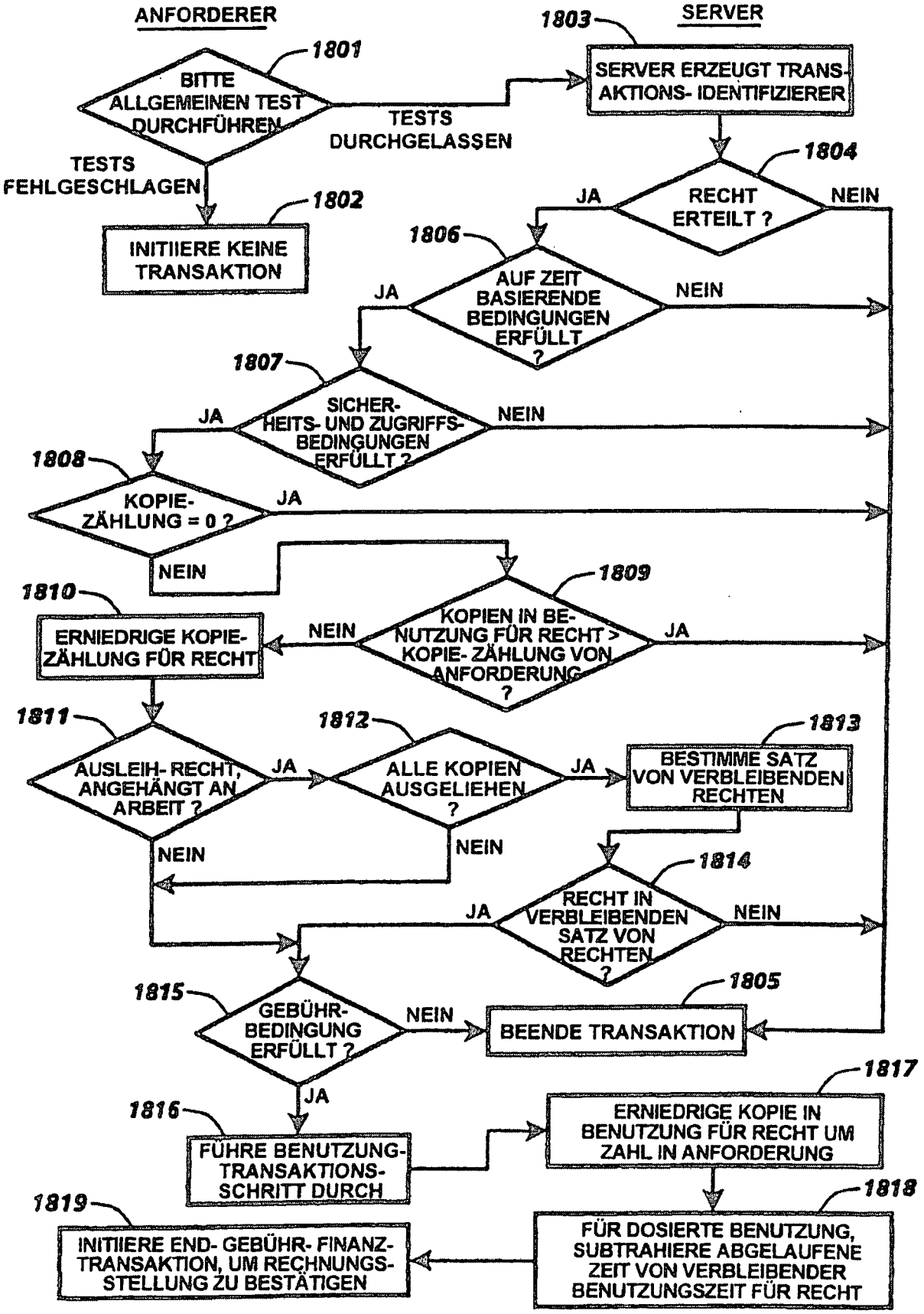
ANFORDERER
SERVER
1801
BITTE ALLGEMEINEN TEST DURCHFÜHREN
TESTS DURCHGELASSEN
TESTS FEHLGESCHLAGEN
1803
SERVER ERZEUGT TRANSAKTIONS- IDENTIFIZIERER
1804
RECHT ERTEILT ?
JA
NEIN
1802
INITIIERE KEINE TRANSAKTION
1806
AUF ZEIT BASIERENDE BEDINGUNGEN ERFÜLLT ?
JA
NEIN
1807
SICHERHEITS- UND ZUGRIFFS- BEDINGUNGEN ERFÜLLT ?
JA
NEIN
1808
KOPIE- ZÄHLUNG = 0 ?
JA
NEIN
1809
KOPIEN IN BENUTZUNG FÜR RECHT > KOPIE- ZÄHLUNG VON ANFORDERUNG ?
NEIN
JA
1810
ERNIEDRIGE KOPIE- ZÄHLUNG FÜR RECHT
1811
AUSLEIH- RECHT, ANGEHÄNGT AN ARBEIT ?
JA
NEIN
1812
ALLE KOPIEN AUSGELIEHEN ?
JA
NEIN
1813
BESTIMME SATZ VON VERBLEIBENDEN RECHTEN
1814
RECHT IN VERBLEIBENDEN SATZ VON RECHTEN ?
JA
NEIN
1815
GEBÜHR- BEDINGUNG ERFÜLLT ?
NEIN
JA
1805
BEENDE TRANSAKTION
1816
FÜHRE BENUTZUNG- TRANSAKTIONS- SCHRITT DURCH
1817
ERNIEDRIGE KOPIE IN BENUTZUNG FÜR RECHT UM ZAHL IN ANFORDERUNG
1818
FÜR DOSIERTE BENUTZUNG, SUBTRAHIERE ABGELAUFENE ZEIT VON VERBLEIBENDER BENUTZUNGSZEIT FÜR RECHT
1819
INITIIERE END- GEBÜHR- FINANZ- TRANSAKTION, UM RECHNUNGS- STELLUNG ZU BESTÄTIGEN

Fig. 18

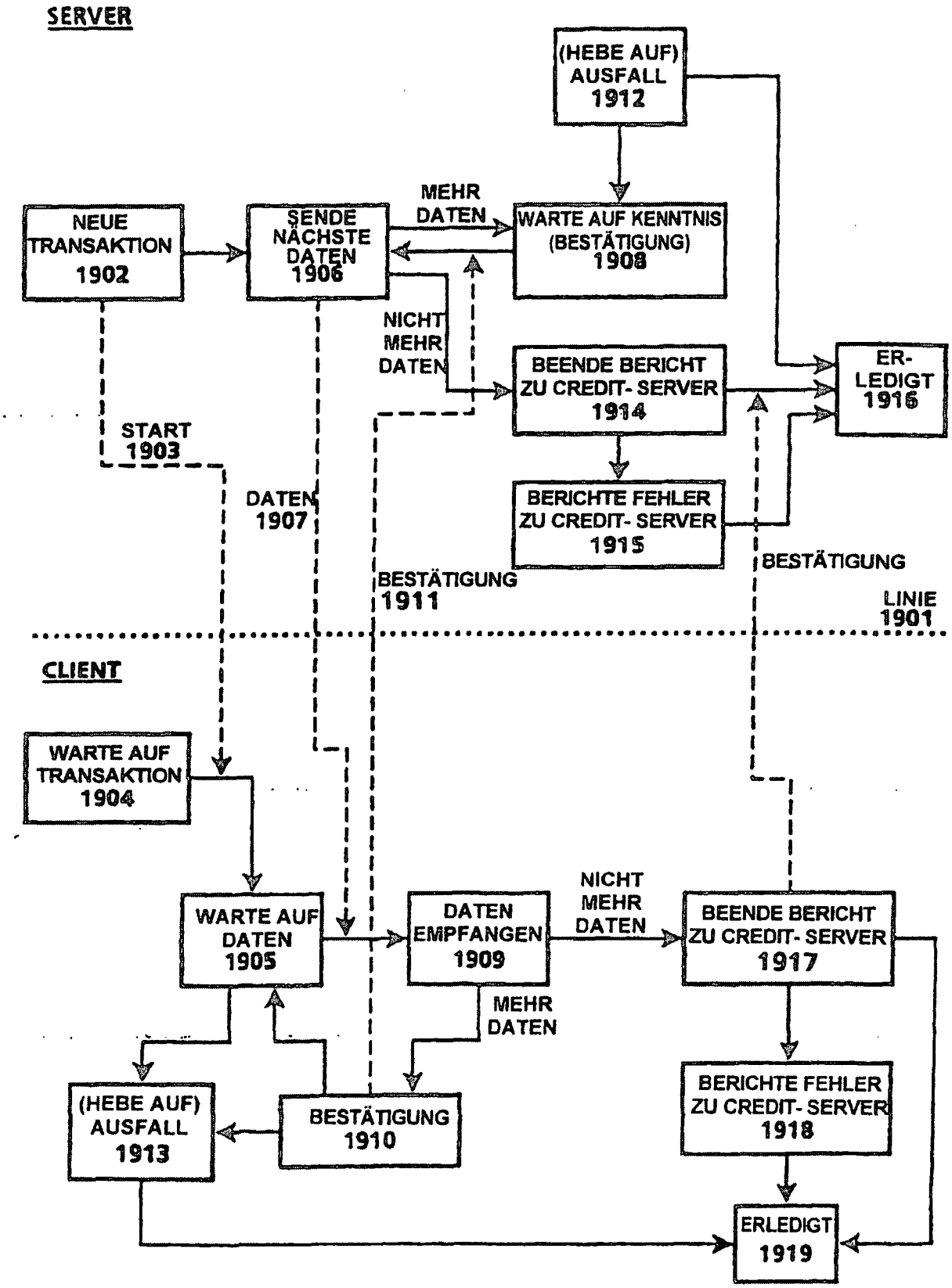
SERVER
(HEBE AUF) AUSFALL 1912
NEUE TRANSAKTION 1902
SENDE NÄCHSTE DATEN 1906
MEHR DATEN
WARTE AUF KENNTNIS (BESTÄTIGUNG) 1908
NICHT MEHR DATEN
BEENDE BERICHT ZU CREDIT- SERVER 1914
ER- LEDIGT 1916
START 1903
DATEN 1907
BERICHTE FEHLER ZU CREDIT- SERVER 1915
BESTÄTIGUNG 1911
BESTÄTIGUNG
LINIE 1901
CLIENT
WARTE AUF TRANSAKTION 1904
WARTE AUF DATEN 1905
DATEN EMPFANGEN 1909
NICHT MEHR DATEN
BEENDE BERICHT ZU CREDIT- SERVER 1917
MEHR DATEN
(HEBE AUF) AUSFALL 1913
BESTÄTIGUNG 1910
BERICHTE FEHLER ZU CREDIT- SERVER 1918
ERLEDIGT 1919

Fig.19