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

(10) **DE 696 36 982 T2** 2007.12.06

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 809 244 B1**
(21) Deutsches Aktenzeichen: **696 36 982.6**
(96) Europäisches Aktenzeichen: **96 118 541.0**
(96) Europäischer Anmeldetag: **19.11.1996**
(97) Erstveröffentlichung durch das EPA: **26.11.1997**
(97) Veröffentlichungstag
der Patenterteilung beim EPA: **21.03.2007**
(47) Veröffentlichungstag im Patentblatt: **06.12.2007**

(51) Int Cl.[8]: ***G06F 1/00*** (2006.01)

(30) Unionspriorität:
12482396 20.05.1996 JP

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Fujitsu Ltd., Kawasaki, Kanagawa, JP

(74) Vertreter:
Mitscherlich & Partner, Patent- und Rechtsanwälte, 80331 München

(72) Erfinder:
Akiyama, Ryota, Nakahara-ku, Kawasaki-shi, Kanagawa 211, JP; Yoshioka, Makoto, Nakahara-ku, Kawasaki-shi, Kanagawa 211, JP; Uchida, Yoshiaki, Nakahara-ku, Kawasaki-shi, Kanagawa 211, JP

(54) Bezeichnung: **Softwarekopiersystem**

Beschreibung

HINTERGRUND DER ERFINDUNG

1. Gebiet der Erfindung

[0001] Die vorliegende Erfindung betrifft Softwarekopiersysteme, und insbesondere ein Softwarekopiersystem, das eine Duplizierung von urheberrechtlich geschützter Software in legitimer Weise in einem Speichermedium eines Nutzers ermöglicht.

2. Beschreibung des Standes der Technik

[0002] Eine große Vielfalt von Softwarevertriebsverfahren wurde in den letzten Jahren nutzbar, und die Verbraucher können Softwareprodukte kaufen, die auf Speichermedien, wie beispielsweise Disketten, Compact Disc – Nurlesespeichern (CD-ROMs) und Halbleiterspeichern gespeichert sind. Sie können auch in Online-Shops verkaufte Softwareprodukte durch Herunterladen über Netze kaufen. Die meisten solcher kommerziellen Softwareprodukte können jedoch einfach auf andere Speichermedien kopiert werden. Dies bedeutet, dass sie dem potentiellen Risiko einer illegalen Duplizierung oder Software-Piraterie ausgesetzt sind, was ein ernstes Problem für urheberrechtlich geschützte Software geworden ist.

[0003] Bezüglich der Softwarevertriebsverfahren für Computeranwendungen, Wörterbücher, Audio- und Videodaten, usw. ist eines der herkömmlichen Verfahren ihr Vertrieb auf einer CD-ROM, die durch einen Sicherungsschlüssel elektronisch gesperrt ist. Wenn ein Nutzer an einem bestimmten Softwareprodukt interessiert ist, tritt er/sie mit einem Zentralstandort in Kontakt, der mit diesem Produkt handelt. Der Nutzer unternimmt dann einen notwendigen Prozess, um es zu kaufen, und empfängt wiederum einen zum Produkt gehörenden Schlüssel. Durch Öffnen des geschützten Softwarearchivs mit diesem Schlüssel kann der Nutzer es schließlich in sein/ihr System installieren.

[0004] Ein weiteres Verfahren des Softwarevertriebs verwendet ein beschreibbares Speichermedium, das im Voraus gebrannte lizenzspezifische Identifikations-Informationen enthält, welche Informationen am Zentralstandort zum Lizenzieren des Rechts zum Kopieren ihrer Softwareprodukte verwaltet werden. Beim Versuch, ein auf einer CD-ROM aufgezeichnetes Softwareprodukt zu duplizieren, senden ein Nutzer oder ein die Speichermedien verkaufender Händler ihre Anfragen an den Zentralstandort. Nach Ablauf einiger notwendiger Prozesse zum Kaufen dieses betreffenden Softwareprodukts empfängt der anfragende Nutzer oder Händler Identifikationsinformationen, die vom Zentralstandort ausgegeben werden. Das betreffende Softwareprodukt kann von der CD-ROM auf das Speichermedium nur dupliziert werden, wenn die empfangenen Identifikationsinformationen mit den auf dem Speichermedium aufgezeichneten lizenzspezifischen Identifikationsinformationen übereinstimmen.

[0005] Aber jeder kann die Software ausführen oder auf sie zugreifen, wenn sie einmal auf seinem/ihrem lokalen Speichergerät, wie beispielsweise einer Festplatte, installiert ist. Dies bedeutet einfach, dass die installierte Software wegen des Fehlens eines Schlüsselschutzes nach wie vor Gegenstand einer illegalen Duplizierung ist.

[0006] Ferner sollten im obigen zweiten Verfahren die lizenzspezifischen Identifikationsinformationen am Zentralstandort in engem Kontakt mit einer Fabrik, wo die Speichermedien hergestellt werden, kontrolliert werden. Ein weiteres Problem mit den Speichermedien besteht darin, dass es erforderlich ist, zwei Arten von Speichermedien in unterschiedlichen Wegen für verschiedene Zwecke zu behandeln: Softwarekopie und allgemeiner Gebrauch.

[0007] Das US-Patent Nr. 4,658,093 offenbart ein System zum sicheren Vertrieb von Software mit einer Basiseinheit, welche die Software benutzt, einer entfernten Autorisierungseinheit, die die Verwendung der Software in der Basiseinheit autorisiert, einer eine Kommunikation zwischen der Basiseinheit und der Autorisierungseinheit vorsehenden Einrichtung, einer Einrichtung in der Basiseinheit zum Sperren der Verwendung der Software, sofern von der Autorisierungseinheit keine Autorisierung zur Verwendung empfangen worden ist, einer Einrichtung in der Basiseinheit zum Kommunizieren von Softwareanfragen an die Autorisierungseinheit, wobei die Anfrage wenigstens eine Identifizierung der Basiseinheit, die Anzahl der angefragten Benutzungen und eine zufällige oder nicht wiederholte Nummer enthält, einer Einrichtung in der Autorisierungseinheit zum Verarbeiten der Anfrage mit der Identifikation der Basiseinheit, der Anzahl von angefragten Benutzungen und der zufälligen Nummer und zum Bereitstellen einer Autorisierung für die angefragte Anzahl von Benutzungen, einer Einrichtung in der Basiseinheit zum Empfangen und Verifizieren der Autorisierung und einer Einrichtung in der Basiseinheit zum Erlauben einer Benutzung der Software für die durch die Autorisierungseinheit autorisierte Anzahl von Benutzungen.

[0008] Die EP 0 302 710 A2 offenbart ein Verfahren zum Steuern der Benutzung und Kopie von Diskettensoftwareinhalten und dergleichen auf nicht autorisierten, über Disketten betriebenen Computersystemen.

[0009] Das US-Patent 5,182,770 offenbart ein integriertes Softwarepiraterieverhinderungssystem, das mehrere charakteristische Identifikationscodes beinhaltet, die Installations- und Softwarekomponenten

identifizieren. Eine separate Sicherheitsvorrichtung ist an dem geschützten Computersystem angebracht und steht mit ihm in Verbindung. Es wird interaktiv betreffend eine richtige Autorisierung des aktuellen Nutzers abgefragt. Dieser Ansatz ist flexibel und sieht eine ökonomische Verfolgung von Lizenzen und ihrer Nutzung von hochentwickelten Programmen vor.

[0010] Die EP 0 665 486 A2 offenbart ein Verfahren zum Schützen von elektronisch veröffentlichten Dokumenten. Es beinhaltet das Betreiben eines Computersystems und eines Netzes für die elektronische Veröffentlichung von Dokumenten.

[0011] IBM, Technical Disclosure Bulletin, Vol. 37, Nr. 4B, April 1994, Seiten 623 bis 625, "Secure Source Data Transport in a Three Party System", offenbart ein Verfahren, das es Informationsanbietern erlaubt, Daten sicher an Informationsabnehmer zu verteilen, die ihrerseits die Daten in Werkzeugen von Dritten verwenden, einschließlich einer Einrichtung zum Erlauben eines Werkzeugs, die ursprünglichen Daten zu analysieren, wobei es dem Informationsabnehmer erlaubt wird, nur als ein Beförderer einer unlesbaren Form der Daten zu agieren.

[0012] Es die Aufgabe der vorliegenden Erfindung, ein Softwarekopierverfahren und ein Softwarekopiersystem vorzusehen, die das Kopieren von urheberrechtlich geschützten Daten, die auf einem Originalspeichermedium aufgezeichnet sind, in einer legitimen Weise auf ein Zielspeichermedium, das ein Nutzer lesen kann und auf das er schreiben kann, zu ermöglichen.

[0013] Die Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst. Die abhängigen Ansprüche enthalten Weiterentwicklungen.

[0014] Um die obige Aufgabe zu lösen, ist gemäß der vorliegenden Erfindung ein Softwarekopiersystem zum Duplizieren von Software, die auf einem Originalspeichermedium aufgezeichnet ist, auf ein Zielspeichermedium in einer legitimen Weise vorgesehen. Ein autorisierter Kopiervorgang wird durch Kommunikationen zwischen einem Endnutzerstandort, der eine Lizenz zum Kopieren des Softwareprodukts beantragt, und einem Zentralstandort, der die Lizenz verwaltet, erzielt.

[0015] Das Softwarekopiersystem weist die folgenden Bauelemente auf. Eine Inhaltsidentifikator-Leseeinrichtung liest einen ersten Identifikator des Originalspeichermediums aus. Dieser erste Identifikator ist dem auf dem Originalspeichermedium aufgezeichneten Softwareprodukt eindeutig zugewiesen. Eine Speichermedienidentifikator-Leseeinrichtung liest einen zweiten Identifikator vom Zielspeichermedium aus. Dieser zweite Identifikator ist dem Zielspeichermedium eindeutig zugewiesen und auf diesem aufgezeichnet. Eine Signaturerzeugungseinrichtung, die am Zentralstandort angeordnet ist, erzeugt eine erste Signatur aus dem durch die Inhaltsidentifikator-Leseeinrichtung ausgelesenen ersten Identifikator und dem durch die Speichermedienidentifikator-Leseeinrichtung gelesenen zweiten Identifikator. Diese erste Signatur dient als Bescheinigung einer Lizenz, das Softwareprodukt zu kopieren. Eine Signaturschreibeinrichtung schreibt die durch die Signaturerzeugungseinrichtung erzeugte erste Signatur in das Zielspeichermedium. Zu einem Nachprüfungszweck erzeugt eine Signaturerzeugungs/vergleichseinrichtung eine zweite Signatur aus dem durch die Inhaltsidentifikator-Leseeinrichtung ausgelesenen ersten Identifikator und dem durch die Speichermedienidentifikator-Leseeinrichtung ausgelesenen zweiten Identifikator. Die Signaturerzeugungs/vergleichseinrichtung vergleicht dann die im Zielspeichermedium gespeicherte erste Signatur mit der zweiten Signatur. Eine Datenkopiereinrichtung ruft das Softwareprodukt aus dem Originalspeichermedium ab und schreibt das Softwareprodukt in das Zielspeichermedium, wenn sich als Ergebnis des durch die Signaturerzeugungs/vergleichseinrichtung durchgeführten Vergleichs herausgestellt hat, dass der erste und der zweite Identifikator identisch sind.

[0016] Um die obige Aufgabe zu lösen, ist auch ein Softwarekopierverfahren zum Duplizieren einer auf einem Originalspeichermedium aufgezeichneten Software auf ein Zielspeichermedium in einer legitimen Weise vorgesehen. Dieses Softwarekopierverfahren weist die folgenden Schritte auf.

[0017] Zuerst werden ein Speichermedienidentifikator, der dem Zielspeichermedium eindeutig zugewiesen ist, und ein Inhaltsidentifikator, der einer betreffenden Datendatei eindeutig zugewiesen ist, von einem Endnutzerstandort an einen Zentralstandort zusammen mit einer eine Softwarelizenz beantragenden Nachricht gesendet. Zweitens wird ein erster Bescheinigungscode am Zentralstandort aus dem Speichermedienidentifikator und dem Inhaltsidentifikator, die vom Endnutzerstandort empfangen werden, erzeugt. Dieser Schritt wird durch einen Signaturerzeugungsvorgang erreicht, der einen Bescheinigungsschlüssel verwendet, der am Zentralstandort verwaltet wird. Drittens wird ein verschlüsselter Bescheinigungsschlüssel am Zentralstandort durch Verschlüsseln des Bescheinigungsschlüssels unter Verwendung eines Nutzerschlüssels erzeugt. Viertens werden der erste Bescheinigungscode und der verschlüsselte Bescheinigungsschlüssel vom Zentralstandort zum Endnutzerstandort geschickt. Fünftens werden der erste Bescheinigungscode und der verschlüsselte Bescheinigungsschlüssel, die vom Zentralstandort am Endnutzerstandort angekommen sind, in das Zielspeichermedium geschrieben. Sechstens erhält man am Endnutzerstandort einen entschlüsselten Bescheinigungsschlüssel durch Ent-

schlüsseln des im Zielspeichermedium gespeicherten verschlüsselten Bescheinigungsschlüssels unter Verwendung des Nutzerschlüssels. Siebtens wird ein zweiter Bescheinigungscode zum Zweck einer Nachprüfung am Endnutzerstandort durch Anwenden eines Signaturerzeugungsvorgangs unter Verwendung des entschlüsselten Bescheinigungsschlüssels auf den Speichermedienidentifikator und den Inhaltsidentifikator erzeugt. Achtens wird der im Zielspeichermedium gespeicherte erste Bescheinigungscode mit dem zweiten Bescheinigungscode verglichen, der am Endnutzerstandort erzeugt wird. Als letztes wird die im Originalspeichermedium gespeicherte betreffende Datendatei ausgelesen und in das Zielspeichermedium geschrieben, falls der erste und der zweite Bescheinigungscode übereinstimmen.

[0018] Obige sowie weitere Aufgaben, Merkmale und Vorteile der vorliegenden Erfindung werden aus der folgenden Beschreibung in Zusammenhang mit den beiliegenden Zeichnungen, die ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung beispielhaft veranschaulichen, besser verständlich.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0019] Fig. 1 ist eine Konzeptansicht eines Softwarekopiersystems gemäß der vorliegenden Erfindung;

[0020] Fig. 2 ist ein Flussdiagramm eines durch ein Softwarekopiersystem ausgeführten Softwareduplizierungsvorgangs in einem ersten Ausführungsbeispiel der vorliegenden Erfindung;

[0021] Fig. 3(A) ist eine Darstellung des Aufbaus einer CD-ROM;

[0022] Fig. 3(B) ist eine Darstellung des Aufbaus einer MO-Disk;

[0023] Fig. 4 ist eine Darstellung eines Prozesses des Duplizierens urheberrechtlich geschützter Software;

[0024] Fig. 5 ist eine Darstellung des Aufbaus eines typischen Signaturprozessors;

[0025] Fig. 6 ist eine Darstellung eines Prozesses des Ausführens eines duplizierten Softwareprogramms;

[0026] Fig. 7 ist ein Flussdiagramm eines durch ein Softwarekopiersystem ausgeführten Softwareduplizierungsvorgangs in einem zweiten Ausführungsbeispiel der vorliegenden Erfindung;

[0027] Fig. 8 ist eine Darstellung eines Prozesses am Zentralstandort;

[0028] Fig. 9 ist eine Darstellung eines Prozesses am Endnutzerstandort; und

[0029] Fig. 10 ist eine Darstellung eines Prozesses des Ausführens eines duplizierten Softwareprogramms.

BESCHREIBUNG DES BEVORZUGTEN AUSFÜHRUNGSBEISPIELS

[0030] Zu Beginn wird die vorliegende Erfindung unter Bezug auf Fig. 1 skizziert, die eine Konzeptansicht eines Softwarekopiersystems gemäß der vorliegenden Erfindung zeigt.

[0031] Wie man in Fig. 1 sieht, weist das Softwarekopiersystem der vorliegenden Erfindung mehrere nachfolgend beschriebene Elemente auf. Eine Inhaltsidentifikator-Leseeinrichtung **2** ist eine Einrichtung zum Auslesen eines in einem Originalspeichermedium **1** gespeicherten ersten Identifikators. Dieser erste Identifikator ist jedem Softwareprodukt, das im Originalspeichermedium **1** aufgezeichnet ist, eindeutig zugewiesen. Eine Speichermedienidentifikator-Leseeinrichtung **4** liest einen zweiten Identifikator aus, der in einem Zielspeichermedium **3** gespeichert ist. Dieser zweite Identifikator ist dem Zielspeichermedium **3** eindeutig zugewiesen. Eine Signaturerzeugungseinrichtung **6**, die am Zentralstandort **5** angeordnet ist, der Lizenzen zum Kopieren von Software verwaltet, erzeugt eine erste Signatur aus dem ersten und dem zweiten Identifikator, die durch die Inhaltsidentifikator-Leseeinrichtung **2** bzw. die Speichermedienidentifikator-Leseeinrichtung **4** ausgelesen wurden. Die erste Signatur dient als eine Bescheinigung einer Lizenz, das Softwareprodukt zu kopieren. Eine Signaturschreibeinrichtung **7** schreibt die erste Signatur, die durch die Signaturerzeugungseinrichtung **6** erzeugt wird, in das Zielspeichermedium **3**. Eine Signaturerzeugungs/vergleichseinrichtung **8** erzeugt eine zweite Signatur aus dem ersten und dem zweiten Identifikator, die durch die Inhaltsidentifikator-Leseeinrichtung **2** bzw. die Speichermedienidentifikator-Leseeinrichtung **4** ausgelesen wurden. Die Signaturerzeugungs/vergleichseinrichtung **8** vergleicht die im Zielspeichermedium **3** gespeicherte erste Signatur mit der zweiten Signatur, die erzeugt wird. Eine Datenkopiereinrichtung **9** ruft das betreffende Softwareprodukt vom Originalspeichermedium **1** ab und schreibt es in das Zielspeichermedium **3**, wenn sich als Ergebnis des durch die Signaturerzeugungs/vergleichseinrichtung **8** durchgeführten Vergleichs herausstellt, dass die erste und die zweite Signatur identisch sind.

[0032] Das Originalspeichermedium **1** enthält mehrere kommerzielle Softwareprodukte, für die jeweils ein Inhaltsidentifikator geschrieben ist. Das Zielspeichermedium **3** hat einen individuellen Speichermedienidentifikator, der beim Hersteller vor dem Auslie-

fern geschrieben wird. Wenn ein Nutzer ein Softwareprodukt aus jenen im Originalspeichermedium **1** auswählt, ruft die Inhaltsidentifikator-Leseeinrichtung **2** einen Inhaltsidentifikator entsprechend dem ausgewählten Softwareprodukt ab, und dann liest die Speichermedienidentifikator-Leseeinrichtung **4** einen im Zielspeichermedium **3** aufgezeichneten Speichermedienidentifikator aus. Diese zwei Identifikatoren werden zusammen mit einer Kaufanfragenachricht an den Zentralstandort **5** übertragen, um eine Lizenz zum Kopieren des betreffenden Softwareprodukts zu beantragen. Am Zentralstandort **5** empfängt die Signaturerzeugungseinrichtung **6** den Inhaltsidentifikator und den Speichermedienidentifikator und sendet an den Nutzer eine Signatur zurück, die aus den empfangenen Identifikatoren erzeugt wird. Diese Signatur autorisiert den Nutzer als einen Lizenznehmer mit dem Recht, das Softwareprodukt zu kopieren. Gleichzeitig mit der Ausgabe der Signatur wird der Nutzer in einer Nutzerprofildatenbank am Zentralstandort **5** registriert, und es wird auch ein Rechnungsstellungsvorgang aufgerufen.

[0033] Auf der Nutzerseite schreibt die Signaturschreibeinrichtung **7** beim Empfang der von der Signaturerzeugungseinrichtung **6** gesendeten Signatur diese in das Zielspeichermedium **3**. Die Signaturerzeugungs/vergleichseinrichtung **8** erzeugt dann lokal eine Signatur aus dem von der Inhaltsidentifikator-Leseeinrichtung **2** abgerufenen Inhaltsidentifikator und dem von der Speichermedienidentifikator-Leseeinrichtung **4** abgerufenen Speichermedienidentifikator. Die Signaturerzeugungs/vergleichseinrichtung **8** vergleicht diese Signatur mit der im Zielspeichermedium **3** gespeicherten, erstgenannten Signatur. Falls die zwei Signaturen übereinstimmen, ruft die Datenkopiereinrichtung **9** das betreffende Softwareprodukt, das in verschlüsselter Form gespeichert ist, vom Originalspeichermedium **1** ab und kopiert es in das Zielspeichermedium **3**. Die nun im Zielspeichermedium **3** gespeicherte Software ist jedoch nicht zur Ausführung bereit, weil sie noch verschlüsselt ist. Der Nutzer muss sie in den Hauptspeicher eines speziellen Prozessors laden, der die verschlüsselte Software decodiert und ausführt.

[0034] Als nächstes wird nun ein erstes Ausführungsbeispiel der vorliegenden Erfindung Bezug nehmend auf Fig. 2 bis Fig. 6 beschrieben. Die folgende Erläuterung nimmt einen solchen Fall an, dass ein auf einer CD-ROM vertriebenes bestimmtes, urheberrechtlich geschütztes Softwareprogramm auf eine magnetooptische (MO) Disk kopiert werden soll.

[0035] Fig. 2 ist ein Flussdiagramm eines durch das Softwarekopiersystem durchgeführten Softwareduplizierungsvorgangs. Um ein Programm auf einer CD-ROM auf eine MO-Disk mit dem Softwarekopiersystem der vorliegenden Erfindung zu kopieren, ist es notwendig, den Schritten zu folgen:

[0036] (S1) Der auf der MO-Disk aufgezeichnete Speichermedienidentifikator IDk und der Softwareidentifikator SIDi des betreffenden Softwareprogramms werden an den Zentralstandort geschickt, der die Lizenz zum Kopieren der Software verwaltet.

[0037] (S2) Dieser Antrag für die Softwarelizenz wird am Zentralstandort verarbeitet, wo ein Bescheinigungscode CS aus dem Speichermedienidentifikator IDk und dem Softwareidentifikator SIDi, die vom Endnutzerstandort empfangen wurden, erzeugt wird. Der Zentralstandort sendet dann den Bescheinigungscode CS an den Endnutzerstandort zurück.

[0038] (S3) Der am Endnutzerstandort angekommene Bescheinigungscode CS wird in einem vorbestimmten Speicherbereich auf der MO-Disk geschrieben.

[0039] (S4) Zu einem Nachprüfungszweck wird ein weiterer Bescheinigungscode CS' lokal am Endnutzerstandort basierend auf dem Speichermedienidentifikator IDk und dem Softwareidentifikator SIDi, die an den Zentralstandort geschickt wurden, erzeugt.

[0040] (S5) Der lokal erzeugte Bescheinigungscode CS' wird mit dem anderen Bescheinigungscode CS, der auf der MO-Disk gespeichert ist, verglichen.

[0041] (S6) Entsprechend dem Ergebnis des Vergleichs zwischen CS und CS' geht der Vorgang auf verschiedene Weisen weiter. Falls die zwei Bescheinigungscodes als identisch erkannt werden, geht der Prozess zum nächsten Schritt S7. Sonst wird der Prozess ohne Kopieren des Softwareprogramms von der CD-ROM auf die MO-Disk beendet.

[0042] (S7) Eine verschlüsselte Softwaredatendatei mit dem Softwareidentifikator SIDi wird von der CD-ROM auf die vorbereitete MO-Disk kopiert.

[0043] Fig. 3(A) und Fig. 3(B) zeigen den Aufbau von Datensätzen auf einer CD-Rom bzw. einer MO-Disk. Der Aufbau einer CD-ROM **11** ist in Fig. 3(A) dargestellt, wo mehrere urheberrechtlich geschützte Softwareprogramme und ein Verwalteranwendungsprogramm MA aufgezeichnet sind. Die urheberrechtlich geschützten Softwareprogramme, die in verschlüsselter Form gespeichert sind, haben ihre jeweiligen Softwareidentifikatoren SIDi (i = 1, 2, ..., n). Das Verwalteranwendungsprogramm MA reguliert die Vorgänge, um die urheberrechtlich geschützten Softwareprogramme von einer CD-ROM auf eine MO-Disk zu kopieren. Bei einer Anfrage zum Kopieren von Software wird dieses Programm in eine am Endnutzerstandort positionierte Gerätestation (z.B. einen Personal Computer) geladen und darauf ausgeführt. D.h. das Verwalteranwendungsprogramm MA ist für die am Endnutzerstandort als Teil des in Fig. 2 dargestellten Prozesses ausgeführten

Schritte verantwortlich.

[0044] Fig. 3(B) ist eine Darstellung der Datensatzstruktur der MO-Disk **12**, auf der ein Speichermedienidentifikator IDk (k = 1, 2, ..., m) aufgezeichnet ist. Obwohl der größte Teil der MO-Disk **12** durch die Endnutzer frei beschrieben und/oder gelesen werden kann, ist der Speichermedienidentifikator IDk in einem speziellen Teil der Disk geschrieben, der nicht überschreibbar ist. Dieser Speichermedienidentifikator IDk kann eine Seriennummer sein, die jedem Medium beim Hersteller vor der Auslieferung eindeutig zugewiesen wird.

[0045] Die folgende Beschreibung präsentiert einen detaillierteren Prozess des Duplizierens urheberrechtlich geschützter Software von einer CD-ROM auf eine MO-Disk unter Bezug auf Fig. 4.

[0046] Fig. 4 zeigt einen Softwarekopierprozess, der grob in zwei Teile unterteilt ist: Schritte am Endnutzerstandort (die rechte Hälfte von Fig. 4) und Schritte am Zentralstandort (die linke Hälfte von Fig. 4). Am Endnutzerstandort führt eine Gerätestation (z.B. ein Personal Computer) aktuelle Datenverarbeitungsjobs durch, die zum Kopieren der Software gehören, während mehrere am Zentralstandort angeordnete Geräte die Lizenz zum Kopieren der Software verwalten. Diese zwei Standorte sind durch eine Kommunikationsleitung oder einen Transportkanal verbunden.

[0047] Die Gerätestation am Endnutzerstandort ist mit einem CD-ROM-Laufwerk und einem MO-Laufwerk (beide nicht dargestellt) ausgestattet. Die CD-ROM **11**, die als Originalspeichermedium dient, das die urheberrechtlich geschützten Softwareprogramme speichert, wird in das CD-ROM-Laufwerk eingeschoben. Andererseits wird die MO-Disk **12**, die als ein Zielspeichermedium dient, in das MO-Laufwerk geladen. Das betreffende Softwareprogramm auf der CD-ROM **11** hat einen Softwareidentifikator SIDi, und der MO-Disk **12** gehört ihr eindeutiger Speichermedienidentifikator IDk.

[0048] Zuallererst startet an der Gerätestation des Endnutzers das Verwalteranwendungsprogramm MA auf der CD-ROM **11** mit einem Annehmen eines Antrags vom Endnutzer zum Kopieren eines speziellen Softwareprogramms. Auf diesen Antrag hin liest das Verwalteranwendungsprogramm MA den entsprechenden Softwareidentifikator SIDi von der CD-ROM **11** aus und extrahiert den Speichermedienidentifikator IDk von der MO-Disk **12**. Diese zwei Identifikatoren werden dann zusammen mit einer Antragsnachricht, die für eine Softwarelizenz notwendige Informationen enthält, an das Softwarelizenzzentrum gesendet.

[0049] Der Zentralstandort empfängt den oben beschriebenen Antrag vom Nutzer und sichert die Inhalte des Antrags in eine Nutzerprofildatenbank **13**. Der empfangene Softwareidentifikator SIDi und empfangene Speichermedienidentifikator IDk werden einem Signaturprozessor **14** zugeführt, wo die Identifikatoren SIDi und IDk in einen Bescheinigungscode CS komprimiert werden. Bei diesem Komprimiervorgang funktioniert ein Bescheinigungsschlüssel KEYc als ein privater Schlüssel (oder geheimer Schlüssel). Der erzeugte Bescheinigungscode CS dient als etwas, was als die „Signatur" in Fig. 1 bezeichnet wird. Der vom Signaturprozessor **14** verwendete Bescheinigungsschlüssel KEYc wird dann an eine Verschlüsselungseinheit **15** geleitet, um mit einem Nutzerschlüssel Ku verschlüsselt zu werden, wodurch ein chiffrierter Text EKU(KEYc) erzeugt wird. Der durch den Signaturprozessor **14** erzeugte Bescheinigungscode CS und der durch die Verschlüsselungseinheit **15** erzeugte chiffrierte Text EKU(KEYc) werden schließlich zusammen mit dem Zentralstandortsidentifikator IDc zum Endnutzerstandort als Antwort auf den Antrag vom Endnutzer übertragen.

[0050] Am Endnutzerstandort extrahiert die Gerätestation den Bescheinigungscode CS und den chiffrierten Text EKU(KEYC) aus den vom Zentralstandort empfangenen Informationen und schreibt sie in die Ziel-MO-Disk **12**. Der Bescheinigungscode CS und der chiffrierte Text EKU(KEYc), die auf der MO-Disk **12** aufgezeichnet sind, werden abgerufen und an das Verwalteranwendungsprogramm geschickt.

[0051] Dann startet in der Gerätestation ein Signaturnachprüfvorgang. Zuerst decodiert eine Entschlüsselungseinheit **16** den chiffrierten Text EKU(KEYc) unter Verwendung des Nutzerschlüssels Ku und extrahiert den Bescheinigungsschlüssel KEYc, der einmal am Zentralstandort verschlüsselt wurde. Aus dem von der CD-ROM **11** abgerufenen Softwareidentifikator SIDi und dem von der MO-Disk **12** abgerufenen Speichermedienidentifikator IDk erzeugt ein Signaturprozessor **17** einen Bescheinigungscode CS' zur Nachprüfung am Endnutzerstandort. Der durch die Entschlüsselungseinheit **16** entschlüsselte Bescheinigungsschlüssel KEYc wird in diesem CS'-Erzeugungsvorgang benutzt. Dann vergleicht ein Komparator **18** den in der MO-Disk **12** geschriebenen Bescheinigungscode CS und den durch den Signaturprozessor **17** erzeugten Bescheinigungscode CS'. Falls das Vergleichsergebnis eine Übereinstimmung der zwei Codes CS und CS' anzeigt, ermöglicht ein Schalter **19** das Schreiben des Softwareprogramms mit dem Softwareidentifikator SIDi auf die Ziel-MO-Disk **12** in der Form verschlüsselter Daten.

[0052] Die folgende Beschreibung präsentiert eine typische Funktion, die durch den Signaturprozessor **14** am Zentralstandort und den Signaturprozessor **17**

am Endnutzerstandort erzielt wird.

[0053] Fig. 5 zeigt die Struktur des Signaturprozessors, der aus einer Exklusiv-ODER-Logik **21** und einer Verschlüsselungseinheit **22** besteht. Die Exklusiv-ODER-Logik **21** führt eine Exklusiv-ODER-Operation an einem Softwareidentifikator SIDi, einem Speichermedienidentifikator IDk und einem Bescheinigungscode CS durch. Die Verschlüsselungseinheit **22** verschlüsselt den Ausgang der Exklusiv-ODER-Logik **21** mit dem Bescheinigungsschlüssel KEYc, um den Bescheinigungscode CS zu erzeugen. Diese zwei Elemente **21** und **22** bilden somit einen Hash-Funktionsoperator.

[0054] In einer blockweisen Weise verschlüsselt die Verschlüsselungseinheit **22** den Softwareidentifikator SIDi und den Speichermedienidentifikator IDk mit dem Bescheinigungsschlüssel KEYc. Die verschlüsselten Ausgangsdaten werden dem Eingang der Exklusiv-ODER-Logik **21** zurückgeführt und mit den nächsten Blockdaten der Exklusiv-ODER-Operation zugeleitet. Der Ausgang der Exklusiv-ODER-Logik **21** wird dann durch die Verschlüsselungseinheit **22** wieder verschlüsselt. Die obigen Vorgänge werden wiederholt, bis der letzte Block eingegeben wird, und das Ergebnis dieser zyklischen Berechnung kommt aus der Verschlüsselungseinheit **22** als ein Bescheinigungscode CS, wenn die Verschlüsselung des letzten Blocks beendet ist.

[0055] Das lizenzierte Softwareprogramm wird auf die MO-Disk **12** in der oben beschriebenen Weise kopiert, aber der Endnutzer kann es nicht ablaufen lassen, weil das Programm noch verschlüsselt ist. Die folgende Beschreibung erläutert, wie es ausgeführt wird.

[0056] Fig. 6 zeigt einen Prozess zum Ausführen eines duplizierten Softwareprogramms. Die MO-Disk **12** enthält den Bescheinigungscode CS, den chiffrierten Text EKU(KEYc), den Speichermedienidentifikator IDk und den Softwareidentifikator SIDi sowie die gespeicherte duplizierte Software in der Form verschlüsselter Daten EKd(DATA). Diese verschlüsselten Daten EKd(DATA) wurden mit einem Schlüssel Kd verschlüsselt, bevor die Software auf die CD-ROM gebrannt wurde, und der Verschlüsselungsschlüssel Kd liegt unter der Verwaltung des Verwalteranwendungsprogramms.

[0057] Die Gerätestation am Endnutzerstandort ruft zuerst von der MO-Disk **12** den Bescheinigungscode CS, den chiffrierten Text EKU(KEYc), den Speichermedienidentifikator IDk und den Softwareidentifikator SIDi ab. Die Entschlüsselungseinheit **16** entschlüsselt den chiffrierten Text EKU(KEYc) mit dem Nutzerschlüssel Ku, wodurch der Bescheinigungsschlüssel KEYc extrahiert wird. Dann erzeugt der Signaturprozessor **17** einen weiteren Bescheinigungscode CS' aus dem Softwareidentifikator SIDi und dem Speichermedienidentifikator IDk, die von der MO-Disk **12** abgerufen wurden, unter Verwendung des durch die Entschlüsselungseinheit **16** entschlüsselten Bescheinigungsschlüssels KEYc. Anschließend vergleicht der Komparator **18** die Bescheinigungscodes CS und CS'. Falls der Vergleich eine Übereinstimmung der zwei Codes CS und CS' angibt, erlaubt der Schalter **19**, dass eine verschlüsselte Datendatei EKd(DATA) mit dem verschlüsselten Softwareprogramm durch eine Entschlüsselungseinheit **25** läuft. Die Entschlüsselungseinheit **25** entschlüsselt die verschlüsselte Datendatei EKd(DATA) unter Verwendung des Schlüssels Kd, den das Verwalteranwendungsprogramm besitzt, wodurch die ursprüngliche Klartext-Datendatei DATA wiederhergestellt wird. Die Inhalte dieser entschlüsselten Datendatei DATA können durch die Zentralverarbeitungseinheit CPU nach dem Laden in den Speicher ausgeführt werden, beide sind Teil einer CPU-Speichereinheit **26** in der Gerätestation.

[0058] Als nächstes wird nun ein zweites Ausführungsbeispiel der vorliegenden Erfindung Bezug nehmend auf Fig. 7 bis Fig. 10 beschrieben. Im zweiten Ausführungsbeispiel hat jedes auf einer CD-ROM aufgezeichnete Softwareprogramm einen ihm eindeutig zugewiesenen Softwareidentifikator DID, und seine entsprechende Datendatei DATA ist als eine verschlüsselte Datendatei EKa(DATA) gespeichert. Diese verschlüsselte Datendatei EKa(DATA) wurde mit einem Originalmedienumsetzschlüssel Ka erzeugt, der aus dem Softwareidentifikator DID und einem Originalschlüssel KM, der an einem Softwarelizenzzentrum verwaltet wird, erzeugt wurde. Das Softwarelizenzzentrum hat die Verantwortung für das Lizenzieren des Rechts, ihre kommerziellen Softwareprodukte zu kopieren. Bezüglich der Zielspeichermedien hat die MO-Disk des Nutzers eine Seriennummer, die als ein Speichermedienidentifikator Mid dient.

[0059] Fig. 7 ist ein Flussdiagramm eines Softwareduplizierungsvorgangs, der unter der obigen Annahme durch das Softwarekopiersystem des zweiten Ausführungsbeispiels durchgeführt wird.

[0060] Um eine Kopie eines auf einer CD-ROM vertriebenen Softwareprogramms zu erhalten, ist es notwendig, durch die folgenden sieben Schritte zu gehen:

[0061] (S11) Der auf der Ziel-MO-Disk aufgezeichnete Speichermedienidentifikator Mid und der Softwareidentifikator DID des betreffenden Softwareprogramms auf der CD-ROM werden vom Endnutzerstandort an das Softwarelizenzzentrum, welches die Lizenz zum Kopieren der Softwareprodukte kontrolliert, gesendet.

[0062] (S12) Am Softwarelizenzzentrum wird überprüft, ob der Softwareidentifikator DID darin registriert ist oder nicht.

[0063] (S13) Der Speichermedienidentifikator Mid und der Softwareidentifikator DID werden durch den im Softwarelizenzzentrum verwalteten Originalschlüssel KM verschlüsselt, wodurch ein Speichermedienumsetzschlüssel Ku bzw. Originalmedienumsetzschlüssel Ka erzeugt werden.

[0064] (S14) Ein chiffrierter Text EMid(Ku, Ka) wird durch Verschlüsseln dieser Speichermedien- und Originalmedienumsetzschlüssel Ku und Ka unter Verwendung des Speichermedienidentifikators Mid erzeugt. Der chiffrierte Text EMid(Ku, Ka) wird zum Endnutzerstandort als eine Antwortnachricht auf die Anfrage geschickt.

[0065] (S15) Der Endnutzerstandort erhält den Speichermedienumsetzschlüssel Ku und den Originalmedienumsetzschlüssel Ka durch Entschlüsseln des empfangenen chiffrierten Textes EMid(Ku, Ka) mit dem Speichermedienidentifikator MID, wobei ein chiffrierter Text EMid(Ku), d.h. ein die MO-Disk betreffender Teil des chiffrierten Textes EMid(Ku, Ka) ohne Versuch einer Entschlüsselung gespeichert wird.

[0066] (S16) Mit dem in Schritt (S15) erhaltenen Originalmedienumsetzschlüssel Ka wird die verschlüsselte Datendatei EKa(DATA) auf der CD-ROM, die dem Softwareidentifikator DID entspricht, entschlüsselt, um die ursprüngliche Klartext-Datendatei DATA wiederherzustellen.

[0067] (S17) Die Klartext-Datendatei DATA wird wieder mit dem in Schritt (S15) erhaltenen Speichermedienumsetzschlüssel Ku verschlüsselt, und die verschlüsselte Datendatei wird auf die MO-Disk gespeichert, wodurch der Softwareduplizierungsvorgang abgeschlossen wird.

[0068] Der oben beschriebene Softwareduplizierungsprozess wird nun in mehr Einzelheiten diskutiert. Im zweiten Ausführungsbeispiel der vorliegenden Erfindung startet der Prozess am Endnutzerstandort mit dem Senden eines Antrags an das Softwarelizenzzentrum, welcher Teil des Prozesses nur aus zwei Dingen wie folgt besteht. Eines ist das Auslesen des Speichermedienidentifikators Mid der Ziel-MO-Disk und des Softwareidentifikators DID der auf der CD-ROM gespeicherten betreffenden Software, und das andere ist das Senden dieser Identifikatoren Mid und DID an das Softwarelizenzzentrum. Die folgende Beschreibung überspringt diese zwei Schritte und beginnt mit den durch das Softwarelizenzzentrum ausgeführten Schritten, das den obigen Antrag vom Endnutzerstandort empfangen hat.

[0069] Fig. 8 erläutert den am Softwarelizenzzentrum ausgeführten Prozess. Beim Empfang der zwei Identifikatoren Mid und DID vom Endnutzerstandort durch eine Kommunikationsleitung leitet das Softwarelizenzzentrum den Speichermedienidentifikator Mid an eine Verschlüsselungseinheit **31** mit dem Originalschlüssel KM unter der Steuerung des Zentrums weiter und führt auch den Softwareidentifikator DID einem Vergleicher **32** zu. Die Verschlüsselungseinheit **31** verschlüsselt den Speichermedienidentifikator Mid unter Verwendung des Originalschlüssels KM, um einen Speichermedienumsetzschlüssel Ku zu erzeugen. Der Vergleicher **32** sucht andererseits eine Inhaltsidentifikatordatei **33**, die jeden Eintrag mit dem empfangenen Softwareidentifikator DID vergleicht, um seine Gültigkeit zu verifizieren. Falls der empfangene Softwareidentifikator DID mit dem einen registrierten in der Inhaltsidentifikatordatei **33** übereinstimmt, schließt der Vergleicher **32** einen Schalter **34**, wodurch der Softwareidentifikator DID einer Verschlüsselungseinheit **35** mit dem Originalschlüssel KM eingegeben werden kann. Die Verschlüsselungseinheit **35** verschlüsselt den Softwareidentifikator DID mit dem Originalschlüssel KM, um einen Originalmedienumsetzschlüssel Ka zu erzeugen. Der durch die Verschlüsselungseinheit **31** erzeugte Speichermedienumsetzschlüssel Ku und der durch die Verschlüsselungseinheit **35** erzeugte Originalmedienumsetzschlüssel Ka werden dann einer Verschlüsselungseinheit **36** zur weiteren Verschlüsselung unter Verwendung des Speichermedienidentifikators Mid eingegeben. Ein durch die Verschlüsselungseinheit **36** erzeugter chiffrierter Text EMid(Ku, Ka) wird an den anfragenden Endnutzer durch die Kommunikationsleitung übertragen. Beim Abschluss der obigen Prozessschritte wird eine Anfrage zur Rechnungsstellung an die Nutzerprofildatenbank **37** ausgegeben und die Kosten werden an den anfragenden Endnutzer berechnet.

[0070] Fig. 9 erläutert den Prozess am Endnutzerstandort, nachdem der oben beschriebene Vorgang am Softwarelizenzzentrum beendet ist. Der vom Softwarelizenzzentrum empfangene chiffrierte Text EMid(Ku, Ka) wird einer Entschlüsselungseinheit **51** gegeben, wobei ein chiffrierter Text EMid(Ku) als Teil des empfangenen chiffrierten Textes EMid(Ku, Ka) in einen vorbestimmten Bereich **41** auf der Ziel-MO-Disk **40** geschrieben wird. Die Entschlüsselungseinheit **51** entschlüsselt den chiffrierten Text EMid(Ku, Ka) unter Verwendung des von der MO-Disk **40** extrahierten Speichermedienidentifikators Mid, wodurch der ursprüngliche Speichermedienumsetzschlüssel Ku und Originalmedienumsetzschlüssel Ka wiederhergestellt werden. Dieser wiederhergestellte Originalmedienumsetzschlüssel Ka wird dann einer Entschlüsselungseinheit **52** als ihr Entschlüsselungsschlüssel eingegeben, während der wiederhergestellte Speichermedienumsetzschlüssel Ku einer Verschlüsselungseinheit **53** als ihr

Verschlüsselungsschlüssel eingegeben wird. Die Entschlüsselungseinheit **52** ruft die verschlüsselte Datendatei EKa(DATA) ab, die dem Softwareidentifikator DID in der CD-ROM **60** entspricht, und entschlüsselt sie mit dem Originalmedienumsetzschlüssel Ka, wodurch die ursprüngliche Klartext-Datendatei DATA wiederhergestellt wird. Diese Datendatei DATA wird durch die Verschlüsselungseinheit **53** mit dem Speichermedienumsetzschlüssel Ku wieder verschlüsselt, und der resultierende chiffrierte Text EKu/DATA) wird auf die Ziel-MO-Disk **40** geschrieben.

[0071] Auf die oben beschriebene Weise wird der chiffrierte Text EKu(DATA) durch den Vorgang unter Verwendung von zwei Umsetzschlüsseln, die aus einem auf der MO-Disk **40** aufgezeichneten eindeutigen Identifikator abgeleitet werden, und eines Originalschlüssels unter der Steuerung des Softwarelizenzzentrums in die MO-Disk **40** geschrieben. Als nächstes wird nun ein Prozess zum Ausführen dieser verschlüsselten Datendatei EKu/DATA) beschrieben.

[0072] Fig. 10 zeigt einen Prozess des Ausführens des Softwareprogramms, das als eine Datendatei in der MO-Disk **40** dupliziert ist. Der chiffrierte Text EMid(Ku) ist in einem Abschnitt **41** als Teil des überschreibbaren Bereichs auf der MO-Disk **40** gespeichert, während der Speichermedienidentifikator Mid in einem nicht überschreibbaren Bereich **42** aufgezeichnet ist. Die verschlüsselte Datendatei EKu(DATA) ist in einem Abschnitt im übrigen überschreibbaren Bereich gespeichert. Wenn das Programm in der verschlüsselten Datendatei EKu(DATA) zur Ausführung aufgerufen wird, werden der Speichermedienidentifikator Mid und der chiffrierte Text EMid(Ku) von der MO-Disk **40** abgerufen und einer Entschlüsselungseinheit **54** eingegeben. Unter Verwendung des Speichermedienidentifikators Mid als dem Entschlüsselungsschlüssel entschlüsselt die Entschlüsselungseinheit **54** den chiffrierten Text EMid(Ku), um den Speichermedienumsetzschlüssel Ku wiederherzustellen. Eine weitere Entschlüsselungseinheit **55** entschlüsselt dann die von der MO-Disk **40** abgerufene verschlüsselte Datendatei EKu(DATA) unter Verwendung des Speichermedienumsetzschlüssels Ku als dem Entschlüsselungsschlüssel. Die resultierende Klartext-Datendatei DATA wird dann nach dem Laden in den Hauptspeicher eines Personal Computers, der an der Endnutzergerätestation arbeitet, ausgeführt.

[0073] Die obige Diskussion wird wie folgt zusammengefasst. Gemäß der vorliegenden Erfindung weist das Softwarekopiersystem eine am Zentralstandort angeordnete Signaturerzeugungseinrichtung zum Erzeugen einer Signatur aus Informationen, die das Zielspeichermedium und die im Originalmedium gespeicherten betreffenden Daten identifizieren, auf. Das System weist auch am Endnutzerstandort eine Signaturschreibeinrichtung zum Schreiben der durch die Signaturerzeugungseinrichtung erzeugten Signatur in das Zielspeichermedium, eine Signaturerzeugungs/vergleichseinrichtung zum Vergleichen einer Signatur, die lokal am Endnutzerstandort erzeugt wird, mit der im Zielspeichermedium geschriebenen Signatur, und eine Datenkopiereinrichtung zum Kopieren des bestreffenden Programms auf das Zielspeichermedium entsprechend dem Ergebnis des Vergleichs auf. Deshalb hat der Zentralstandort nur eine zu dem Identifikator des Zielspeichermediums gehörende Signatur auszugeben und es besteht keine Notwendigkeit, lizenzspezifische Informationen in engem Kontakt mit Fabriken der Speichermedienhersteller zu verwalten. Dies beseitigt auch die Lagerkontrolle bei den Herstellern und Händlern für die beim Kopieren von Software zu benutzenden Speichermedien.

[0074] Die obige Erläuterung soll für die Grundsätze der vorliegenden Erfindung nur als beispielhaft angesehen werden. Da zahlreiche Modifikationen und Änderungen für den Fachmann offensichtlich sein werden, ist es weiter nicht erwünscht, die Erfindung auf die exakte Konstruktion und die exakten Anwendungen, die dargestellt und beschrieben sind, einzuschränken, und demgemäß sollen alle geeigneten Modifikationen und Äquivalente so angesehen werden, dass sie in den Schutzumfang der Erfindung in den anhängenden Ansprüchen fallen.

Patentansprüche

1. Softwarekopierverfahren zum Duplizieren von Software, die in einem Originalspeichermedium (**1**) aufgezeichnet ist, auf ein Zielspeichermedium (**3**) in einer legitimen Weise, die durch Kommunikationen zwischen einem Endnutzerstandort, der eine Lizenz zum Kopieren der Software beantragt, und einem Zentralstandort (**5**) der die Lizenz verwaltet, erzielt wird, wobei das Softwarekopierverfahren die Schritte aufweist:

– Senden eines Speichermedienidentifikators (IDk), der dem Zielspeichermedium (**3**) eindeutig zugeordnet ist, und eines Inhaltsidentifikators (SIDi), der einer betreffenden Datendatei eindeutig zugeordnet ist, zusammen mit einer eine Softwarelizenz beantragenden Nachricht vom Endnutzerstandort zum Zentralstandort (**5**);

– Erzeugen eines ersten Bescheinigungscodes (CS), der als eine Signatur dient, am Zentralstandort (**5**) aus dem Speichermedienidentifikator (IDK) und dem Inhaltsidentifikator (SIDi), die von der Endnutzerseite empfangen wurden, durch einen Signaturerzeugungsvorgang, der einen Bescheinigungsschlüssel (KEYc) benutzt, der am Zentralstandort (**5**) verwaltet wird;

– Erzeugen eines verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)) durch Verschlüsseln des Bescheinigungsschlüssels (KEYc) unter Verwen-

dung eines Nutzerschlüssels (KU) am Zentralstandort;
– Senden des ersten Bescheinigungscodes (CS) und des verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)) vom Zentralstandort (**5**) zum Endnutzerstandort;
– Schreiben des ersten Bescheinigungscodes (CS) und des verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)), die vom Zentralstandort (**5**) empfangen wurden, am Endnutzerstandort in das Zielspeichermedium (**3**);
– Erhalten eines entschlüsselten Bescheinigungsschlüssels (KEYc) durch Entschlüsseln des verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)), der im Zielspeichermedium (**3**) gespeichert ist, unter Verwendung des Nutzerschlüssels (KU) am Endnutzerstandort;
– Erzeugen eines zweiten Bescheinigungscodes (CS') für einen Nachprüfzweck durch Anwenden eines Signaturerzeugungsvorgangs, der den entschlüsselten Bescheinigungsschlüssel (KEYc) verwendet, auf den Speichermedienidentifikator (IDk) und den Inhaltsidentifikator (SIDi) am Endnutzerstandort;
– Vergleichen des im Zielspeichermedium **13**) gespeicherten ersten Bescheinigungscodes (CS) mit dem zweiten Bescheinigungscode (CS'), der am Endnutzerstandort erzeugt wird; und
– Auslesen der im Originalspeichermedium (**1**) gespeicherten betreffenden Datendatei und Schreiben der betreffenden Datendatei in das Zielspeichermedium (**3**), falls der erste und der zweite Bescheinigungscode (CS, CS') übereinstimmen.

2. Softwarekopiersystem zum Duplizieren einer in einem Originalspeichermedium (**1**) aufgezeichneten Software auf ein Zielspeichermedium (**3**) in einer legitimierten Weise, die durch Kommunikationen zwischen einem Endnutzerstandort, der eine Lizenz zum Kopieren der Software beantragt, und einem Zentralstandort (**5**), der die Lizenz verwaltet, erreicht wird, wobei das Softwarekopiersystem aufweist:
– eine Einrichtung zum Senden eines Speichermedienidentifikators (IDK), der dem Zielspeichermedium (**3**) eindeutig zugeordnet ist, und eines Inhaltsidentifikators (SIDi), der einer betreffenden Datendatei eindeutig zugeordnet ist, zusammen mit einer eine Softwarelizenz beantragenden Nachricht vom Endnutzerstandort zum Zentralstandort (**5**);
– eine Einrichtung (**6**) zum Erzeugen eines ersten Bescheinigungscodes (CS), der als eine Signatur dient, am Zentralstandort (**5**) aus dem Speichermedienidentifikator (IDk) und dem Inhaltsidentifikator (SIDi), die von der Endnutzerseite empfangen wurden, durch einen Signaturerzeugungsvorgang, der einen Bescheinigungsschlüssel (KEYc) benutzt, der am Zentralstandort (**5**) verwaltet wird;
– eine Einrichtung zum Erzeugen eines verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)) durch Verschlüsseln des Bescheinigungsschlüssels (KEYc) unter Verwendung eines Nutzerschlüssels (Ku) am Zentralstandort;
– eine Einrichtung zum Senden des ersten Bescheinigungscodes (CS) und des verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)) vom Zentralstandort (**5**) zum Endnutzerstandort;
– eine Einrichtung zum Schreiben des ersten Bescheinigungscodes (CS) und des verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)), die vom Zentralstandort (**5**) empfangen wurden, am Endnutzerstandort in das Zielspeichermedium (**3**);
– eine Einrichtung zum Erhalten eines entschlüsselten Bescheinigungsschlüssels (KEYc) durch Entschlüsseln des verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)), der im Zielspeichermedium (**3**) gespeichert ist, unter Verwendung des Nutzerschlüssels (Ku) am Endnutzerstandort;
– eine Einrichtung (**8**) zum Erzeugen eines zweiten Bescheinigungscodes (CS') für einen Nachprüfzweck durch Anwenden eines Signaturerzeugungsvorgangs, der den entschlüsselten Bescheinigungsschlüssel (KEYc) verwendet, auf den Speichermedienidentifikator (IDk) und den Inhaltsidentifikator (SIDi) am Endnutzerstandort;
– eine Einrichtung (**8**) zum Vergleichen des im Zielspeichermedium (**3**) gespeicherten ersten Bescheinigungscodes (CS) mit dem zweiten Bescheinigungscode (CS'), der am Endnutzerstandort erzeugt wird; und
– eine Einrichtung zum Auslesen der im Originalspeichermedium (**1**) gespeicherten betreffenden Datendatei und zum Schreiben der betreffenden Datendatei in das Zielspeichermedium (**3**), falls der erste und der zweite Bescheinigungscode (CS, CS') übereinstimmen.

3. Softwarekopiersystem nach Anspruch 2, bei welcher die Einrichtung (**6**) zum Erzeugen von Bescheinigungscodes aufweist:
– eine Signaturverarbeitungseinrichtung (**14**) zum Verschlüsseln des durch eine Inhaltsidentifikator-Leseeinrichtung (**2**) gelesenen ersten Identifikators (SIDi) und des durch eine Speichermedienidentifikator-Leseeinrichtung (**4**) gelesenen zweiten Identifikators (IDk) unter Verwendung eines am Zentralstandort (**5**) verwalteten Bescheinigungsschlüssels (KEYc), um einen Bescheinigungscode (CS), der als die erste Signatur (CS) dient, zu erzeugen und zu übertragen, und
– eine Verschlüsselungseinrichtung (**15**) zum Verschlüsseln des Bescheinigungsschlüssels (KEYc) unter Verwendung eines am Zentralstandort (**5**) registrierten Nutzerschlüssels (Ku) und Senden des verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)) zur Verwendung in der Einrichtung (**8**) zum Erzeugen von Bescheinigungscodes, um die zweite Signatur (CS') zu erzeugen.

4. Softwarekopiersystem nach Anspruch 3, bei welcher die Einrichtung (**8**) zum Erzeugen von Be-

scheinigungscodes aufweist:
– eine Entschlüsselungseinrichtung (**16**) zum Entschlüsseln des verschlüsselten Bescheinigungsschlüssels (EKU(KEYc)) unter Verwendung des Nutzerschlüssels (Ku), der am Zentralstandort (**5**) registriert ist, um einen entschlüsselten Bescheinigungsschlüssel zu erzeugen,
– eine Bescheinigungscode-Erzeugungseinrichtung (**17**) zum Erzeugen eines weiteren Bescheinigungscodes (CS') zur Nachprüfung, der als die zweite Signatur (CS') dient, durch Verschlüsseln des durch eine Inhaltsidentifikator-Leseeinrichtung (**2**) gelesenen ersten Identifikators (SIDi) und des durch eine Speichermedienidentifikator-Leseeinrichtung (**4**) gelesenen zweiten Identifikators (IDk) unter Verwendung des entschlüsselten Bescheinigungsschlüssels (KEYc), und
– eine Vergleichseinrichtung (**18**) zum Vergleichen des Bescheinigungscodes (CS') zur Nachprüfung, der durch die Bescheinigungscode-Erzeugungseinrichtung (**17**) erzeugt wurde, mit dem Bescheinigungscode (CS), der als die erste Signatur (CS) im Zielspeichermedium (**3**) gespeichert ist.

Es folgen 10 Blatt Zeichnungen

Anhängende Zeichnungen

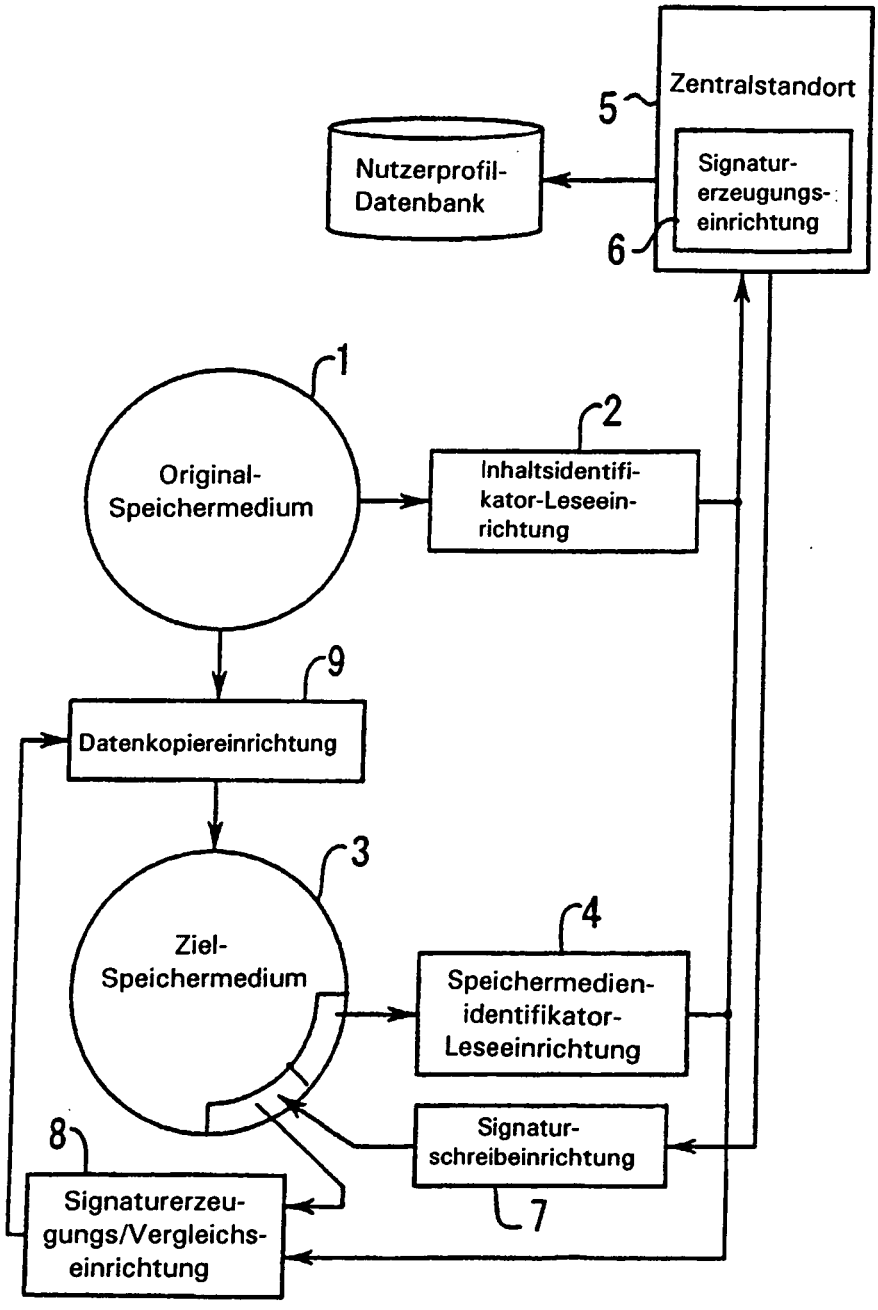


FIG. 1

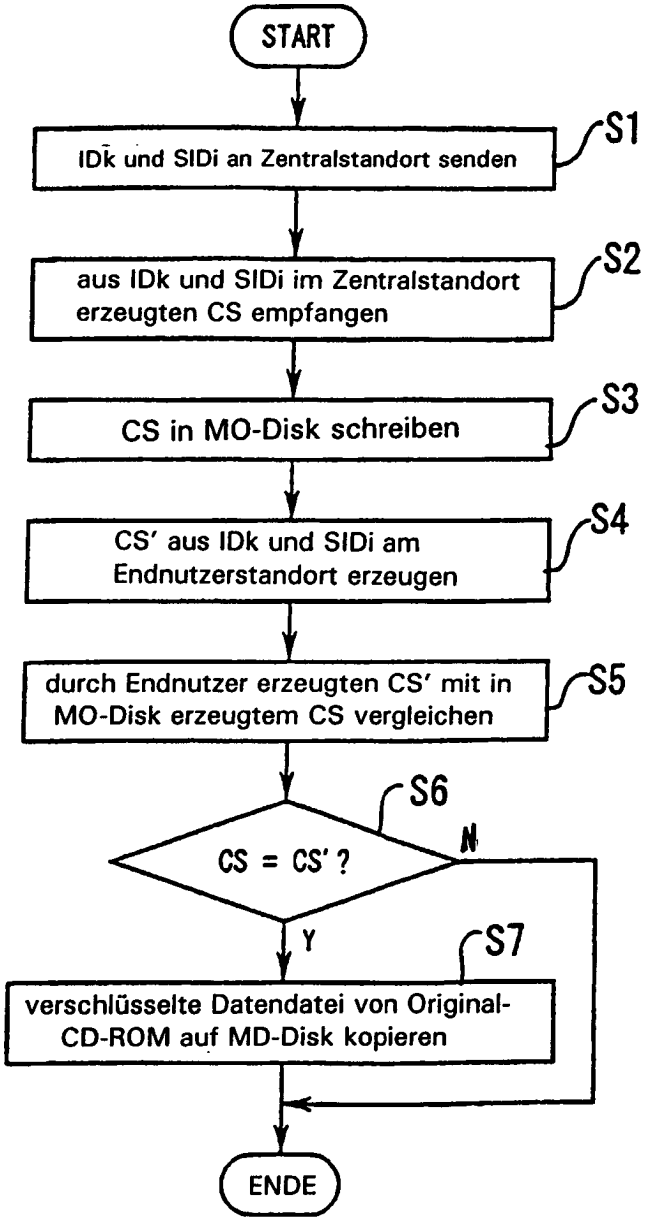

START
IDk und SIDi an Zentralstandort senden
S1
aus IDk und SIDi im Zentralstandort erzeugten CS empfangen
S2
CS in MO-Disk schreiben
S3
CS' aus IDk und SIDi am Endnutzerstandort erzeugen
S4
durch Endnutzer erzeugten CS' mit in MO-Disk erzeugtem CS vergleichen
S5
S6
CS = CS' ?
N
Y
S7
verschlüsselte Datendatei von Original-CD-ROM auf MD-Disk kopieren
ENDE

FIG. 2

FIG. 3 (A)

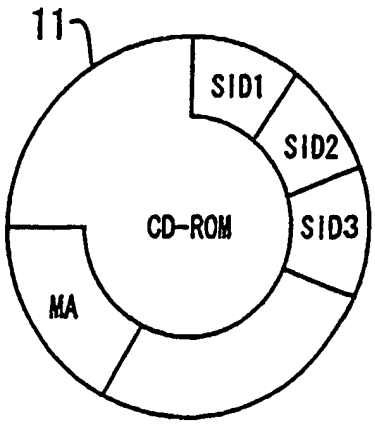
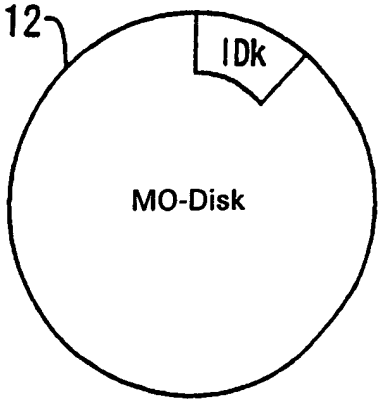


FIG. 3 (B)



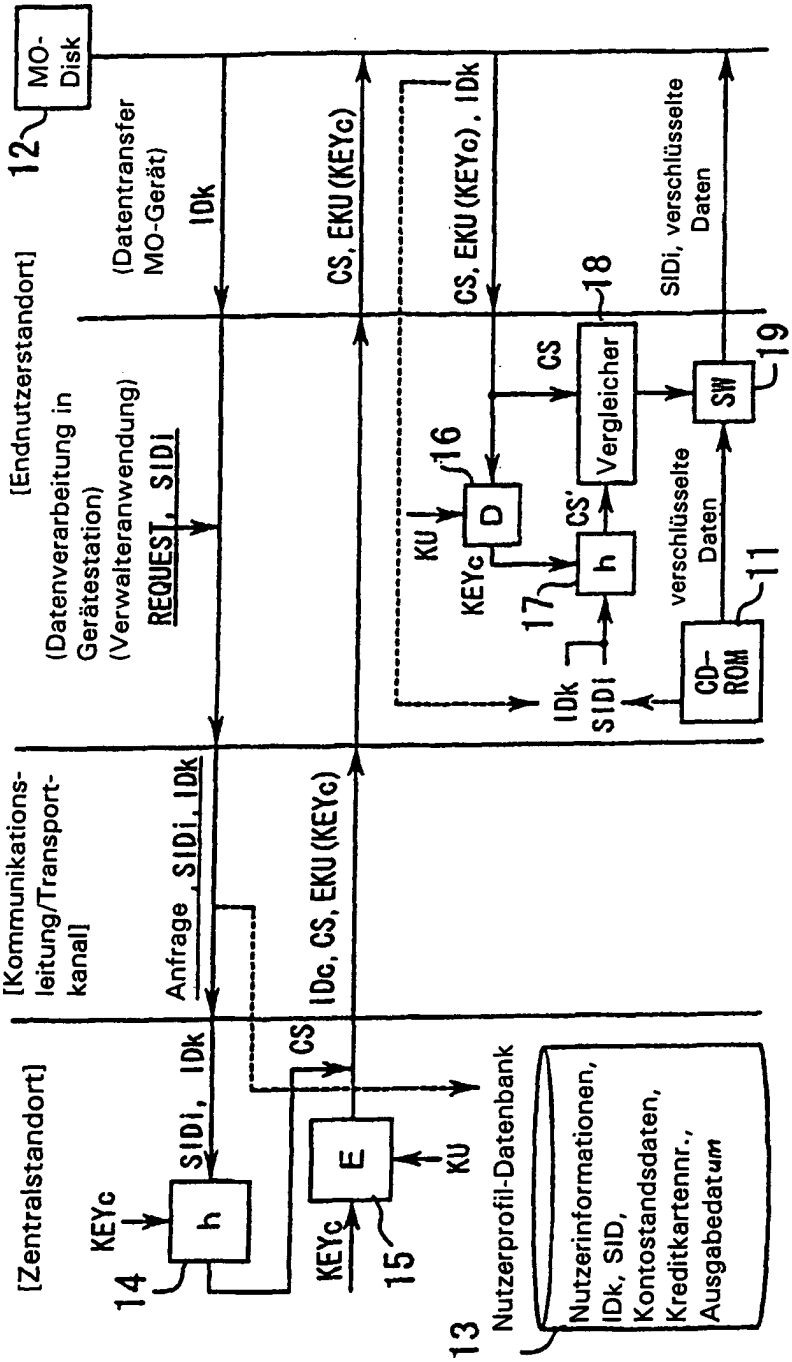

[Zentralstandort]
[Kommunikations-leitung/Transport-kanal]
[Endnutzerstandort]
(Datenverarbeitung in Gerätestation)
(Verwalteranwendung)
(Datentransfer MO-Gerät)
MO-Disk
12
REQUEST, SIDi
Anfrage, SIDi, IDk
IDc, CS, EKU(KEYc)
IDk
CS, EKU(KEYc)
CS, EKU(KEYc), IDk
SIDi, verschlüsselte Daten
verschlüsselte Daten
KEYc
14
h
SIDi, IDk
CS
E
KEYc
15
KU
13
Nutzerprofil-Datenbank
Nutzerinformationen, IDk, SID, Kontostandsdaten, Kreditkartennr., Ausgabedatum
KU
16
D
KEYc
17
h
CS'
Vergleicher
18
CS
SW
19
IDk
SIDi
CD-ROM
11

FIG. 4

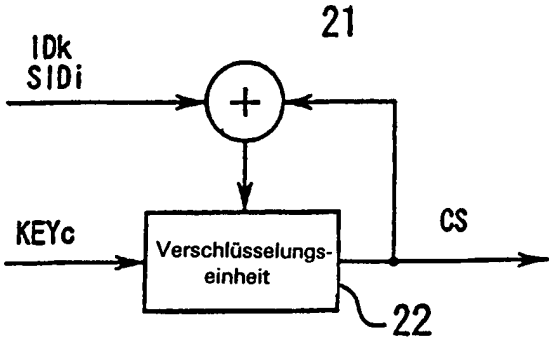


FIG. 5

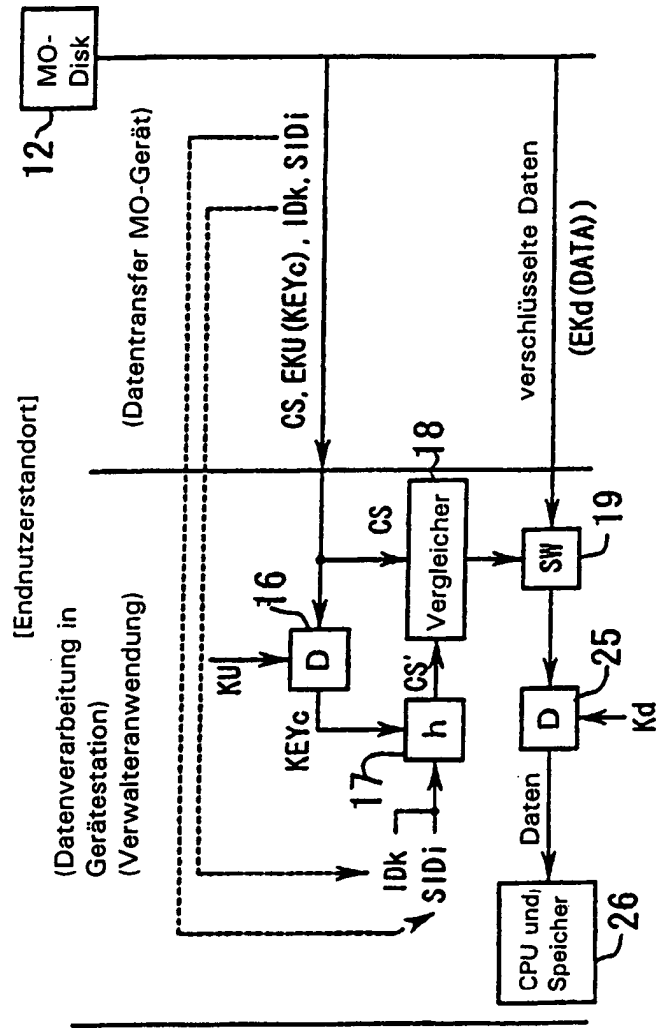

MO-Disk
12
(Datentransfer MO-Gerät)
CS, EKU(KEYc), IDk, SIDi
verschlüsselte Daten
(EKd(DATA))
[Endnutzerstandort]
(Datenverarbeitung in Gerätestation)
(Verwalteranwendung)
18
CS
Vergleicher
SW
19
16
KU
D
KEYc
h
CS'
17
IDk
SIDi
D
25
Kd
Daten
CPU und Speicher
26

FIG. 6

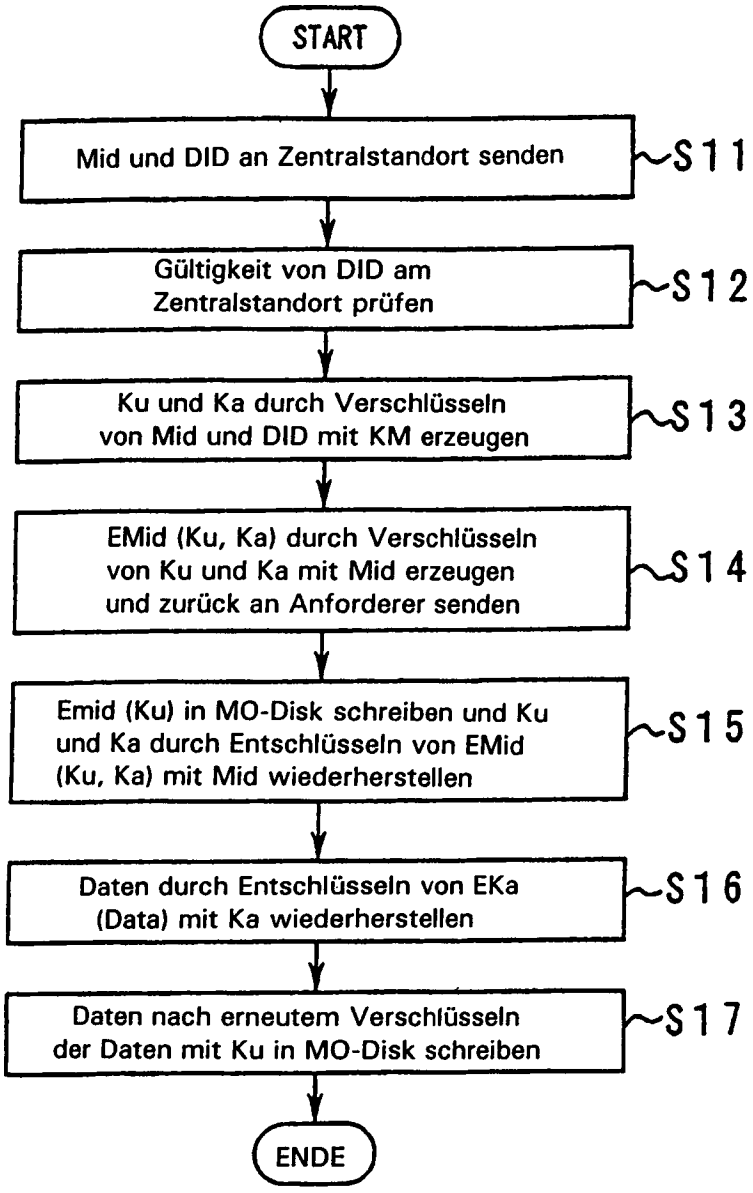

START
Mid und DID an Zentralstandort senden
S11
Gültigkeit von DID am Zentralstandort prüfen
S12
Ku und Ka durch Verschlüsseln von Mid und DID mit KM erzeugen
S13
EMid (Ku, Ka) durch Verschlüsseln von Ku und Ka mit Mid erzeugen und zurück an Anforderer senden
S14
Emid (Ku) in MO-Disk schreiben und Ku und Ka durch Entschlüsseln von EMid (Ku, Ka) mit Mid wiederherstellen
S15
Daten durch Entschlüsseln von EKa (Data) mit Ka wiederherstellen
S16
Daten nach erneutem Verschlüsseln der Daten mit Ku in MO-Disk schreiben
S17
ENDE

FIG. 7

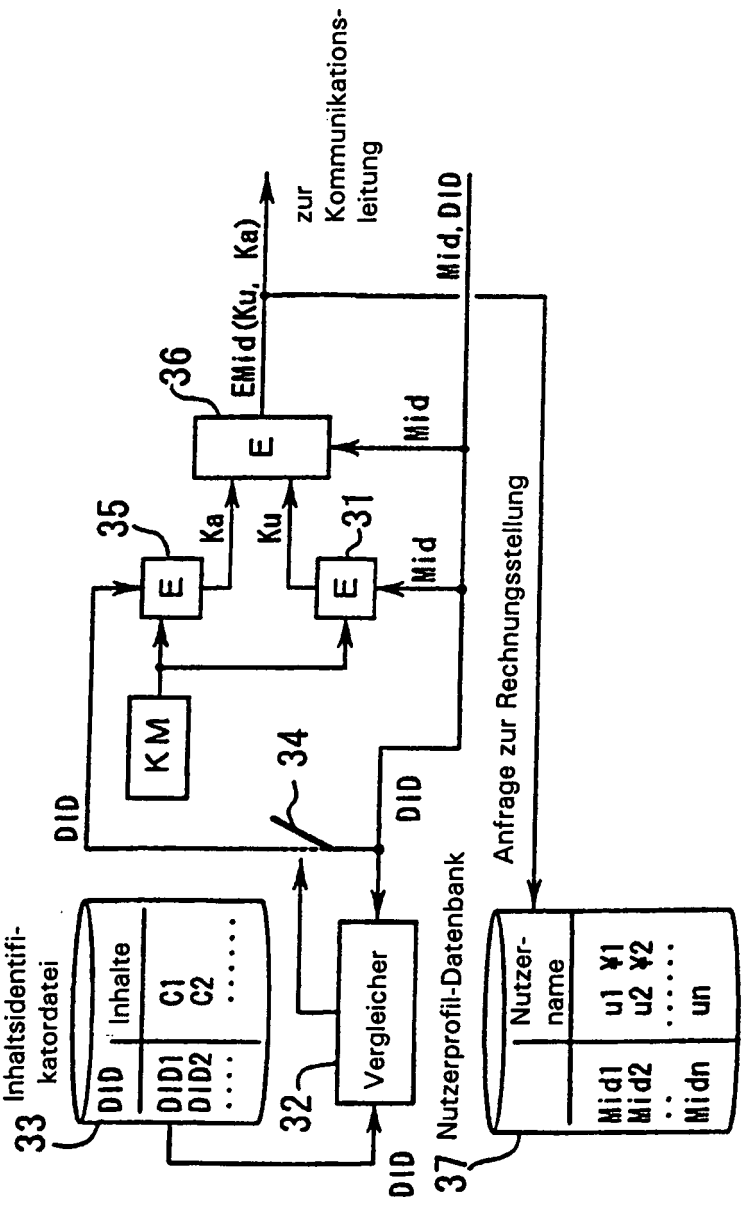

zur Kommunikations-leitung
EMid(Ku, Ka)
Mid, DID
36
E
Mid
35
Ka
Ku
31
E
E
Mid
KM
34
DID
DID
Anfrage zur Rechnungsstellung
Inhaltsidentifi-katordatei
DID
Inhalte
DID1
DID2
C1
C2
33
32
Vergleicher
DID
Nutzerprofil-Datenbank
Nutzer-name
u1 ¥1
u2 ¥2
un
Mid1
Mid2
Midn
37

FIG. 8

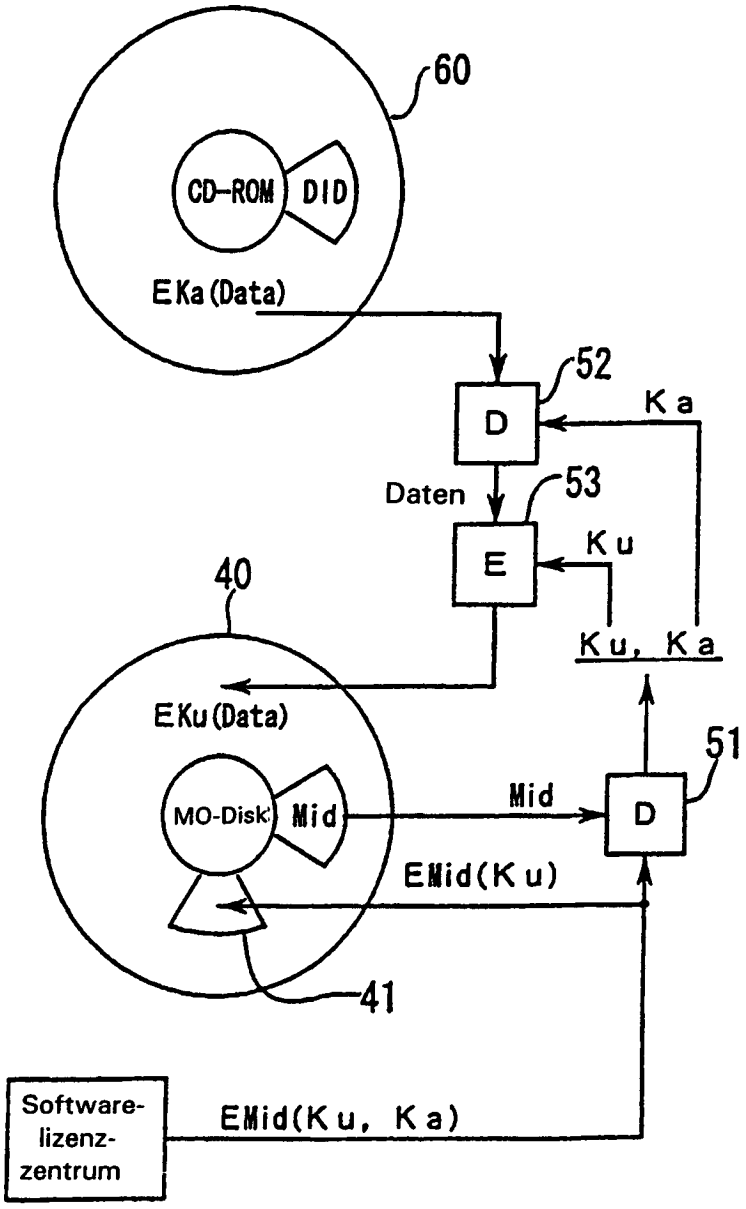

60
CD-ROM
DID
EKa(Data)
52
D
Ka
Daten
53
E
Ku
40
Ku, Ka
EKu(Data)
51
MO-Disk
Mid
Mid
D
EMid(Ku)
41
Software-
lizenz-
zentrum
EMid(Ku, Ka)

FIG. 9

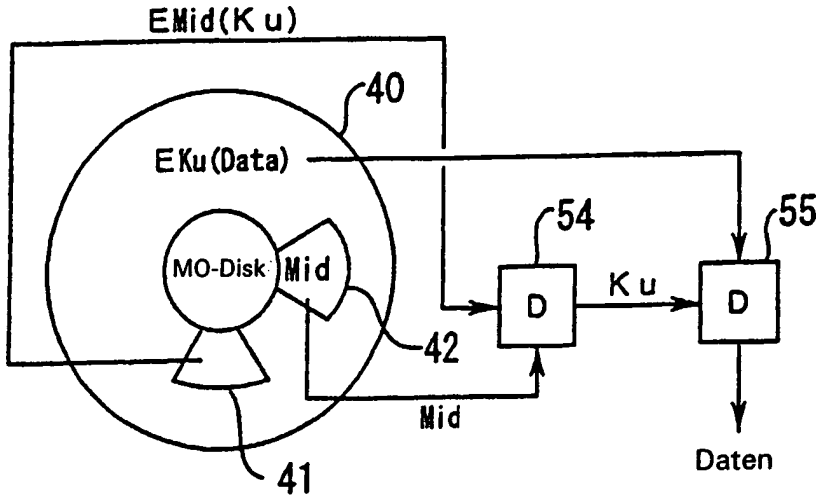


FIG. 10