(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
2. März 2006 (02.03.2006)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2006/021383 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00, G11B 20/00

(21) Internationales Aktenzeichen: PCT/EP2005/008997

(22) Internationales Anmeldedatum:
19. August 2005 (19.08.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 040 462.3 20. August 2004 (20.08.2004) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **BRÄUTIGAM, Thomas** [DE/DE]; Kapellenstrasse 56a, 83083 Riedering (DE). **JOHNE, Andreas** [DE/DE]; Bahnhofstrasse 47a, 82194 Gröbenzell (DE).

(74) Anwalt: **KLUNKER.SCHMITT-NILSON.HIRSCH**; Winzererstrasse 106, 80797 München (DE).

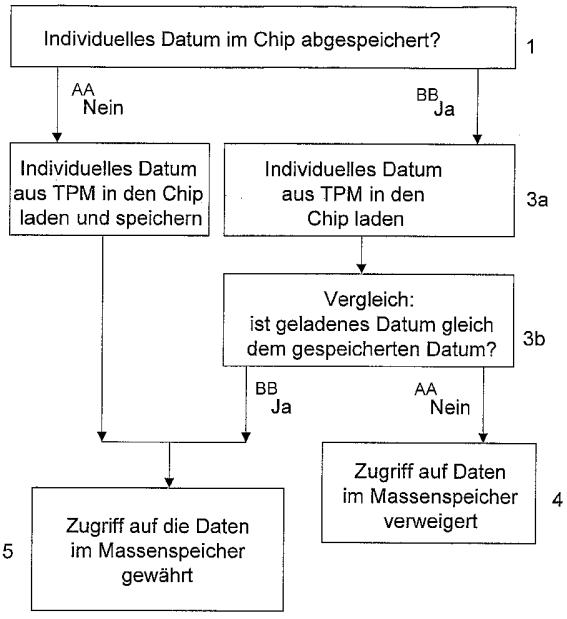
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW,

[Fortsetzung auf der nächsten Seite]

(54) Title: AUTHENTICATION-SECURED ACCESS TO A DATA CARRIER COMPRISING A MASS STORAGE DEVICE AND CHIP

(54) Bezeichnung: DURCH AUTHENTISIERUNG GESICHERTER ZUGRIFF AUF EINEN DATENTRÄGER MIT MASSENSPEICHER UND CHIP



1. INDIVIDUAL DATUM STORED IN CHIP?
AA. NO
BB. YES
2. INDIVIDUAL DATUM FROM TPM LOADED AND STORED IN THE CHIP
3a. INDIVIDUAL DATUM FROM TPM STORED IN THE CHIP
3b. COMPARISON: IS LOADED DATUM THE SAME AS THE STORED DATUM
5. ACCESS TO DATA IN MASS STORAGE DEVICE GRANTED
4. ACCESS TO DATA IN MASS STORAGE DEVICE REFUSED

(57) Abstract: The invention relates to a method for accessing the mass storage device of a data carrier comprising a mass storage device and a chip. Said data carrier is personalised on a service device for accessing the data carrier, by means of an individual datum of the service device, that is stored in the chip, such that the data carrier can only be used with said service device.

(57) Zusammenfassung: Die Erfindung schafft ein Verfahren zum Zugreifen auf den Massenspeicher eines Datenträgers mit einem Massenspeicher und einem Chip. Der Datenträger ist oder wird durch ein individuelles Datum einer Nutzungseinrichtung, die in dem Chip abgespeichert wird bzw. bereits dort abgespeichert ist, auf eine Nutzungseinrichtung zum Zugreifen auf den Datenträger personalisiert, damit der Datenträger nur mit dieser Nutzungseinrichtung genutzt werden kann.

WO 2006/021383 A1

GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Durch Authentisierung gesicherter Zugriff auf einen Datenträger mit Massenspeicher und Chip

Die Erfindung betrifft ein Verfahren zum Zugreifen auf den Massenspeicher eines Datenträgers mit einem Massenspeicher und einem Chip, wobei für die Nutzung der Daten eine Authentisierung zwingend erforderlich ist. Weiter betrifft die Erfindung einen entsprechenden durch ein Erfordernis der Authentisierung gesicherten Datenträger, sowie ein Verfahren zum Laden von Daten in einen solchen Datenträger.

Der Datenträger im Sinn der Erfindung mit einem Massenspeicher ist z.B. ein Datenträger mit einem optischen (Massen-)Speicher wie z.B. einen Compact-Disk (CD), wiederbeschreibbare CD (CD-RW), Digital Versatile Disk (DVD) oder DVD-RW. Alternativ kann als Datenträger ein Datenträger mit einem elektronischen Massenspeicher wie z.B. einem Flash-Speicher, ROM oder EEPROM-Speicher vorgesehen sein, z.B. eine Compact Flash (CF) Speicherkarte, eine Secure Disk (SD) Speicherkarte, eine Multi Media Disk (MMD) oder eine ähnliche Speicherkarte, wie sie z.B. in digitalen Multimediageräten wie z.B. Digitalkameras, Camcordern, MP3-Playern und dergleichen verwendet wird. Ein Datenträger mit einem optischen Massenspeicher hat wahlweise eine runde Form, entsprechend einer üblichen CD oder DVD. Alternativ hat der Datenträger mit einem optischen Massenspeicher eine rechteckige Form, entsprechend einer Chipkarte, die z.B. die Außenmaße einer Chipkarte gemäß ISO/IEC 7816 hat, die aber zusätzlich ein Mittelloch und einen ringförmigen Massenspeicher hat, wobei die Außenmaße des Datenträgers in Bezug auf das Mittelloch die Abmessungen einer üblichen CD oder DVD nicht überschreiten, so dass der optische Massenspeicher des Datenträgers in einem handelsüblichen CD- oder DVD-Laufwerk ausgelesen werden kann.

Der Chip bei der Erfindung ist vorzugsweise in ein Chipmodul integriert und derart kontaktiert, dass er mit einem Schreib- und/oder Lesegerät kontaktlos und/oder kontaktbehaftet kontaktierbar ist. Wahlweise ist der Chip gemäß ISO/IEC 7816 (kontaktbehaftet) bzw. ISO/IEC 10 536 (kontaktlos) bzw. ISO/IEC 14 443 (kontaktlos) kontaktierbar. Alternativ ist der Chip nach einem beliebigen anderen Protokoll kontaktierbar, z.B. USB, RS232/V.24.

Programm-Software zur Installation in Rechnern jeder Art wie z.B. Personal Computern oder Kleinrechnern (Personal Digital Assistant, Mobiltelefon) wird verbreitet in Datenträgern mit optischen Massenspeichern wie z.B. CDs oder DVDs ausgeliefert. Musikdaten und Filmdaten sind ebenfalls verbreitet in CDs und DVDs gespeichert. Multimediadaten für digitale Multimediageräte wie Digitalkameras, digitale Camcorder, Musik-/Film-Abspielgeräte wie MP3-Player und dergleichen sind häufig in Datenträgern mit elektronischen Massenspeichern gespeichert wie Compact Flash (CF) Speicherkarten, Secure Disk (SD) Speicherkarten etc.

Zum Schutz gegen Raubkopien sind die Daten im Massenspeicher häufig ganz oder teilweise verschlüsselt. Hierdurch sind die Daten beispielsweise unlesbar. Multimediadaten wie Musikdaten oder Filmdaten können durch die Verschlüsselung verzerrt oder verrauscht sein. Bei Demo-Versionen kann vorgesehen sein, dass die Daten mit Ausnahme eines zu Demonstrationszwecken freigegebenen Teils der Daten verschlüsselt sind.

Aus DE 196 16 819 A1 ist eine CD mit einem Chip als Zugriffsschutz für die Informationen der CD bekannt. Die CD hat einen kreisförmigen CD-Körper mit einer informationstragenden Schicht. Zusätzlich sind in die CD ein Chip und eine Spule zur kontaktlosen Übertragung von Daten zwischen dem Chip und einem Datenverarbeitungsgerät integriert. In dem Chip sind Daten

gespeichert und können Daten verarbeitet werden, ohne die keine oder keine korrekte Bearbeitung der auf der CD gespeicherten Informationen möglich ist. Die gespeicherten Daten im Chip sind z.B. Schlüssel oder Algorithmen zur Entschlüsselung der auf der CD gespeicherten Informationen.

Aus WO 00/51119 ist eine CD-ROM oder ähnliche optische Scheibe mit einem Chip als Zugriffsschutz für die Daten der CD-ROM bekannt. In der CD-ROM sind Daten abgespeichert, die ganz oder teilweise verschlüsselt sind. Der Chip enthält einen geheimen Schlüssel, mit dem sich die verschlüsselten Daten der CD-ROM entschlüsseln lassen, ohne dass der Schlüssel den Chip verlässt, sowie eine Datenaustauscheinrichtung. Vorzugsweise enthält der Chip den zum Entschlüsseln erforderlichen Kryptoprozessor. Der Schlüssel kann für jede CD-ROM individuell sein. Bei der Herstellung der CD-ROM werden Daten mit dem Schlüssel verschlüsselt und in die CD-ROM gespeichert. Der verwendete Schlüssel wird in den Chip gespeichert, zum wieder Entschlüsseln der verschlüsselten Daten. Bei der Nutzung der CD-ROM werden Daten aus der CD-ROM in einen Rechner ausgelesen und vom Rechner aus an den Chip gesandt. Im Chip werden die Daten mit dem Schlüssel entschlüsselt und schließlich über die Datenaustauscheinrichtung des Chips ausgegeben, z.B. an den Rechner. Für jede Nutzung der CD-ROM ist somit der Zugriff auf den Chip erforderlich. Daher ist eine Kopie der CD-ROM, bei der nur der optische Speicher kopiert wird, nicht funktionsfähig. Dadurch, dass die Daten innerhalb des Chips entschlüsselt werden und der Schlüssel den Chip nie verlässt, kann weiter der Schlüssel nicht kopiert werden. Folglich kann keine funktionsfähige Kopie der CD-ROM angefertigt werden.

Die aus WO 00/51119 bekannte CD-ROM mit dem Chip kann somit zwar nicht kopiert werden. Das Original der CD-ROM kann allerdings beliebig

genutzt, beispielsweise auf unterschiedlichen Computern bzw. Abspielgeräten, und beliebig an andere Nutzer weiterverliehen werden.

Häufig ist es gewünscht, dass nur der berechtigte Erstnutzer, z.B. der zahlende Käufer oder ein anderweitig Berechtigter, die CD-ROM nutzen kann. Dieses Problem ist bei der CD-ROM aus WO 00/51119 nicht gelöst.

Aus WO 02/11081 ist ein weiterer Datenträger (z.B. CD oder DVD) mit einem optischen Speicher, in dem Daten zumindest teilweise verschlüsselt abgespeichert sind, und mit einem Chip, in dem ein Schlüssel zum Entschlüsseln der verschlüsselten Daten abgespeichert ist, bekannt. Gemäß WO 02/11081 werden bei einem Verfahren zum Auslesen des Datenträgers die Daten mit einer Schreib/Lesevorrichtung aus dem optischen Speicher ausgelesen, an den Chip geliefert, innerhalb des Chips mit dem Schlüssel entschlüsselt und anschließend an die Schreib/Lesevorrichtung ausgegeben. Der Chip führt an der Schreib/Lesevorrichtung eine Authentifikationsprüfung durch. Nur nach einer positiv verlaufenen Authentifikationsprüfung der Schreib/Lesevorrichtung gibt der Chip eine Auslesen der in dem optischen Speicher enthaltenen verschlüsselten Daten durch die Schreib/-Lesevorrichtung frei. Wie das Erzwingen der Authentifikation erzielt wird, ist in WO 02/11081 nicht angegeben. Ein Datenträger, der eine solche Authentifikation erzwingt und somit die Daten im optischen Speicher gegen unbefugte Nutzung schützt, ist in WO 02/11081 ebenfalls nicht angegeben.

Ausgehend von dem aus WO 02/11081 bekannten Verfahren zum Auslesen von Daten aus dem Datenträger liegt der Erfindung die Aufgabe zu Grunde, ein sicheres Verfahren zum Zugreifen auf den Massenspeicher eines Datenträgers der eingangs genannten Art zu schaffen, bei dem für die Nutzung der Daten eine Authentisierung zwingend erforderlich ist, und einen ent-

sprechenden Datenträger sowie ein Verfahren zum Laden von Daten in einen solchen Datenträger anzugeben.

Die Aufgabe wird gelöst durch ein Verfahren nach einem der unabhängigen Verfahrensansprüche und durch einen Datenträger nach dem unabhängigen Vorrichtungsanspruch. Vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Das erfindungsgemäße Verfahren zum Zugreifen auf den Massenspeicher eines Datenträgers gemäß dem unabhängigen Anspruch 1 geht von einem Datenträger mit einem Massenspeicher und einem Chip aus. Für den Zugriff auf den Massenspeicher mittels einer Nutzungseinrichtung ist eine Authentisierung der Nutzungseinrichtung gegenüber dem Chip zwingend erforderlich. Gemäß der Erfindung wird das zwingende Erfordernis der Authentisierung dadurch erreicht, dass bei einem Zugriff einer Nutzungseinrichtung auf den Datenträger, um auf den Massenspeicher zuzugreifen, der Chip daraufhin überprüft wird, ob in dem Chip ein für die Nutzungseinrichtung individuelles Datum abgespeichert ist, durch das der Datenträger im Hinblick auf die Nutzungseinrichtung personalisiert ist. Der Zugriff auf den Massenspeicher des Datenträgers, in dem die begehrten Daten (Nutzdaten) abgespeichert sind, wird nur ermöglicht, falls in dem Chip mindestens ein vorbestimmtes individuelles Datum der Nutzungseinrichtung abgespeichert ist.

Falls in dem Chip kein individuelles Datum abgespeichert ist, wird der Zugriff auf den Massenspeicher des Datenträgers zumindest vorerst nicht gewährt. In dem Fall, wenn in dem Chip ein individuelles Datum abgespeichert ist, muss es sich um ein individuelles Datum genau der zugreifenden Nutzungseinrichtung handeln. Der Datenträger muss mit anderen Worten auf eine spezielle Nutzungseinrichtung personalisiert sein. Die in seinem

Massenspeicher abgespeicherten Daten (Nutzdaten) können nur mittels der Nutzungseinrichtung, auf die der Datenträger personalisiert ist, genutzt werden. Hierdurch kann beispielsweise festgelegt werden, dass nur ein vorbestimmter Computer oder ein vorbestimmter CD-Spieler oder DVD-Spieler oder Speicherkartenleser den Datenträger nutzen kann.

Daher ist gemäß Anspruch 1 ein besonders sicheres Verfahren zum Zugreifen auf den Massenspeicher bei einem Datenträger mit einem Massenspeicher und einem Chip geschaffen, bei dem für den Zugriff auf den Massenspeicher mittels einer Nutzungseinrichtung eine Authentisierung der Nutzungseinrichtung gegenüber dem Chip zwingend erforderlich ist.

Wahlweise ist der Chip mit mehreren unterschiedlichen individuellen Daten einer einzelnen Nutzungseinrichtung personalisiert.

Vorzugsweise wird, falls gemäß der Überprüfung kein individuelles Datum im Chip abgespeichert ist, mindestens ein vorbestimmtes individuelles Datum der Nutzungseinrichtung in den Chip gespeichert. Mit anderen Worten wird der Datenträger auf die Nutzungseinrichtung personalisiert, wenn er noch nicht auf eine spezifische Nutzungseinrichtung personalisiert ist, beispielsweise weil der Datenträger erstmalig in Betrieb genommen wird.

Weiter wird vorzugsweise, bevor das vorbestimmte individuelle Datum der Nutzungseinrichtung in den Chip gespeichert wird, durch den Chip an die Nutzungseinrichtung ein im Chip abgespeicherter Verschlüsselungsschlüssel gesendet. Die Nutzungseinrichtung verschlüsselt das vorbestimmte individuelle Datum mit dem Verschlüsselungsschlüssel und sendet das verschlüsselte individuelle Datum an den Chip.

Vorzugsweise werden, falls gemäß der Überprüfung in dem Chip bereits mindestens ein vorbestimmtes individuelles Datum abgespeichert ist, das im Chip abgespeicherte individuelle Datum und ein entsprechendes aus der zugreifenden Nutzungseinrichtung bereitgestelltes Datum miteinander verglichen. Nur bei einem positiven Vergleichsergebnis wird der Zugriff der Nutzungseinrichtung auf den Massenspeicher des Datenträgers ermöglicht.

Vorzugsweise sind die Daten in dem Massenspeicher zumindest teilweise verschlüsselt abgespeichert, wobei in dem Chip weiter ein Schlüssel zum Entschlüsseln der verschlüsselten Daten abgespeichert ist. Die Verschlüsselung der Daten bietet einen zusätzlichen Schutz und verhindert, dass der Massenspeicher des Datenträgers ggf. unter Umgehung des Chips genutzt wird.

Vorzugsweise werden weiter, nachdem der Zugriff auf den Massenspeicher gewährt worden ist, weil der Datenträger auf die zugreifende Nutzungseinrichtung personalisiert ist (d.h. nachdem sich die Nutzungseinrichtung gegenüber dem Chip authentisiert hat bzw. nachdem der Chip personalisiert worden ist), die Daten aus dem Massenspeicher mit dem Schlüssel aus dem Chip entschlüsselt.

Gemäß einer bevorzugten Ausführungsform werden die Daten innerhalb des Chips entschlüsselt. Dies hat den Vorteil, dass der Schlüssel den Chip nicht verlassen muss. Alternativ, und falls die Nutzungseinrichtung (Computer, CD-Spieler, DVD-Spieler) ein Sicherheitsmodul wie z.B. ein TPM (Trusted Platform Modul) hat, werden die Daten wahlweise im Sicherheitsmodul (z.B. TPM) entschlüsselt.

Das individuelle Datum wird vorzugsweise geheim gehalten. Auf diese Weise ist sicher gestellt, dass das individuelle Datum nicht abgehört und kopiert werden kann. Beispielsweise ist das individuelle Datum dadurch geheim gehalten, dass es verschlüsselt im Chip abgelegt ist bzw. wird und außerhalb des Chips niemals im Klartext bereitgehalten wird, beispielsweise den Chip nie im Klartext verlässt. Alternativ kann vorgesehen sein, dass das individuelle Datum den Chip gar nicht verlässt.

Die Nutzungseinrichtung weist vorzugsweise einen Mikroprozessor auf, wobei als individuelles Datum ein individueller Parameter des Mikroprozessors verwendet wird, insbesondere die Mikroprozessor-Seriennummer. Der Mikroprozessor kann, je nach Art des Nutzungsgeräts, der Mikroprozessor eines Computers sein oder ein Mikroprozessor eines CD/DVD-Laufwerks eines Computers oder ein Mikroprozessor eines CD/DVD-Abspielgeräts bzw. CD/DVD-Aufnahme-Abspielgeräts mit einem Mikroprozessor.

Gemäß einer bevorzugten Ausführungsform ist das mindestens eine individuelle Datum in der Nutzungseinrichtung in einem Sicherheitsmodul wie z.B. einem Trusted Platform Modul (TPM) abgespeichert. Das Sicherheitsmodul (z.B. Trusted Platform Modul (TPM)) hat einen Mikroprozessor-Chip, in dem Daten verschlüsselt installiert sind. Für einen Computer ist beispielsweise bevorzugt die Seriennummer oder ein anderer individueller Parameter des Computer-Mikroprozessors in einem Sicherheitsmodul (z.B. TPM) verschlüsselt installiert. Weiter kann ein Computer oder andere Nutzungseinrichtung weitere elektronische Komponente aufweisen, wie z.B. einen Mikroprozessor und/oder eine CPU und/oder eine Netzwerkkarte und/oder einen Massenspeicher und/oder ein Sicherheitsmodul. In diesem Fall ist in dem Sicherheitsmodul wahlweise - alternativ oder zusätzlich zur Seriennummer (bzw. sonstigem individuellen Parameter) des Mikroprozes-

sors - ein individueller Parameter (z.B. Seriennummer) einer oder mehrerer der genannten oder weiterer elektronischer Komponenten installiert. Das Sicherheitsmodul (z.B. TPM) ermöglicht es einem Nutzer, die im Sicherheitsmodul (z.B. TPM) verschlüsselt installierten Daten auszulesen und zu Bearbeitungszwecken zur Verfügung zu stellen, beispielsweise um einen Vergleich mit anderen Daten durchzuführen, ohne dass die Daten dem Nutzer im Klartext zur Verfügung gelangen, d.h. wobei die ausgelesenen Daten gegenüber dem Nutzer geheim bleiben.

Die Daten im Massenspeicher können mit einem symmetrischen oder mit einem asymmetrischen Verschlüsselungsverfahren verschlüsselt sein.

Vorzugsweise ist der im Chip abgespeicherte Schlüssel für jeden Datenträger individuell. Zum Verschlüsseln der Daten, bevor sie in den Massenspeicher gespeichert werden, wird vorzugsweise ein universeller Schlüssel verwendet, der für eine Vielzahl von Datenträgern identisch ist.

Wahlweise ist der Chip dazu eingerichtet, dass in dem Chip individuelle Daten mehrerer Nutzungseinrichtungen abgespeichert werden können. In diesem Fall ist der Datenträger auf mehrere Nutzungseinrichtungen personalisiert, von denen jede zur Nutzung der Daten im Massenspeicher des Datenträgers berechtigt ist.

Der Datenträger gemäß der Erfindung weist mindestens einen Massenspeicher und einen Chip auf. Weiter weist der Datenträger vorzugsweise eine Kontaktiereinrichtung zum Kontaktieren des Chips auf, wahlweise eine Kontaktiereinrichtung für kontaktbehaftete Kontaktierung und/oder eine Kontaktiereinrichtung für kontaktlose Kontaktierung. Um eine durch den Chip eventuell entstehende ungünstige Gewichtsverteilung auszugleichen,

kann der Datenträger weiter ein oder mehrere Ausgleichsgewichte aufweisen.

Bei einem Verfahren zum Laden von Daten von einer Datenquelle in den Massenspeicher eines Datenträgers mit einem Massenspeicher und einem Chip wird bei einem Zugriff auf den Datenträger, um Daten in den Massenspeicher zu laden, der Chip daraufhin überprüft wird, ob in dem Chip mindestens ein für eine Nutzungseinrichtung individuelles Datum abgespeichert ist, durch das der Datenträger im Hinblick auf die mindestens eine vorbestimmte Nutzungseinrichtung personalisiert ist. Das Laden von Daten in den Massenspeicher wird nur ermöglicht, falls in dem Chip mindestens ein vorbestimmtes individuelles Datum einer Nutzungseinrichtung abgespeichert ist. Nachfolgend ist ein Zugriff auf die Daten im Massenspeicher nur mit der mindestens einen Nutzungseinrichtung, auf die der Datenträger personalisiert ist, möglich.

Die Daten werden wahlweise unter Zwischenschaltung eines kontaktbehafteten Computernetzwerks von der Datenquelle an den Datenträger übermittelt, um in den Massenspeicher des Datenträgers geladen zu werden. Das Computernetzwerk kann beispielsweise ein Internet-Netzwerk, Intranet-Netzwerk oder dergleichen sein. Wahlweise werden die Daten per E-Mail an den Datenträger übermittelt.

Wahlweise werden Daten unter Zwischenschaltung eines kontaktlosen Netzwerks von der Datenquelle an den Datenträger übermittelt, um in den Massenspeicher des Datenträgers geladen zu werden. Das kontaktlose Netzwerk kann beispielsweise ein Mobilfunknetzwerk sein, wie z.B. ein GSM oder UMTS Netzwerk, oder ein WLAN-Netzwerk (WLAN = Wireless Local Area Network). In einem Mobilfunknetzwerk werden die Daten

wahlweise per SMS übertragen oder mit einem Dienst zur direkten Datenübertragung.

Die Daten können wahlweise von der Datenquelle direkt an den Datenträger übermittelt werden. Alternativ werden die Daten zuerst von der Datenquelle an ein Endgerät wie z.B. einen Computer, Notebook, Mobiltelefon, PDA (Personal Digital Assistant) oder dergleichen übermittelt und von dem Endgerät in den Massenspeicher des Datenträgers geladen.

Beispielsweise ist der Datenträger eine CD oder DVD mit Chip. Im Chip ist eine Seriennummer oder dergleichen angespeichert. Die Daten werden zuerst von der Datenquelle in einen Computer etc. geladen und anschließend auf CD oder DVD gebrannt.

Das Laden der Daten wird vorzugsweise wie folgt vorgenommen:

- das im Chip abgespeicherte individuelle Datum vom Chip wird in den Verfügungsbereich der Datenquelle übermittelt,
- unter der Verfügung der Datenquelle wird das übermittelte individuelle Datum ausgewertet und
- die Daten werden an den Datenträger übermittelt, um sie in den Massenspeicher zu laden.

Dabei können natürlich die Daten wieder über die Vermittlung eines Endgeräts an den Datenträger übermittelt werden.

Vorzugsweise werden die Daten verschlüsselt in den Massenspeicher geladen. Gemäß einer bevorzugten Ausführungsform werden die Daten mit einem Schlüssel verschlüsselt, der aus dem individuellen Datum im Chip des Datenträgers ermittelt ist.

Im folgenden wird die Erfindung an Hand von Ausführungsbeispielen und unter Bezugnahme auf die Zeichnung näher erläutert, in der zeigen:

Fig. 1 eine beispielhafte erfindungsgemäße CD/DVD, die einen optischen Speicher, einen Chip, ein Kontaktfeld zum Kontaktieren des Chips und zwei Ausgleichsgewichte aufweist;

Fig. 2 ein Beispiel für ein zur Anbringung auf einer CD/DVD vorgesehenes Kontaktfeld zur kontaktbehafteten Kontaktierung eines auf der CD/DVD angeordneten Chips;

Fig. 3 ein weiteres Beispiel für ein zur Anbringung auf einer CD/DVD vorgesehenes Kontaktfeld zur kontaktbehafteten Kontaktierung eines auf der CD/DVD angeordneten Chips;

Fig. 4 eine erfindungsgemäße CD/DVD mit einem optischen Speicher, einem Chip und einem Ausgleichsgewicht, sowie eine für die erfindungsgemäße CD/DVD eingerichtete Leseeinrichtung mit einer Einrichtung zum Zugreifen auf den Chip;

Fig. 5 ein Flussdiagramm zur Veranschaulichung eines Verfahrens zum Zugreifen auf den Massenspeicher eines Datenträgers, gemäß einer bevorzugten Ausführungsform der Erfindung;

Fig. 6 ein Flussdiagramm zur Veranschaulichung eines Verfahrens zum Zugreifen auf den Massenspeicher eines Datenträgers, gemäß einer weiteren bevorzugten Ausführungsform der Erfindung;

Fig. 7 ein Flussdiagramm zur Veranschaulichung einer Variante des Verfahrens aus Fig. 6, bei der eine Personalisierung des Datenträgers auf mehrere Nutzungseinrichtungen möglich sein kann.

Fig. 1 zeigt eine beispielhafte erfindungsgemäße CD/DVD 100. Die CD/DVD 100 hat, wie eine herkömmliche CD/DVD, ein Mittelloch 101, rund um das ein ringförmiger, von optischem Speicher freier Bereich 102 angeordnet ist, rund um den ein weiterer ringförmiger Datenbereich 103 angeordnet ist. Im Datenbereich 103 ist ein optischer Speicher (Massenspeicher) vorgesehen. Im Unterschied zu einer herkömmlichen CD/DVD 100 sind bei der erfindungsgemäßen CD/DVD 100 aus Fig. 1 im freien Bereich 102 zwischen dem optischen Speicher 103 und dem Mittelloch 101 ein Chip 104, ein Kontaktfeld 105 zum Kontaktieren des Chips 104 und zwei Ausgleichsgewichte 106 angeordnet. Der Chip 104 und die Ausgleichsgewichte 106 sind so angeordnet, dass die CD/DVD 100 möglichst keine Unwucht hat, und dass der Schwerpunkt möglichst im Mittelpunkt der kreisförmigen CD/DVD 100 liegt. Wahlweise sind keine oder eine andere geeignete Anzahl und Anordnungsweise von Ausgleichsgewichten vorgesehen.

Fig. 2 zeigt ein Beispiel für ein zur Anbringung auf einer CD/DVD wie der in Fig. 1 gezeigten vorgesehenes Kontaktfeld 205 zur kontaktbehafteten Kontaktierung eines ebenfalls auf der CD/DVD angeordneten Chips. Das Kontaktfeld ist ringförmig gestaltet, so dass es auf einer CD/DVD 100 wie der in Fig. 1 gezeigten im freien Bereich 102 zwischen dem Mittelloch 101 und dem Datenbereich 103 angeordnet werden kann. Das Kontaktfeld 205 hat acht (allgemein typischerweise zwei bis zehn) einzelne Kontaktflächen in Gestalt von Ringsegmenten, die entlang einer Kreisbahn angeordnet sind.

Fig. 3 zeigt ein weiteres Beispiel für ein zur Anbringung auf einer CD/DVD vorgesehenes Kontaktfeld 305. Das Kontaktfeld 305 ist, ähnlich wie das Kontaktfeld 205 aus Fig. 2, ringförmig gestaltet, hat aber sechs konzentrisch zueinander angeordnete, ringförmige Kontaktflächen.

Bei einer erfindungsgemäßen CD/DVD ist beispielsweise im freien Bereich 102 zwischen dem Mittelloch 101 und dem Datenbereich 103 ein Kontaktfeld 205, 305 gemäß Fig. 2 oder Fig. 3, damit ein auf der CD/DVD 100 angeordneter Chip 104 kontaktiert werden kann. Die einzelnen Kontaktflächen (z.B. sechs bzw. acht Stücke) können z.B. gemäß ISO/IEC 7816 oder einem anderen Protokoll (USB, RS232/V.24, etc.) ansteuerbar sein. Das Kontaktfeld gemäß Fig. 3 mit den ringförmigen Kontaktflächen hat dabei den Vorteil, dass es auch dann kontaktiert werden kann, wenn die CD/DVD in Rotationsbewegung ist, z.B. weil gerade auf den ringförmigen optischen Speicher zugegriffen wird oder werden soll.

Fig. 4 zeigt eine erfindungsgemäße CD/DVD 100 mit einem optischen Speicher 103, einem Chip 104 und einem Ausgleichsgewicht, sowie eine für die erfindungsgemäße CD/DVD 100 eingerichtete Leseeinrichtung 410 mit einer Einrichtung zum Zugreifen auf den Chip.

Fig. 5 zeigt ein Flussdiagramm zur Veranschaulichung der Grundzüge eines Verfahrens zum Zugreifen auf den Massenspeicher eines Datenträgers, gemäß einer bevorzugten Ausführungsform der Erfindung. Der Datenträger hat einen Massenspeicher mit Daten und einen Chip. Mit einer Nutzungseinrichtung wird versucht, auf die Daten im Massenspeicher zuzugreifen.

In Schritt 1 wird geprüft, ob der Chip des Datenträgers ein vorbestimmtes individuelles Datum enthält. Falls der Chip das vorbestimmte individuelle

Datum nicht enthält oder keinerlei individuelles Datum enthält, wird in Schritt 2 das individuelle Datum aus einem Sicherheitsmodul der Nutzungseinrichtung, das hier als Trusted Platform Modul TPM gestaltet ist, in den Chip geladen und im Chip abgespeichert, wodurch der Datenträger auf die Nutzungseinrichtung personalisiert wird. Nachfolgend wird der Zugriff auf die Daten im Massenspeicher gewährt. Falls hingegen in dem Chip bereits ein vorbestimmtes individuelles Datum abgespeichert ist, wird in Schritt 3a das individuelle Datum in den Chip geladen und in Schritt 3b das geladene individuelle Datum mit dem bereits abgespeicherten individuellen Datum verglichen. Falls das geladene individuelle Datum und das bereits abgespeicherte individuelle Datum unterschiedlich sind, wird der Zugriff auf die Daten im Massenspeicher verweigert. Falls dagegen das geladene individuelle Datum und das bereits abgespeicherte individuelle Datum gleich sind, wird der Zugriff auf die Daten im Massenspeicher gewährt. Falls in dem Chip individuelle Daten mehrerer Nutzungseinrichtungen abgespeichert sind und der Datenträger also auf mehrere Nutzungseinrichtungen personalisiert ist, wird geprüft, ob unter den individuellen Daten ein individuelles Datum der gerade zugreifenden Nutzungseinrichtung ist und ansonsten analog verfahren wie bei einem Datenträger, der auf nur eine einzige Nutzungseinrichtung personalisiert ist.

Fig. 6 zeigt ein ähnliches Flussdiagramm wie das in Fig. 5 gezeigte. Im Vergleich zum Verfahren gemäß Fig. 5 wird bei dem Verfahren gemäß Fig. 6 zunächst in jedem Fall in Schritt 1a ein vorbestimmtes individuelles Datum aus dem Sicherheitsmodul (hier ebenfalls beispielhaft als Trusted Platform Modul TPM gestaltet) der Nutzungseinrichtung in den Chip geladen. Danach wird in Schritt 1b überprüft, ob der Chip des Datenträgers ein vorbestimmtes individuelles Datum enthält. Falls der Chip das vorbestimmte individuelle Datum nicht enthält wird in Schritt 2 das individuelle Datum aus

dem TPM der Nutzungseinrichtung im Chip abgespeichert, wodurch der Datenträger auf die Nutzungseinrichtung personalisiert wird. Nachfolgend wird der Zugriff auf die Daten im Massenspeicher gewährt. Falls hingegen in dem Chip bereits ein vorbestimmtes individuelles Datum abgespeichert ist, wird in Schritt 3 das nun bereits geladene individuelle Datum mit dem vorab abgespeicherten individuellen Datum verglichen. Der weitere Verfahrensverlauf ist der gleiche wie beim Verfahren von Fig. 5.

In Fig. 7 ist eine Variante des Verfahrens aus Fig. 6 gezeigt, bei der ein Datenträger auf mehrere Nutzungseinrichtungen personalisiert sein kann. Bei der Variante aus Fig. 7 wird im Anschluss an Schritt 3, falls in dem Chip bereits ein individuelles Datum vorgefunden wird, dieses aber nicht einem in Schritt 1a geladenen individuellen Datum der gerade zugreifenden Nutzungseinrichtung entspricht bzw. nicht zu der zugreifenden Nutzungseinrichtung gehört, in einem Schritt 3-1 geprüft, ob eine Personalisierung des Datenträgers auf eine weitere Nutzungseinrichtung zulässig ist. Falls nein, wird, wie gemäß Fig. 6 gehabt, der Zugriff auf Daten im Massenspeicher verweigert (Schritt 4). Falls hingegen eine Personalisierung des Datenträgers auf eine weitere Nutzungseinrichtung zulässig ist ("Ja"), wird das in Schritt 1a geladene Datum in einem Schritt 6 im Chip des Datenträgers abgespeichert, um den Datenträger auf eine weitere Nutzungseinrichtung zu personalisieren. Schließlich wird in Schritt 7 der Zugriff auf die Daten im Massenspeicher des Datenträgers gewährt.

Im Folgenden werden im Detail Verfahren zum Zugreifen auf eine erfindungsgemäße CD mit Chip gemäß bevorzugten Ausführungsformen der Erfindung im Einzelnen dargelegt. Die CD hat einen optischen Speicher mit einem verschlüsselten Bereich, in dem Daten verschlüsselt abgelegt sind, und einem unverschlüsselten Bereich zum Booten. Der verschlüsselte bzw.

unverschlüsselte Bereich kann jeweils zusammenhängend sein oder alternativ mehrere unzusammenhängende Teilbereiche haben. Im Chip ist ein Schlüssel zum Entschlüsseln der Daten abgespeichert. Auf die CD wird mit einem CD-Laufwerk eines Computers zugegriffen. Der Computer enthält ein Sicherheitsmodul, hier beispielhaft als Trusted Platform Modul TPM gestaltet, in dem die Mikroprozessornummer des Mikroprozessors des Computers sicher abgespeichert ist. Als individuelles Datum wird bei den beispielhaft beschriebenen Verfahren die Mikroprozessornummer des Computers aus dem TPM des Computers verwendet. Alternativ oder zusätzlich kann die Seriennummer einer anderen Computerkomponente (Netzwerkkarte, Massenspeicher etc.) verwendet werden bzw. ein anderes individuelles Datum als die Seriennummer des Mikroprozessors bzw. der Computerkomponente.

Für andere Arten von Datenträgern (DVD, SC, CF, MMC), für andere Arten von Abspielgeräten für Datenträger, insbesondere für andere CD/DVD-Laufwerke wie z.B. CD/DVD-Laufwerke in CD/DVD-Abspielgeräten funktioniert das Verfahren analog.

Die CD wird in das CD-Laufwerk des Computers (bzw. Abspielgeräts etc.) eingelegt. Aus dem unverschlüsselten Bereich des optischen Massenspeichers der CD wird ein Installations-Programm (Start- bzw. Boot-Programm) hochgefahren, durch das eine erste Kommunikation mit der CD ermöglicht wird. Das Installations-Programm erkennt, dass eine Nutzungseinrichtung über ein CD-Laufwerk versucht, auf die CD zuzugreifen und verlangt vom Nutzer, die Authentisierung der zugreifenden Nutzungseinrichtung durchzuführen. Hierzu muss auf den Chip der CD zugegriffen werden.

Gemäß einer ersten Alternative enthält das CD-Laufwerk einen Chipleser (genauer Chip-Lese-Schreibgerät). In diesem Fall beginnt als nächstes der Chipleser die Kommunikation mit dem Chip der CD.

Gemäß einer zweiten Alternative hat das CD-Laufwerk keinen Chipleser. In diesem Fall wird der Nutzer aufgefordert, die CD aus dem CD-Laufwerk zu nehmen. Nachfolgend kontaktiert der Nutzer den Chip mit einem kontaktbehafteten oder kontaktlosen Chipleser. Gemäß einer bevorzugten Variante wird ein kontaktloser Chipleser verwendet, der in den Computer integriert ist. Weiter vorzugsweise ist der integrierte Chipleser über eine NFC-Schnittstelle kontaktierbar, die "automatisch" mit dem Chip in Kommunikation tritt, sobald die CD nahe genug angenähert worden ist.

Der Chipleser (intern oder extern) tritt in Kontakt mit dem TPM des Computers und sendet an das TPM eine Aufforderung, die Mikroprozessornummer an den Chip zu senden, sowie einen Transportschlüssel, mit dem das TPM die Mikroprozessornummer verschlüsseln soll. Der Transportschlüssel ist vorzugsweise ein öffentlicher Schlüssel eines PKI-Schlüsselpaares. Das TPM verschlüsselt im TPM die Mikroprozessornummer mit dem Transportschlüssel und sendet die verschlüsselte Mikroprozessornummer an den Chip der CD. Der Chip empfängt die verschlüsselte Mikroprozessornummer, entschlüsselt sie mit dem geheimen Schlüssel zu dem PKI-Schlüsselpaar und speichert sie im Chip ab.

Als nächstes überprüft der Chipleser, ob in dem Chip eine Mikroprozessornummer eines Computers abgespeichert ist. Wahlweise erfolgt die Überprüfung, ob in dem Chip eine Mikroprozessornummer eines Computers abgespeichert ist, bereits vor dem Anfordern der Mikroprozessornummer beim TPM.

Falls im Chip noch keine Mikroprozessornummer abgespeichert ist, wird die geladene Mikroprozessornummer in einen dafür vorgesehenen Speicher des Chips abgelegt (bzw. wird, falls noch keine Mikroprozessornummer geladen worden ist, die Mikroprozessornummer vom TPM des Computers angefordert, wie oben beschrieben, und dann in dem Speicher abgelegt). Hierdurch ist die CD auf den Computer personalisiert worden.

Die CD ist nun bereit zum Entschlüsseln der Daten im optischen Speicher. Das entsprechende Verfahren wird später noch beschrieben.

Falls im Chip bereits eine Mikroprozessornummer abgespeichert ist, vergleicht der Chip die vom TPM gelieferte Mikroprozessornummer mit der Mikroprozessornummer, die bereits zur Personalisierung der CD im Chip abgespeichert ist.

Falls die gelieferte und die bereits abgespeicherte Mikroprozessornummer nicht übereinstimmen, wird der Zugriff auf die Daten im optischen Speicher der CD verwehrt.

Falls die gelieferte und die bereits abgespeicherte Mikroprozessornummer übereinstimmen, ist die CD bereit zum Entschlüsseln der Daten im optischen Speicher.

Zum Entschlüsseln der Daten im optischen Speicher der CD wird die Kommunikation wieder an das CD-Laufwerk übergeben. Bedarfsweise muss dazu die CD, die zuvor aus dem CD-Laufwerk entnommen worden ist, wieder in das CD-Laufwerk eingelegt werden. Das CD-Laufwerk liest die verschlüsselten bzw. teilweise verschlüsselten Daten aus dem optischen Speicher der

CD in einen für das CD-Laufwerk und den Chipleser gleichermaßen zugänglichen Zwischenspeicher.

Nachfolgend wechselt die Kommunikation wieder auf den Chip, wobei bedarfsweise die CD wieder aus dem CD-Laufwerk entnommen und mit dem Chipleser gekoppelt werden muss. Der Chipleser überträgt die zuvor in den Zwischenspeicher übertragenen Daten in den Chip.

Im Chip werden die Daten entschlüsselt. Alternativ werden die Daten im Zwischenspeicher des CD-Laufwerks entschlüsselt, wozu der im Chip abgespeicherte Entschlüsselungsschlüssel an das CD-Laufwerk übertragen wird, wobei der Entschlüsselungsschlüssel vorzugsweise nie im Klartext den Chip verlässt, also selbst wieder verschlüsselt ist.

Die entschlüsselten Daten werden in einen dafür vorgesehenen Speicher des Computers installiert und können nachfolgend bestimmungsgemäß verwendet werden.

In der Nutzungseinrichtung ist das individuelle Datum, mit dem der Datenträger personalisiert worden ist oder noch werden soll, wahlweise in einem Sicherheitsmodul (z.B. TPM) vorgesehen. Das Sicherheitsmodul kann beispielsweise in einem Computer, einem Schreib-/Leselaufwerk eines Computers, einem Abspielgerät für den Datenträger oder einer der Komponenten eines solchen Abspielgeräts vorgesehen sein. Ein - kontaktloses (insbesondere NFC, alternativ anderes Protokoll) oder kontaktbehaftetes - Lesegerät für den Chip des Datenträgers kann ebenfalls in einem Computer, einem Schreib-/Leselaufwerk eines Computers, einem Abspielgerät für den Datenträger oder einer der Komponenten eines solchen Abspielgeräts vorgesehen sein. Das Lesegerät für den Chip des Datenträgers und das Sicherheitsmodul

(z.B. TPM) der Nutzungseinrichtung können wahlweise getrennt oder in Kombination miteinander untergebracht sein, wahlweise in demselben Teil der Nutzungseinrichtung oder in unterschiedlichen Teilen der Nutzungseinrichtung.

Die Daten können beispielsweise Programmdaten eine Programms sein, das nun im Computer installiert werden kann.

Gemäß einer alternativen Ausführungsform der Erfindung ist der Datenträger eine Musik-CD mit einem optischen Speicher, in dem Musikdaten abgespeichert sind, die derart teilweise verschlüsselt sind, dass die Musik, die den Daten entspricht, zwar analog (akustisch) ausgegeben werden kann, dies aber nur in schlechter, verrauschter Tonqualität. In unverrauschter Form können die Daten analog nur ausgegeben werden, nachdem sie entschlüsselt worden sind.

Gemäß einer weiteren alternativen Ausführungsform der Erfindung ist der Datenträger eine Film-DVD mit einem optischen Speicher, in dem Filmdaten abgespeichert sind. Ansonsten entspricht die DVD der weiter oben beschriebenen Musik-CD. Alternativ ist als Datenträger eine Musik/Film-DVD vorgesehen.

Gemäß einer Weiterbildung der Erfindung, die in einer anderen, am selben Tag eingereichten Patentanmeldung beschrieben ist, weist der Datenträger zusätzlich ein Zustandskennzeichen auf, durch das der Umfang der Nutzung des Datenträgers begrenzt ist, z.B. die Anzahl von Malen der Nutzung oder/ und die Nutzungsdauer. Beispielsweise kann als Zustandskennzeichen ein Flag oder Zähler vorgesehen sein, der gesetzt bzw. hochgezählt (alternativ heruntergezählt) wird, wenn Daten aus dem Massenspeicher ge-

nutzt werden, z.B. abgespielt oder installiert werden. Wahlweise wird, wenn die Daten wieder deinstalliert werden, das Flag wieder gelöscht bzw. der Zähler wieder heruntergezählt (alternativ hochgezählt).

Patentansprüche

1. Verfahren zum Zugreifen auf den Massenspeicher eines Datenträgers mit einem Massenspeicher und einem Chip, wobei für den Zugriff auf den Massenspeicher mittels einer Nutzungseinrichtung eine Authentisierung der Nutzungseinrichtung gegenüber dem Chip zwingend erforderlich ist,
dadurch gekennzeichnet, dass
bei einem Zugriff einer Nutzungseinrichtung auf den Datenträger, um auf den Massenspeicher zuzugreifen, der Chip daraufhin überprüft wird, ob in dem Chip ein für die Nutzungseinrichtung individuelles Datum abgespeichert ist, durch das der Datenträger im Hinblick auf die Nutzungseinrichtung personalisiert ist, und der Zugriff auf den Massenspeicher höchstens ermöglicht wird, falls in dem Chip mindestens ein vorbestimmtes individuelles Datum der zugreifenden Nutzungseinrichtung abgespeichert ist.

2. Verfahren nach Anspruch 1, wobei, falls gemäß der Überprüfung kein individuelles Datum im Chip abgespeichert ist, mindestens ein vorbestimmtes individuelles Datum der Nutzungseinrichtung in den Chip gespeichert wird.

3. Verfahren nach Anspruch 2, wobei, bevor das vorbestimmte individuelle Datum der Nutzungseinrichtung in den Chip gespeichert wird,
der Chip an die Nutzungseinrichtung einen im Chip abgespeicherten Verschlüsselungsschlüssel sendet und
die Nutzungseinrichtung das vorbestimmte individuelle Datum mit dem Verschlüsselungsschlüssel verschlüsselt und das verschlüsselte individuelle Datum an den Chip sendet.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei, falls gemäß der Überprüfung in dem Chip bereits mindestens ein vorbestimmtes individuelles Datum abgespeichert ist:
die Bereitstellung des individuellen Datums der zugreifenden Nutzungseinrichtung aus der Nutzungseinrichtung angefordert wird,
das im Chip abgespeicherte individuelle Datum und das aus der zugreifenden Nutzungseinrichtung bereitgestellte Datum miteinander verglichen werden und
höchstens bei einem positiven Vergleichsergebnis der Zugriff der Nutzungseinrichtung auf den Massenspeicher des Datenträgers ermöglicht wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, wobei die Daten in dem Massenspeicher zumindest teilweise verschlüsselt abgespeichert sind, und wobei in dem Chip weiter ein Schlüssel zum Entschlüsseln der verschlüsselten Daten abgespeichert ist.

6. Verfahren nach Anspruch 5, wobei die Daten aus dem Massenspeicher mit dem Schlüssel aus dem Chip entschlüsselt werden.

7. Verfahren nach Anspruch 6, wobei die Daten innerhalb des Chips entschlüsselt werden.

8. Verfahren nach Anspruch 6, wobei die Daten in einem Sicherheitsmodul, insbesondere Trusted Platform Modul (TPM), der Nutzungseinrichtung entschlüsselt werden.

9. Verfahren nach einem der Ansprüche 1 bis 8, wobei das individuelle Datum geheim gehalten wird.

10. Verfahren nach einem der Ansprüche 1 bis 9, wobei die Nutzungseinrichtung mindestens eine elektronische Komponente aufweist und wobei als individuelles Datum ein individueller Parameter der elektronischen Komponente verwendet wird, insbesondere die Seriennummer der Komponente.

11. Verfahren nach Anspruch 10, wobei als elektronische Komponente vorgesehen ist: ein Mikroprozessor und/oder eine CPU und/oder eine Netzwerkkarte und/oder ein Massenspeicher und/oder ein Sicherheitsmodul.

12. Verfahren nach einem der Ansprüche 1 bis 11, wobei das mindestens eine individuelle Datum in der Nutzungseinrichtung in einem Sicherheitsmodul, insbesondere Trusted Platform Modul (TPM), abgespeichert ist.

13. Verfahren nach einem der Ansprüche 1 bis 12, wobei die Nutzungseinrichtung eine Datenverarbeitungseinrichtung, wie ein Computer, mit zumindest einer Leseeinheit für den Massenspeicher ist.

14. Verfahren nach einem der Ansprüche 1 bis 12, wobei die Nutzungseinrichtung eine Ausgabeeinrichtung, wie eine Ausgabeeinrichtung zur analogen Ausgabe von Multimediadaten wie z.B. Musikdaten und/oder Filmdaten, ist.

15. Verfahren nach einem der Ansprüche 1 bis 14, wobei als Massenspeicher ein optischer Speicher vorgesehen ist.

16. Datenträger mit einem Massenspeicher und einem Chip, wobei für den Zugriff auf den Massenspeicher mittels einer Nutzungseinrichtung eine Authentisierung der Nutzungseinrichtung gegenüber dem Chip zwingend erforderlich ist,

dadurch gekennzeichnet, dass
in dem Datenträger ein Verfahren nach einem der Ansprüche 1 bis 15 implementiert ist und dass der Datenträger dazu eingerichtet ist, dass bei einem Zugriff einer Nutzungseinrichtung auf den Datenträger, um auf den Massenspeicher zuzugreifen, der Chip daraufhin überprüft wird, ob in dem Chip ein für die Nutzungseinrichtung individuelles Datum abgespeichert ist, durch das der Datenträger im Hinblick auf die Nutzungseinrichtung personalisiert ist, und der Zugriff auf den Datenträger höchstens ermöglicht wird, falls in dem Chip mindestens ein vorbestimmtes individuelles Datum der zugreifenden Nutzungseinrichtung abgespeichert ist.

17. Datenträger nach Anspruch 16, der als CD oder DVD gestaltet ist, wobei als Massenspeicher ein optischer Speicher vorgesehen ist.

18. Verfahren zum Laden von Daten von einer Datenquelle in den Massenspeicher eines Datenträgers mit einem Massenspeicher und einem Chip, wobei für den Zugriff auf den Massenspeicher mittels einer Nutzungseinrichtung eine Authentisierung der Nutzungseinrichtung gegenüber dem Chip zwingend erforderlich ist,
dadurch gekennzeichnet, dass
bei einem Zugriff auf den Datenträger, um Daten in den Massenspeicher zu laden, der Chip daraufhin überprüft wird, ob in dem Chip mindestens ein für eine Nutzungseinrichtung individuelles Datum abgespeichert ist, durch das der Datenträger im Hinblick auf die mindestens eine vorbestimmte Nutzungseinrichtung personalisiert ist, und das Laden von Daten in den Massenspeicher höchstens ermöglicht wird, falls in dem Chip mindestens ein vorbestimmtes individuelles Datum einer Nutzungseinrichtung abgespeichert ist, wobei nachfolgend ein Zugriff auf die Daten im Massenspeicher

höchstens mit der mindestens einen Nutzungseinrichtung, auf die der Datenträger personalisiert ist, möglich ist.

19. Verfahren nach Anspruch 18, wobei die Daten unter Zwischenschaltung eines kontaktbehafteten Computernetzwerks von der Datenquelle an den Datenträger übermittelt werden, um in den Massenspeicher des Datenträgers geladen zu werden.

20. Verfahren nach Anspruch 18 oder 19, wobei die Daten unter Zwischenschaltung eines kontaktlosen Netzwerks von der Datenquelle an den Datenträger übermittelt werden, um in den Massenspeicher des Datenträgers geladen zu werden.

21. Verfahren nach einem der Ansprüche 18 bis 20, wobei zum Laden der Daten

- das im Chip abgespeicherte individuelle Datum vom Chip in den Verfügungsbereich der Datenquelle übermittelt wird
- unter der Verfügung der Datenquelle das übermittelte individuelle Datum ausgewertet wird und
- die Daten an den Datenträger übermittelt werden, um sie in den Massenspeicher zu laden.

22. Verfahren nach einem der Ansprüche 18 bis 21, wobei die Daten verschlüsselt in den Massenspeicher geladen werden.

23. Verfahren nach Anspruch 22, wobei die Daten mit einem Schlüssel verschlüsselt werden, der aus dem individuellen Datum im Chip des Datenträgers ermittelt ist.

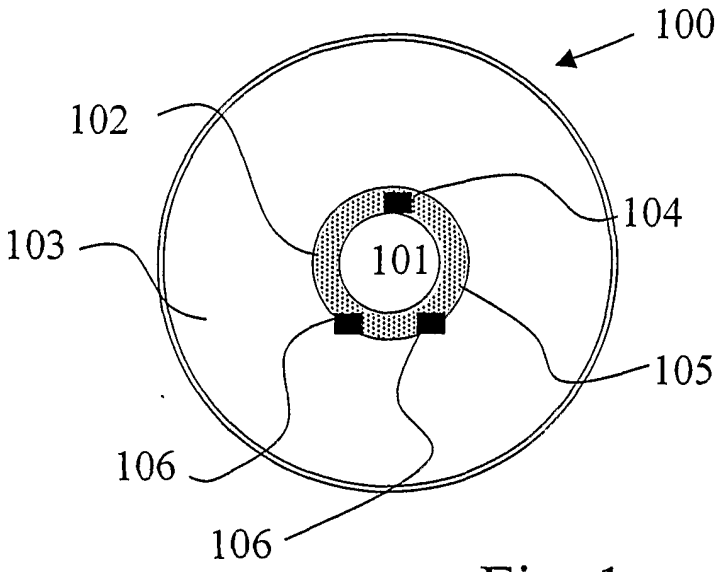


Fig. 1

Fig. 2

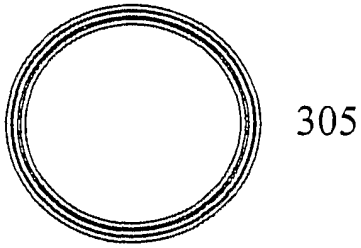


Fig. 3

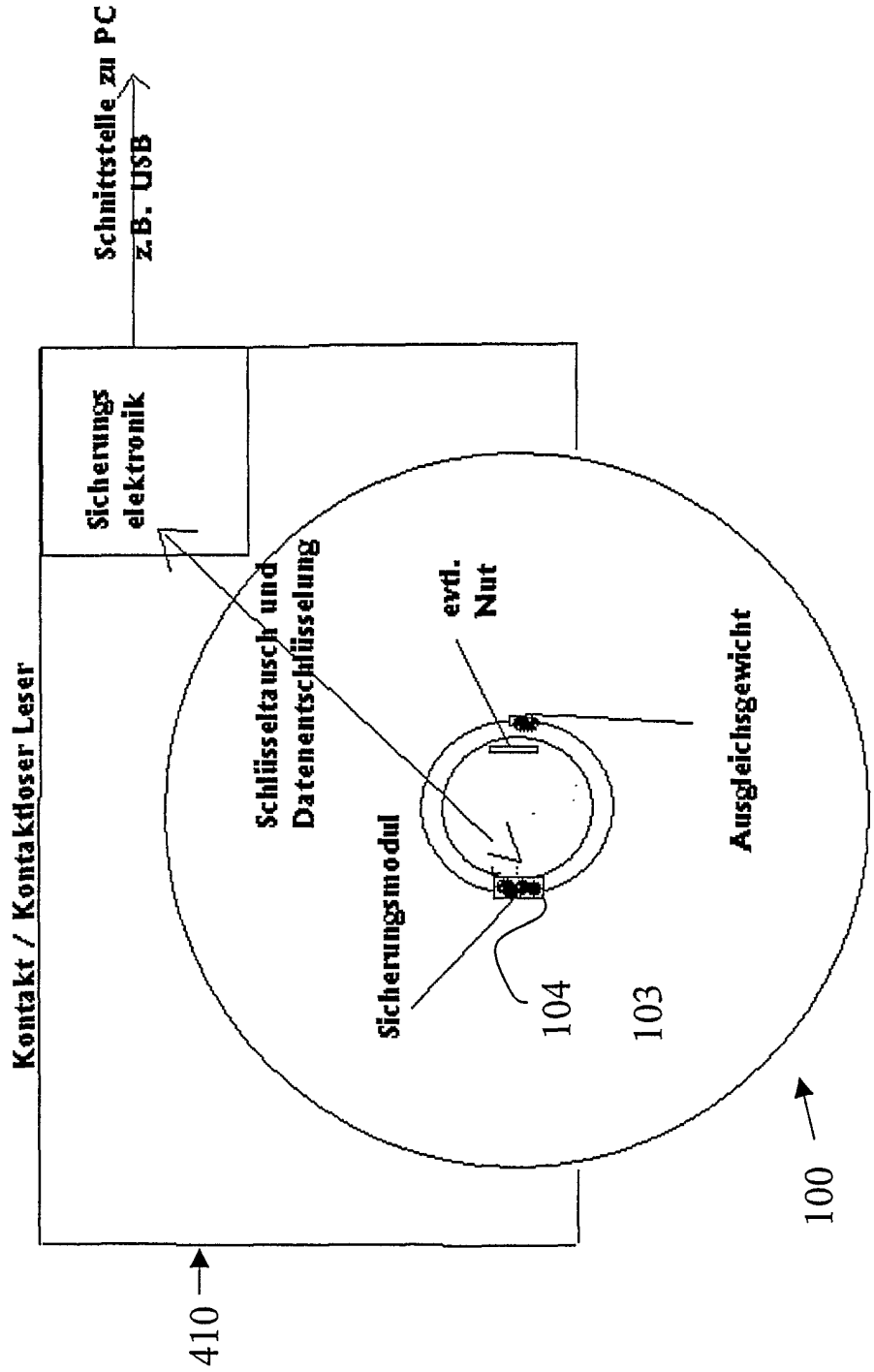

Schnittstelle zu PC
z.B. USB
Sicherungs elektronik
Kontakt / Kontaktloser Leser
Schlüsseltausch und Datenentschlüsselung
evtl. Nut
Sicherungsmodul
Ausgleichsgewicht
104
103
100
410

Fig. 4

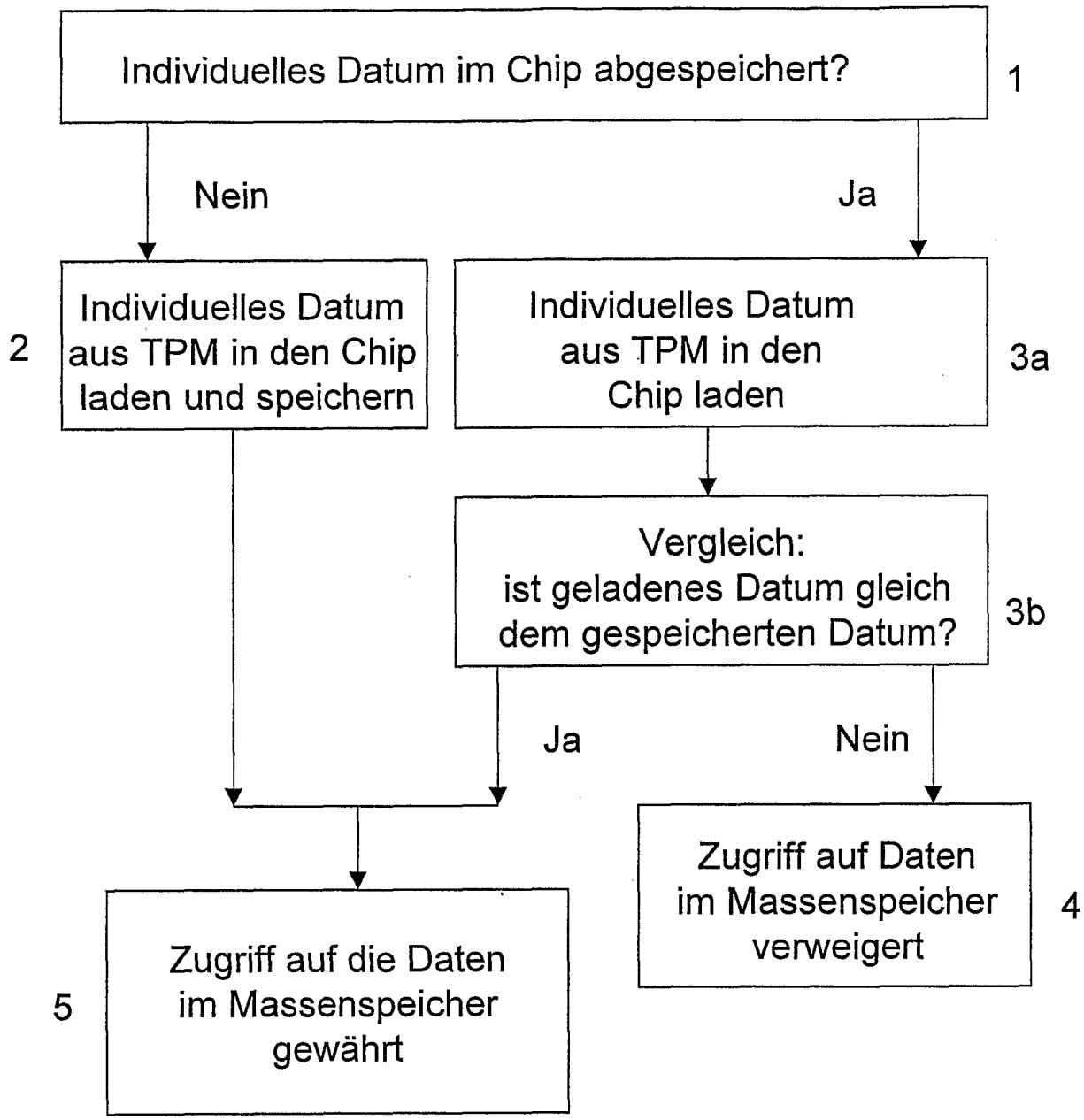

Individuelles Datum im Chip abgespeichert?
1
Nein
Ja
2
Individuelles Datum aus TPM in den Chip laden und speichern
Individuelles Datum aus TPM in den Chip laden
3a
Vergleich: ist geladenes Datum gleich dem gespeicherten Datum?
3b
Ja
Nein
Zugriff auf Daten im Massenspeicher verweigert
4
5
Zugriff auf die Daten im Massenspeicher gewährt

Fig. 5

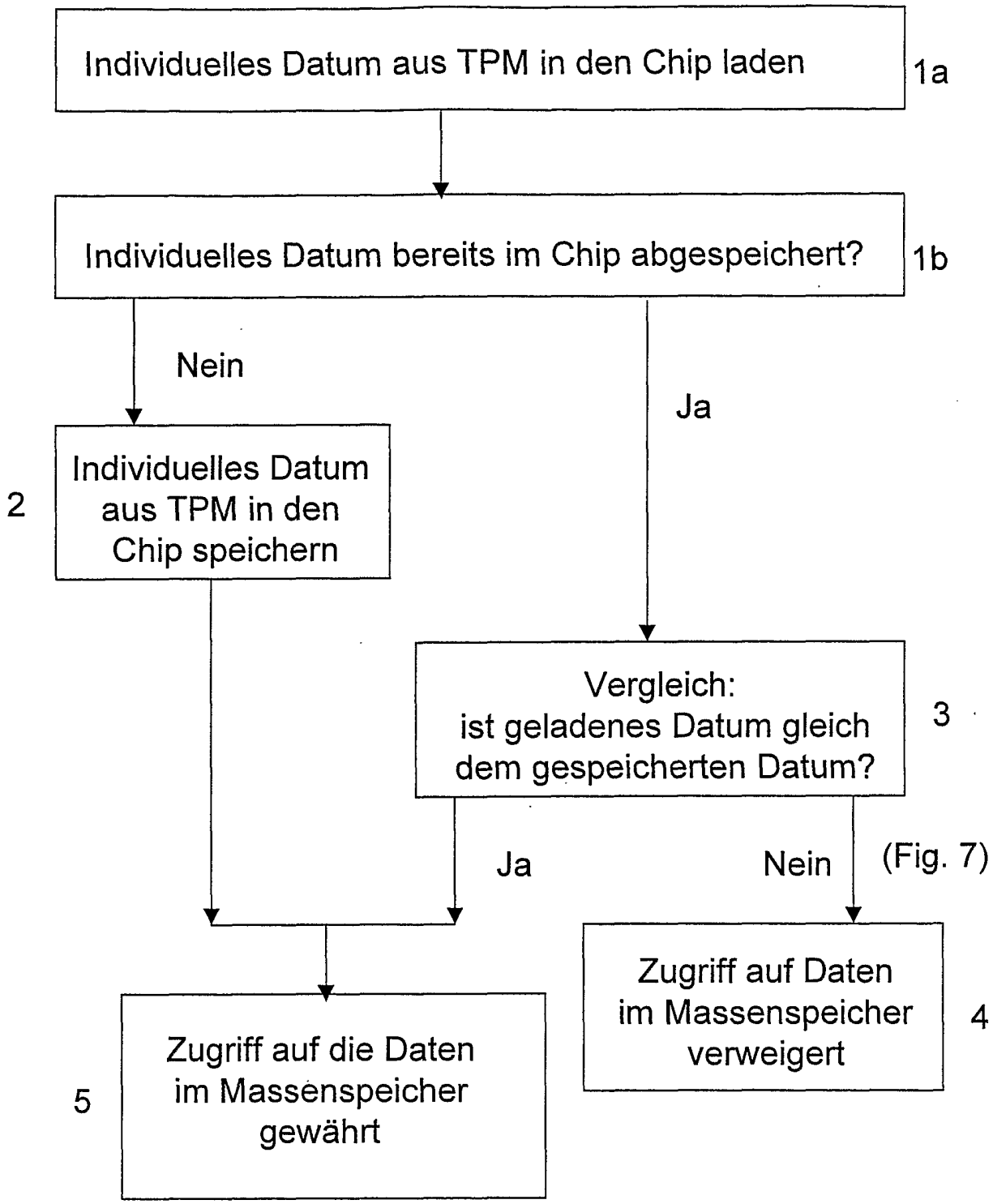

Individuelles Datum aus TPM in den Chip laden
1a
Individuelles Datum bereits im Chip abgespeichert?
1b
Nein
Ja
2
Individuelles Datum aus TPM in den Chip speichern
Vergleich: ist geladenes Datum gleich dem gespeicherten Datum?
3
Ja
Nein
(Fig. 7)
Zugriff auf Daten im Massenspeicher verweigert
4
5
Zugriff auf die Daten im Massenspeicher gewährt

Fig. 6

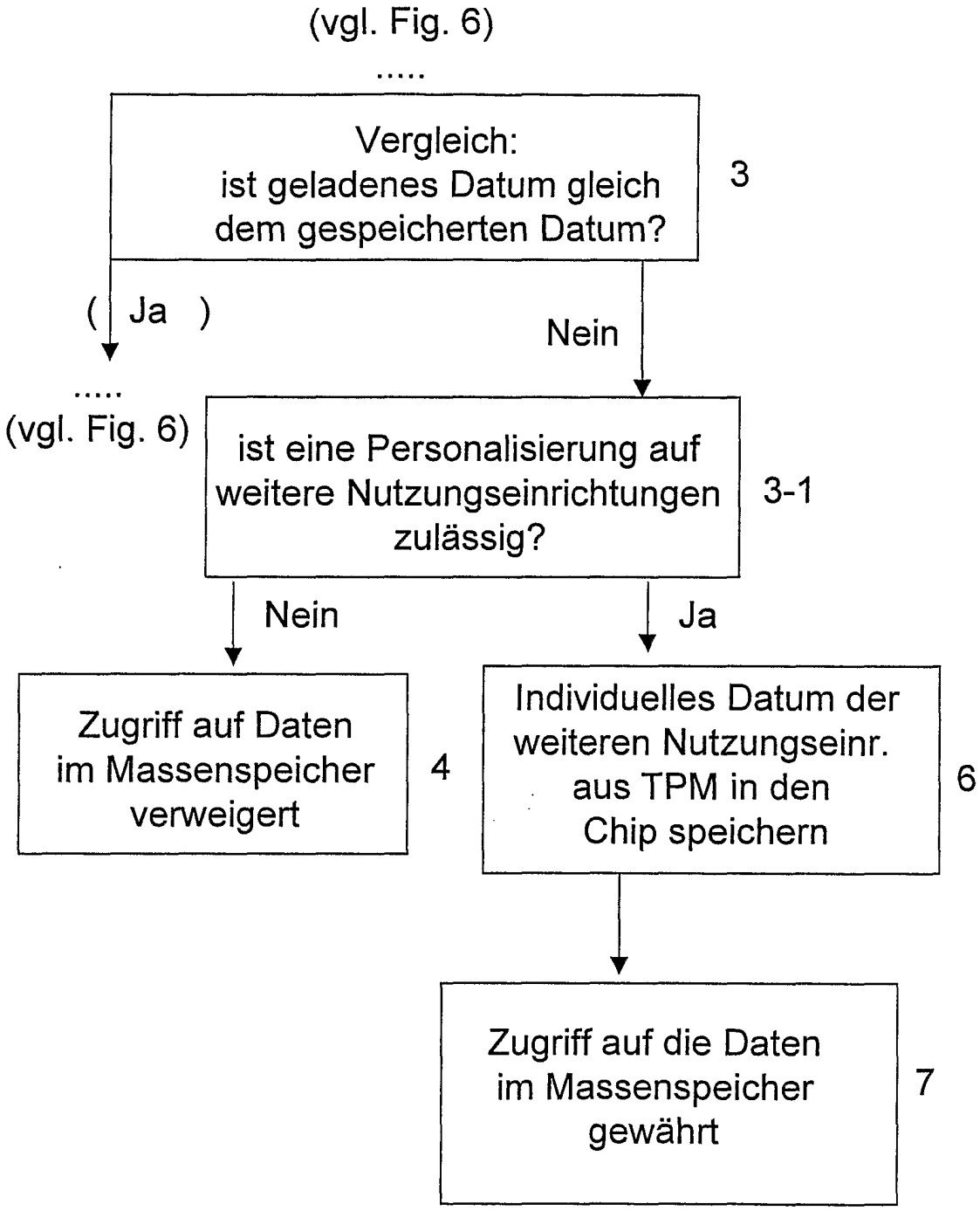

(vgl. Fig. 6)
.....
Vergleich:
ist geladenes Datum gleich
dem gespeicherten Datum?
3
(Ja)
Nein
.....
(vgl. Fig. 6)
ist eine Personalisierung auf
weitere Nutzungseinrichtungen
zulässig?
3-1
Nein
Ja
Zugriff auf Daten
im Massenspeicher
verweigert
4
Individuelles Datum der
weiteren Nutzungseinr.
aus TPM in den
Chip speichern
6
Zugriff auf die Daten
im Massenspeicher
gewährt
7

Fig. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/008997

A. CLASSIFICATION OF SUBJECT MATTER
G06F1/00 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 357 005 B1 (DEVAUX FRANCOIS ET AL) 12 March 2002 (2002-03-12) columns 3,4; figure 1	1-23
A	WO 02/11081 A (ORGA KARTENSYSTEME GMBH; BORMANN, FRANK, C; FISCHER, DIRK; FIEDLER, AL) 7 February 2002 (2002-02-07) cited in the application the whole document	1-23
A	US 5 991 399 A (GRAUNKE ET AL) 23 November 1999 (1999-11-23) column 7	1-23
A	US 2003/079133 A1 (BREITER GERD ET AL) 24 April 2003 (2003-04-24) the whole document	1-23

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 November 2005	25/11/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Damp, S

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/008997

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 905 798 A (NERLIKAR ET AL) 18 May 1999 (1999-05-18) the whole document	1-23
A	WO 94/06071 A (ABDULHAYOGLU, MELIH) 17 March 1994 (1994-03-17) the whole document	1-23
A	DE 103 01 927 A1 (NEUEN, WALTER W) 5 August 2004 (2004-08-05) the whole document	1-23
A	FR 2 790 346 A (SCHLUMBERGER SYSTEMES) 1 September 2000 (2000-09-01) cited in the application the whole document	1-23
A	EP 1 349 058 A (TDK CORPORATION) 1 October 2003 (2003-10-01) the whole document	1-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/008997

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6357005 B1	12-03-2002	AT 193384 T	15-06-2000
		CA 2261629 A1	05-02-1998
		DE 69702135 D1	29-06-2000
		DE 69702135 T2	09-11-2000
		DK 912920 T3	30-10-2000
		EP 0912920 A1	06-05-1999
		ES 2147016 T3	16-08-2000
		FR 2751767 A1	30-01-1998
		WO 9804966 A1	05-02-1998
		GR 3034219 T3	29-12-2000
		JP 2001502102 T	13-02-2001
WO 0211081 A	07-02-2002	AU 6223601 A	13-02-2002
US 5991399 A	23-11-1999	AU 1820199 A	05-07-1999
		WO 9931842 A1	24-06-1999
US 2003079133 A1	24-04-2003	CN 1592876 A	09-03-2005
		WO 03036441 A2	01-05-2003
		EP 1466226 A2	13-10-2004
		JP 2005506627 T	03-03-2005
US 5905798 A	18-05-1999	NONE	
WO 9406071 A	17-03-1994	AU 4971993 A	29-03-1994
		EP 0610497 A1	17-08-1994
		JP 7503566 T	13-04-1995
DE 10301927 A1	05-08-2004	NONE	
FR 2790346 A	01-09-2000	AT 284069 T	15-12-2004
		CN 1341259 A	20-03-2002
		DE 60016383 D1	05-01-2005
		EP 1155410 A1	21-11-2001
		ES 2233336 T3	16-06-2005
		WO 0051119 A1	31-08-2000
		HK 1045212 A1	12-08-2005
		JP 2002538566 A	12-11-2002
EP 1349058 A	01-10-2003	WO 02061567 A1	08-08-2002
		JP 3569226 B2	22-09-2004
		JP 2002196891 A	12-07-2002
		TW 528953 B	21-04-2003
		US 2004042363 A1	04-03-2004

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/008997

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
G06F1/00 G11B20/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F G11B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 6 357 005 B1 (DEVAUX FRANCOIS ET AL) 12. März 2002 (2002-03-12) Spalten 3,4; Abbildung 1	1-23
A	WO 02/11081 A (ORGA KARTENSYSTEME GMBH; BORMANN, FRANK, C; FISCHER, DIRK; FIEDLER, AL) 7. Februar 2002 (2002-02-07) in der Anmeldung erwähnt das ganze Dokument	1-23
A	US 5 991 399 A (GRAUNKE ET AL) 23. November 1999 (1999-11-23) Spalte 7	1-23
A	US 2003/079133 A1 (BREITER GERD ET AL) 24. April 2003 (2003-04-24) das ganze Dokument	1-23

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
18. November 2005	25/11/2005

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Damp, S

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/008997

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 905 798 A (NERLIKAR ET AL) 18. Mai 1999 (1999-05-18) das ganze Dokument	1-23
A	WO 94/06071 A (ABDULHAYOGLU, MELIH) 17. März 1994 (1994-03-17) das ganze Dokument	1-23
A	DE 103 01 927 A1 (NEUEN, WALTER W) 5. August 2004 (2004-08-05) das ganze Dokument	1-23
A	FR 2 790 346 A (SCHLUMBERGER SYSTEMES) 1. September 2000 (2000-09-01) in der Anmeldung erwähnt das ganze Dokument	1-23
A	EP 1 349 058 A (TDK CORPORATION) 1. Oktober 2003 (2003-10-01) das ganze Dokument	1-23

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internales Aktenzeichen
PCT/EP2005/008997

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 6357005 B1	12-03-2002	AT 193384 T	15-06-2000
		CA 2261629 A1	05-02-1998
		DE 69702135 D1	29-06-2000
		DE 69702135 T2	09-11-2000
		DK 912920 T3	30-10-2000
		EP 0912920 A1	06-05-1999
		ES 2147016 T3	16-08-2000
		FR 2751767 A1	30-01-1998
		WO 9804966 A1	05-02-1998
		GR 3034219 T3	29-12-2000
		JP 2001502102 T	13-02-2001
WO 0211081 A	07-02-2002	AU 6223601 A	13-02-2002
US 5991399 A	23-11-1999	AU 1820199 A	05-07-1999
		WO 9931842 A1	24-06-1999
US 2003079133 A1	24-04-2003	CN 1592876 A	09-03-2005
		WO 03036441 A2	01-05-2003
		EP 1466226 A2	13-10-2004
		JP 2005506627 T	03-03-2005
US 5905798 A	18-05-1999	KEINE	
WO 9406071 A	17-03-1994	AU 4971993 A	29-03-1994
		EP 0610497 A1	17-08-1994
		JP 7503566 T	13-04-1995
DE 10301927 A1	05-08-2004	KEINE	
FR 2790346 A	01-09-2000	AT 284069 T	15-12-2004
		CN 1341259 A	20-03-2002
		DE 60016383 D1	05-01-2005
		EP 1155410 A1	21-11-2001
		ES 2233336 T3	16-06-2005
		WO 0051119 A1	31-08-2000
		HK 1045212 A1	12-08-2005
		JP 2002538566 A	12-11-2002
EP 1349058 A	01-10-2003	WO 02061567 A1	08-08-2002
		JP 3569226 B2	22-09-2004
		JP 2002196891 A	12-07-2002
		TW 528953 B	21-04-2003
		US 2004042363 A1	04-03-2004