



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
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

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.

(57) Zusammenfassung: Die Erfindung schafft ein Verfahren zur Sicherung der Daten im Massenspeicher eines Datenträgers mit einem Massenspeicher und mit einem Chip gegen unbefugte Nutzung. Bei einem Zugriff einer Nutzungseinrichtung auf den Datenträger, um die Daten im Massenspeicher zu nutzen, wird mindestens ein Zustandskennzeichen des Datenträgers überprüft, durch das ein maximaler Umfang der zulässigen Nutzung der Daten im Massenspeicher festgelegt ist. Nur falls der gemäss dem Zustandskennzeichen festgelegte maximale Umfang der zulässigen Nutzung der Daten eine weitere Nutzung der Daten zulässt, kann die Nutzung der Daten im Massenspeicher gewährt werden.

Sicherung von Daten eines Datenträgers mit Massenspeicher und Chip gegen unbefugte Nutzung

Die Erfindung betrifft ein Verfahren zur Sicherung von Daten eines Datenträgers mit einem Massenspeicher und einem Chip gegen unbefugte Nutzung, sowie einen entsprechenden Datenträger.

Der Datenträger mit einem Massenspeicher ist z.B. ein Datenträger mit einem optischen 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 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.

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 Multimediage-

räte 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..

5

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
10 vorgesehen sein, dass die Daten mit Ausnahme eines zu Demonstrationszwecken freigegebenen Teils der Daten verschlüsselt sind.

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-
15 ROM sind Daten abgespeichert, wobei alle oder ein Teil der Daten verschlüsselt sind. Der Chip enthält einen 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
20 Schlüssel kann für jede CD-ROM individuell sein. 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. Bei der Herstellung der CD-
25 ROM werden Daten mit einem geheimen Schlüssel verschlüsselt und in die CD-ROM gespeichert. Der verwendete geheime Schlüssel wird in den Chip gespeichert, zum wieder Entschlüsseln der verschlüsselten Daten. Dadurch, dass die Daten im Chip entschlüsselt werden und der Schlüssel den Chip nie

verlässt, kann der Schlüssel nicht kopiert werden. Folglich kann keine funktionsfähige Kopie der CD-ROM angefertigt werden.

Bei der CD-ROM aus WO 00/51119 kann der Besitzer des Originals der CD-ROM, die den Chip aufweist, die Daten beliebig oft entschlüsseln und nutzen und die entschlüsselten Daten beliebig lange nutzen.

Häufig besteht jedoch der Wunsch, dass die Nutzung von Daten in einem Datenträger mit einem Massenspeicher dem Umfang nach begrenzt ist. Beispielsweise soll im Massenspeicher gespeicherte Software, die zum Installieren in einem Rechner vorgesehen ist, nur ein einziges Mal oder eine vorbestimmte Anzahl von Malen installiert werden dürfen. Bei einem anderen Beispiel sollen Multimediadaten wie z.B. Musik oder Filmdaten nur eine vorbestimmte Anzahl von Malen (evtl. nur ein einziges Mal) abgespielt werden dürfen. Oft ist gewünscht, dass die Nutzungsdauer der Daten begrenzt ist.

Aufgabe der Erfindung ist es, ein Verfahren zur Zugriffssicherung für Daten eines Datenträgers der eingangs genannten Art mit einem Massenspeicher und einem Chip zu schaffen, bei dem der Umfang der Nutzung der Daten begrenzt ist, insbesondere die Anzahl der möglichen Nutzungen der Daten und/oder die Nutzungsdauer begrenzt ist.

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

In Anspruch 1 ist ein Verfahren zur Sicherung der Daten im Massenspeicher eines Datenträgers gegen unbefugte Nutzung angegeben. Der Datenträger

hat einen Massenspeicher, in dem die Daten abgespeichert sind, und einen Chip. In dem Chip ist gemäß der Erfindung mindestens ein Zustandskennzeichen implementiert, durch das ein maximaler Umfang der zulässigen Nutzung der Daten im Massenspeicher festgelegt ist. Bei dem Verfahren

5 wird bei einem Zugriff einer Nutzungseinrichtung auf den Datenträger, um die Daten im Massenspeicher zu nutzen, das Zustandskennzeichen des Datenträgers überprüft. Nur falls der gemäß dem Zustandskennzeichen festgelegte maximale Umfang der zulässigen Nutzung der Daten eine weitere Nutzung der Daten zulässt, wird die Nutzung der Daten im Massenspeicher

10 gewährt.

Hat das Zustandskennzeichen dagegen einen Wert, der angibt, dass der maximale Umfang der möglichen Nutzung bereits erreicht bzw. überschritten ist, können die Daten nicht genutzt werden.

15

Daher ist gemäß Anspruch 1 ein Verfahren zur Zugriffssicherung der Daten im Massenspeicher eines Datenträgers angegeben, bei dem der Umfang der Nutzung der Daten begrenzt ist.

20 Vorzugsweise wird das Zustandskennzeichen innerhalb des Chips überprüft.

Wahlweise wird die Nutzung der Daten nicht gewährt, weil das Zustandskennzeichen keine weitere Nutzung der Daten zulässt, indem der Zugriff auf

25 den Massenspeicher verwehrt wird.

Wahlweise sind die Daten in dem Massenspeicher zumindest teilweise verschlüsselt abgespeichert, wobei in dem Chip weiter ein Schlüssel zum Entschlüsseln der verschlüsselten Daten abgespeichert ist.

- 5 -

Bei Ausführungsformen der Erfindung, bei denen die Daten in dem Massenspeicher zumindest teilweise verschlüsselt abgespeichert sind, wobei in dem Chip weiter ein Schlüssel zum Entschlüsseln der verschlüsselten Daten abgespeichert ist, wird vorzugsweise nur falls der gemäß dem Zustandskennzeichen festgelegte maximale Umfang der zulässigen Nutzung der Daten eine weitere Nutzung der Daten zulässt, der Zugriff auf den Schlüssel zum Entschlüsseln der Daten gewährt. Mit anderen Worten ist bei - ganz oder teilweise - verschlüsselten Daten vorzugsweise der im Chip abgespeicherte

5 Schlüsselschlüssel zum Entschlüsseln der Daten mit dem Zustandskennzeichen abgesichert. Wenn das Zustandskennzeichen eine weitere Nutzung der Daten nicht zulässt, ist der Zugriff auf den Schlüssel verwehrt. Somit können auch die Daten nicht genutzt werden.

10 Der maximale Umfang der Nutzung umfasst vorzugsweise eine maximale Anzahl von zulässigen Nutzungen und/oder eine maximale Nutzungsdauer.

Vorzugsweise werden weiter die Daten aus dem Massenspeicher, sofern der

20 Zugriff auf sie gewährt wird, außerhalb des Massenspeichers zur Nutzung bereitgestellt.

Weiter vorzugsweise werden die Daten außerhalb des Massenspeichers bereitgestellt, indem sie in einem externen Speicher außerhalb des Massenspeichers und außerhalb des Chips installiert werden. Vorzugsweise werden die

25 Daten in der Nutzungseinrichtung installiert. Die Nutzungseinrichtung kann beispielsweise ein Computer sein.

Wahlweise werden die zur Nutzung bereitgestellten Daten an ein Ausgabegerät, insbesondere an ein Ausgabegerät für Multimediadaten wie z.B. Musikdaten und/oder Filmdaten, bereitgestellt.

- 5 Vorzugsweise wird das Zustandskennzeichen bei jedem Bereitstellen der Daten zu ihrer Nutzung außerhalb des Massenspeicher, insbesondere bei jeder Installation der Daten in einem externen Speicher, derart verändert, dass der maximale Umfang der zulässigen Nutzung verringert wird. Wahlweise wird das Zustandskennzeichen vor oder nach dem Bereitstellen ver-
- 10 ändert. Insbesondere wird das Zustandskennzeichen wahlweise vor oder nach der Installation der Daten in einem externen Speicher verändert.

- Weiter wird das Zustandskennzeichen vorzugsweise bei jedem Rückgängigmachen des Bereitstellens der Daten zu ihrer Nutzung, insbesondere bei
- 15 jeder Deinstallation der Daten aus einem externen Speicher, derart verändert, dass der maximale Umfang der zulässigen Nutzung erhöht wird. Wahlweise führt das Rückgängigmachen des Bereitstellens nur dann zu der Veränderung des Zustandskennzeichens, so dass der maximale Umfang der zulässigen Nutzung erhöht wird, falls das Rückgängigmachen innerhalb ei-
- 20 nes vorbestimmten Zeitintervalls erfolgt. Das Zeitintervall kann beispielsweise ein Lizenzzeitraum sein, während dessen die Nutzung der Daten zulässig ist. Nach Ablauf des Zeitintervalls (z.B. Lizenzzeitraums) führt in diesem Fall das Rückgängigmachen (z.B. Deinstallation der Daten) nicht mehr zu der Veränderung des Zustandskennzeichens, durch die der maximale
- 25 Umfang der zulässigen Nutzung erhöht würde. Wahlweise wird das Zustandskennzeichen vor oder nach dem Rückgängigmachen des Bereitstellens verändert. Insbesondere wird das Zustandskennzeichen wahlweise vor oder nach der Deinstallation der Daten in einem externen Speicher verändert.

- Als Zustandskennzeichen wird wahlweise ein Flag mit zwei unterschiedlichen möglichen Zuständen verwendet. Alternativ wird als Zustandskennzeichen ein Zähler mit mehr als zwei unterschiedlichen möglichen Zuständen verwendet. Der Zähler wird beispielsweise bei jeder Installation der Daten in einem Computer oder dergleichen um einen vorbestimmten Zähler-
- 5 schritt (z.B. um eins) erhöht und bei jeder Deinstallation der Daten wieder um den Zähler schritt verringert. Hat der Zähler eine Höchstgrenze erreicht, ist keine weitere Installation der Daten mehr möglich. Alternativ wird der Zähler bei Installation verringert und bei Deinstallation erhöht, und eine weitere
- 10 Installation ist z.B. nicht mehr möglich, sobald der Zählerstand den Wert Null erreicht hat. Wahlweise führt eine Deinstallation der Daten nur innerhalb eines vorbestimmten Lizenzzeitraums zu einer Verringerung (bzw. Erhöhung) des Zählerstandes um den vorbestimmten Zähler schritt.
- 15 Der Massenspeicher ist vorzugsweise ein optischer Speicher. Alternativ kann der Massenspeicher auch ein elektronischer Massenspeicher sein.

- Bei Ausführungsformen, bei denen die Daten im Massenspeicher zumindest teilweise verschlüsselt sind, werden die Daten wahlweise innerhalb des
- 20 Chips entschlüsselt. Alternativ können die Daten in einem Sicherheitsmodul, z.B. einem Trusted Platform Modul (TPM), der Nutzungseinrichtung entschlüsselt werden. Das Sicherheitsmodul (z.B. TPM) hat einen Mikroprozessor-Chip, in dem Daten verschlüsselt installiert sind. Für einen Computer ist beispielsweise die Seriennummer des Computer-Mikroprozessors und/oder
- 25 einer oder mehrerer weiterer Computerkomponenten wie z.B. Netzwerkkarte, Massenspeicher etc. in einem Sicherheitsmodul (z.B. TPM) verschlüsselt installiert. Alternativ oder zusätzlich zur Seriennummer können andere individuelle Daten des Computer-Mikroprozessors bzw. der Computerkomponente installiert sein. Das Sicherheitsmodul (z.B. TPM) ermöglicht es ei-

5 nem 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.

10 Gemäß einer Weiterbildung wird weiter eine Zugriffsberechtigung überprüft. Ein Zugriff auf den Datenträger wird nur nach einer erfolgreichen Verifizierung der Zugriffsberechtigung möglich. Vorzugsweise wird zuerst die Zugriffsberechtigung (PIN etc.) überprüft, bevor anschließend das Zustandskennzeichen überprüft werden kann. Die Überprüfung der Zugangsberechtigung kann insbesondere mit einem Passwort und/oder einer PIN und/oder einem biometrischen Identifizierungsmerkmal wie z.B. Fingerabdruck, Augeniris, Gesichtsform, Handform oder dergleichen durchgeführt
15 werden. Wahlweise wird für die Überprüfung der Zugangsberechtigung ein gesondertes Sicherheitselement wie z.B. ein "Dongle" verwendet.

20 Gemäß einer anderen Weiterbildung des Verfahrens wird nach jedem Bereitstellen der Daten zur Nutzung ein kumulativer Zähler um einen vorbestimmten Zähler schritt erhöht (inkrementiert). Der kumulative Zähler wird nicht verringert (dekrementiert), wenn die Bereitstellung der Daten zur Nutzung rückgängig gemacht wird, weil z.B. die Daten deinstalliert werden. Mit dem kumulativen Zähler wird somit die Gesamtzahl von Nutzungen der Daten aus dem Massenspeicher gezählt.

25

Vorzugsweise wird das Zustandskennzeichen innerhalb des Chips überprüft. Dies hat den Vorteil, dass die Überprüfung in der gegen unbefugte Manipulationen gesicherten Umgebung des Chips erfolgt. Vorzugsweise ist das Zustandskennzeichen innerhalb des Chips abgespeichert. Falls nun zu-

- 9 -

dem die Überprüfung im Chip stattfindet, braucht das Zustandskennzeichen den Chip niemals zu verlassen und ist daher besonders gut gegen Manipulationen gesichert. Wahlweise ist das Zustandskennzeichen verschlüsselt im Chip abgespeichert. Wahlweise ist das Zustandskennzeichen von außerhalb
5 des Chips nicht veränderbar. Wahlweise ist das Zustandskennzeichen von außerhalb des Chips höchstens auslesbar und also überprüfbar, nicht aber veränderbar. Wahlweise ist der Zugriff auf das Zustandskennzeichen von außerhalb des Chips völlig verwehrt, so dass nur interne Datenverarbeitungsvorgänge innerhalb des Chips auf das Zustandskennzeichen zugreifen
10 können. Wahlweise ist das Zustandskennzeichen verschlüsselt abgespeichert, so dass es zusätzlich gegen Manipulationen gesichert ist.

Der erfindungsgemäße Datenträger ist vorzugsweise als optischer Datenträger mit einem optischen Massenspeicher, insbesondere CD, CD-RW, DVD
15 oder DVD-RW, gestaltet, der zusätzlich den Chip aufweist. Alternativ kann der Datenträger auch als elektronischer Datenträger mit einem elektronischen Massenspeicher gestaltet sein, der zusätzlich einen zumindest logisch gesonderten Chip hat, in dem das Zustandskennzeichen und ggf. der Schlüssel abgespeichert bzw. implementiert sind.

20

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

Fig. 1 eine erfindungsgemäße CD/DVD, die einen optischen Speicher, einen
25 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;

- 5 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;

10 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;

15 Fig. 5 ein Flussdiagramm zur Veranschaulichung eines Verfahrens zur Zugriffssicherung der Daten im Massenspeicher eines Datenträgers mit einem Massenspeicher und mit einem Chip, gemäß einer bevorzugten Ausführungsform der Erfindung.

Fig. 1 zeigt eine erfindungsgemäße CD/DVD 100. Die CD/DVD 100 hat, wie
20 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
25 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 Anzahl von Ausgleichsgewichten vorgesehen.

Fig. 2 zeigt ein Beispiel für ein zur Anbringung auf einer CD/DVD wie der
5 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
10 einzelne Kontaktflächen (allgemein typischerweise eine Anzahl von zwei bis zehn 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
15 vorgesehenes Kontaktfeld 305. Das Kontaktfeld 305 ist, ähnlich wie das Kontaktfeld 205 aus Fig. 2, ringförmig gestaltet, hat aber sechs (allgemein ca. 2 bis 10) konzentrisch zueinander angeordnete, ringförmige Kontaktflächen.

Bei einer erfindungsgemäßen CD/DVD ist beispielsweise im freien Bereich
20 102 zwischen dem Mittelloch 101 und dem Datenbereich 103 ein Kontaktfeld 205, 305 gemäß Fig. 2 oder Fig. 3 vorgesehen, damit ein auf der CD/DVD 100 angeordneter Chip 104 kontaktiert werden kann. Die einzelnen Kontaktflächen (z.B. sechs bzw. acht Stück) können z.B. gemäß ISO/IEC 7816, USB, RS232/V.24 oder einem anderen Protokoll ansteuerbar sein.

25

Fig. 4 zeigt eine weitere 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 eines Verfahrens zur Zugriffssicherung der Daten im Massenspeicher eines Datenträgers mit einem Massenspeicher und mit einem Chip gemäß einer bevorzugten Ausführungsform der Erfindung.

In einem ersten Schritt 1 wird eine PIN überprüft und, falls die PIN verifiziert wird, zu Schritt 2 fortgeschritten. Falls keine PIN-Prüfung erforderlich ist, beginnt das Verfahren mit Schritt 2. In Schritt 2 wird ein in dem Chip implementierter Zähler überprüft, der die Anzahl von erfolgten Nutzungen der Daten angibt und auf eine zulässige Höchstzahl von Nutzungen begrenzt. Falls gemäß dem Zähler die zulässige Höchstzahl von Nutzungen bereits erreicht ist, wird in Schritt 3 der Zugriff auf die Daten im Massenspeicher verweigert. Falls gemäß dem Zähler die zulässige Höchstzahl von Nutzungen noch nicht erreicht ist, wird in Schritt 4 der Zugriff auf die Daten im Massenspeicher gewährt. Im Anschluss an Schritt 4 werden in Schritt 5 die Daten in einem Computer installiert und der Zähler im Chip des Datenträgers um eins hochgezählt (inkrementiert). Falls die Daten wieder deinstalliert würden, würde der Zähler wieder um eins heruntergezählt (dekrementiert).

Der Chip, in dem der Zähler implementiert ist, ist typischerweise ein Mikroprozessorchip mit einem Betriebssystem und einer oder mehreren Applikationen. Der Zähler wird typischerweise durch den Mikroprozessor, und typischerweise unter Verwendung des Betriebssystems hochgezählt bzw. heruntergezählt. Der Zähler kann insbesondere wahlweise als Betriebssystemfunktion oder als Applikation in dem Chip implementiert sein.

Im Folgenden wird im Detail eine bevorzugte Ausführungsform eines erfindungsgemäßen Verfahrens zur Zugriffssicherung der Daten im Massenspeicher eines Datenträgers mit einem Massenspeicher und einem Chip beschrieben.

5

Der Datenträger ist eine DVD mit einem optischen Massenspeicher. Im optischen Massenspeicher sind Daten eines Programms abgespeichert, das im Speicher eines Computers installiert werden soll, um es nachfolgend auf dem Computer ablaufen zu lassen. Die Daten sind zumindest teilweise verschlüsselt. Die DVD hat im optischen Speicher weiter einen unverschlüsselten Bereich zum Booten der DVD. An der DVD ist, beispielsweise wie in Fig. 1 oder Fig. 4 dargestellt, ein Chip montiert. Im Chip ist ein Schlüssel zum Entschlüsseln der Daten im optischen Massenspeicher abgespeichert. Optional ist im Chip eine PIN abgespeichert. Der Zugriff auf den Schlüssel im

10 Chip ist mit einem erfindungsgemäßen Zustandskennzeichen abgesichert, das ebenfalls im Chip implementiert ist. Das Zustandskennzeichen ist ein Flag mit zwei Zuständen, gelöscht und gesetzt.

Für andere Arten von Datenträgern (CD, SC, CF, MMC) mit optischen oder elektronischen Massenspeichern, 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.

25 Ein Nutzer, der das Programm in einem Computer installieren möchte, legt die DVD in das DVD-Laufwerk des Computers (bzw. Abspielgeräts etc.) ein. Aus dem unverschlüsselten Bereich des optischen Massenspeichers der DVD wird ein Installations-Programm (Start- bzw. Boot-Programm) hochgefahren, durch das eine erste Kommunikation mit der DVD ermöglicht wird.

Das Installations-Programm erkennt, dass eine Nutzungseinrichtung über ein DVD-Laufwerk versucht, auf die DVD zuzugreifen und verlangt vom Nutzer zunächst die Eingabe einer PIN. Bei alternativen Ausführungsformen ist eine PIN-Eingabe nicht erforderlich. Der Nutzer gibt bei der vorliegenden Ausführungsform die PIN über eine Tastatur ein, z.B. über die Tastatur des Computers. Bei einem Abspielgerät kann alternativ die PIN über Tasten eingegeben werden, die am Abspielgerät ohnehin vorhanden sind, oder das Abspielgerät weist ein oder mehrere zusätzliche Tasten auf.

10

Zur Überprüfung und Verifizierung der PIN muss auf den Chip der CD zugegriffen werden.

Gemäß einer ersten Alternative enthält das DVD-Laufwerk einen Chipleser (genauer ein Chip-Lese-Schreibgerät). In diesem Fall beginnt als nächstes der Chipleser die Kommunikation mit dem Chip der CD. Die Kommunikation kann kontaktlos oder kontaktbehaftet erfolgen.

Gemäß einer zweiten Alternative hat das DVD-Laufwerk keinen Chipleser. In diesem Fall wird der Nutzer aufgefordert, die DVD aus dem DVD-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 DVD nahe genug angenähert worden ist.

Der Chipleser (intern oder extern) sendet die eingegebene PIN an den Chip. Im Chip werden die eingegebene PIN und die abgespeicherte PIN vergli-

chen. Wahlweise ist die PIN-Überprüfung mit einem an sich bekannten Fehlbedienungszähler gekoppelt, der die Anzahl falscher PIN-Eingaben registriert und bei zu häufiger falscher PIN-Eingabe den Chip sperrt.

- 5 Falls die PINs übereinstimmen, wird die Überprüfung des Zustandskennzeichens ermöglicht. Bei Ausführungsformen des Verfahrens ohne PIN-Prüfung wird sofort mit der Überprüfung des Zustandskennzeichens begonnen, sobald der Chip mit dem Chipleser angesprochen wird.
- 10 Das Zustandskennzeichen ist ein im Chip der CD implementiertes Flag. Das Flag wird nun mit dem Chipleser (intern oder extern) überprüft. Die DVD wird im vorliegenden Beispiel zum ersten Mal benutzt. Das Flag ist daher (noch) gelöscht, wodurch angegeben ist, dass eine (weitere) Nutzung der Daten zulässig ist.
- 15 Nachdem das Flag im Chip als gelöscht erkannt worden ist, geht die Kommunikation auf das DVD-Laufwerk über, und die Daten aus dem optischen Massenspeicher werden in einen Zwischenspeicher gelesen, der sowohl für das DVD-Laufwerk als auch für den Chipleser zugänglich ist. Anschließend
- 20 werden die Daten in den Chip gelesen. Im Chip werden die Daten mit dem Schlüssel entschlüsselt.

Die entschlüsselten Daten werden schließlich in den Computer installiert.

- 25 Sobald die Installation der Daten im Computer abgeschlossen ist, wird das Flag (Zustandskennzeichen) im Chip des Datenträgers gesetzt. Hierdurch wird kenntlich gemacht und erzielt, dass keine nochmalige Installation der Daten möglich ist. Bei alternativen Ausführungsformen wird das Flag an einem anderen Punkt im Verfahrensablauf gesetzt. Beispielsweise wird das

Flag alternativ gesetzt, nachdem die verschlüsselten Daten in den Zwischenspeicher gelesen worden sind. Alternativ wird das Flag gesetzt, nachdem die Daten entschlüsselt worden sind. Alternativ wird das Flag gesetzt, nachdem es überprüft und als gelöscht erkannt worden ist.

5

Dass die Daten nicht nochmals installiert werden können, wird beispielsweise dadurch erzielt, dass, nachdem das gesetzte Flag erkannt worden ist, kein Zugriff auf den optischen Massenspeicher gewährt wird, so dass die Daten nicht zum Entschlüsseln aus dem optischen Massenspeicher ausgelesen werden können. Alternativ oder zusätzlich wird, nachdem das gesetzte Flag erkannt worden ist, kein Zugriff auf den Schlüssel gewährt, so dass die verschlüsselten Daten zwar ggf. ausgelesen werden können, aber nicht entschlüsselt werden können.

15 Werden die Daten unter Verwendung des Datenträgers wieder von dem Computer deinstalliert, wird das Flag wieder gelöscht, sobald die Deinstallation abgeschlossen ist oder sobald zumindest vorbestimmte Teilschritte der Deinstallation abgeschlossen sind, so dass die Daten nicht mehr nutzbar sind. Dabei wird zur Deinstallation vorzugsweise eine im Datenträger im-

20 plementierte Deinstallationsfunktion verwendet.

Bei alternativen Ausführungsformen ist an Stelle eines Flag ein Zähler in dem Chip installiert, der um eins hochgezählt (bzw. alternativ heruntergezählt) wird, sobald die Installation der Daten abgeschlossen wird, und der

25 um eins heruntergezählt (bzw. alternativ hochgezählt) wird, wenn die Daten wieder deinstalliert werden.

Gemäß einer Weiterbildung der Erfindung, die in einer anderen, am selben Tag eingereichten Patentanmeldung beschrieben ist, ist der Datenträger zu-

- 17 -

sätzlich auf eine oder mehrere vorbestimmte Nutzungseinrichtungen personalisiert, so dass die Nutzung des Datenträgers nur mit der bzw. den vorbestimmten Nutzungseinrichtung(en) möglich ist.

Patentansprüche

1. Verfahren zur Sicherung der Daten im Massenspeicher eines Datenträgers mit einem Massenspeicher und mit einem Chip gegen unbefugte Nutzung
- 5 **dadurch gekennzeichnet, dass**
- bei einem Zugriff einer Nutzungseinrichtung auf den Datenträger, um die Daten im Massenspeicher zu nutzen,
- mindestens ein Zustandskennzeichen des Datenträgers überprüft wird, durch das ein maximaler Umfang der zulässigen Nutzung der Daten im
- 10 Massenspeicher festgelegt ist,
- und die Nutzung der Daten im Massenspeicher höchstens gewährt wird, falls der gemäß dem Zustandskennzeichen festgelegte maximale Umfang der zulässigen Nutzung der Daten eine weitere Nutzung der Daten zulässt,.
- 15 2. Verfahren nach Anspruch 1, 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.
- 20 3. Verfahren nach Anspruch 2, wobei der Zugriff auf den Schlüssel zum Entschlüsseln der Daten höchstens gewährt wird, falls der gemäß dem Zustandskennzeichen festgelegte maximale Umfang der zulässigen Nutzung der Daten eine weitere Nutzung der Daten zulässt.
- 25 4. Verfahren nach einem der Ansprüche 1 bis 3, wobei der maximale Umfang der Nutzung eine maximale Anzahl von zulässigen Nutzungen und/oder eine maximale Nutzungsdauer umfasst.

- 19 -

5. Verfahren nach einem der Ansprüche 1 bis 4, wobei weiter die Daten aus dem Massenspeicher außerhalb des Massenspeichers zur Nutzung bereitgestellt werden.
- 5 6. Verfahren nach Anspruch 5, wobei die Daten außerhalb des Massenspeichers bereitgestellt werden, indem sie in einem externen Speicher außerhalb des Massenspeichers und außerhalb des Chips installiert werden.
7. Verfahren nach Anspruch 6, wobei die Daten in der Nutzungseinrichtung
10 installiert werden.
8. Verfahren nach einem der Ansprüche 5 bis 7, wobei die zur Nutzung bereitgestellten Daten an ein Ausgabegerät, insbesondere an ein Ausgabegerät für Multimediadaten wie z.B. Musikdaten und/oder Filmdaten, bereitgestellt werden.
15
9. Verfahren nach einem der Ansprüche 5 bis 8, wobei das Zustandskennzeichen bei - insbesondere wahlweise vor oder nach - einem, insbesondere jedem, Bereitstellen der Daten zu ihrer Nutzung außerhalb des Massenspeicher, insbesondere bei jeder Installation der Daten in einem externen Speicher, derart verändert wird, dass der maximale Umfang der zulässigen Nutzung verringert wird.
- 20
10. Verfahren nach einem der Ansprüche 5 bis 9, wobei das Zustandskennzeichen bei - insbesondere wahlweise vor oder nach - einem, insbesondere jedem, Rückgängigmachen des Bereitstellens der Daten zu ihrer Nutzung, insbesondere bei jeder Deinstallation der Daten aus einem externen Speicher, derart verändert wird, dass der maximale Umfang der zulässigen Nutzung erhöht wird.
- 25

- 20 -

11. Verfahren nach einem der Ansprüche 1 bis 10, wobei als Zustandskennzeichen ein Flag mit zwei unterschiedlichen möglichen Zuständen verwendet wird.
- 5 12. Verfahren nach einem der Ansprüche 1 bis 11, wobei als Zustandskennzeichen ein Zähler mit mehr als zwei unterschiedlichen möglichen Zuständen verwendet wird.
13. Verfahren nach einem der Ansprüche 1 bis 12, wobei als Massenspeicher
10 ein optischer Speicher vorgesehen ist.
14. Verfahren nach einem der Ansprüche 1 bis 13, wobei weiter eine Zugriffsberechtigung überprüft wird - insbesondere mit einem Passwort und/oder einer PIN und/ oder einem biometrischen Identifizierungsmerk-
15 mal oder einem gesonderten Sicherheitselement - und wobei ein Zugriff auf den Datenträger höchstens nach einer erfolgreichen Verifizierung der Zugriffsberechtigung ermöglicht wird.
15. Verfahren nach einem der Ansprüche 1 bis 14, wobei das Zustandskenn-
20 zeichen innerhalb des Chips überprüft wird.
16. Verfahren nach einem der Ansprüche 1 bis 15, wobei das Zustandskennzeichen innerhalb des Chips abgespeichert ist.
- 25 17. Verfahren nach einem der Ansprüche 1 bis 16, wobei das Zustandskennzeichen von außerhalb des Chips höchstens auslesbar ist und/oder von außerhalb des Chips nicht veränderbar ist.

- 21 -

18. Verfahren nach einem der Ansprüche 1 bis 17, wobei das Zustandskennzeichen verschlüsselt abgespeichert ist.

19. Datenträger mit einem Massenspeicher und einem Chip und mit einem in
5 dem Chip implementierten Verfahren nach einem der Ansprüche 1 bis 18,
dadurch gekennzeichnet, dass
der Datenträger mindestens ein in dem Datenträger implementiertes Zustandskennzeichen aufweist, durch das ein maximaler Umfang der zulässigen Nutzung der Daten im Massenspeicher festgelegt ist.

10

20. Datenträger nach Anspruch 19, der als optischer Datenträger, insbesondere CD, CD-RW, DVD oder DVD-RW, gestaltet ist.

1/3

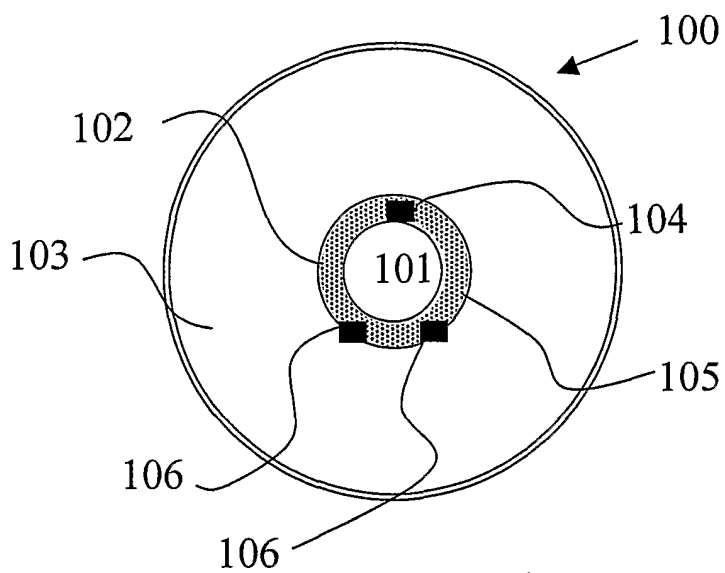


Fig. 1

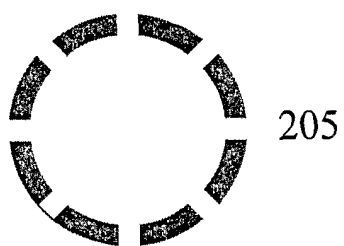


Fig. 2

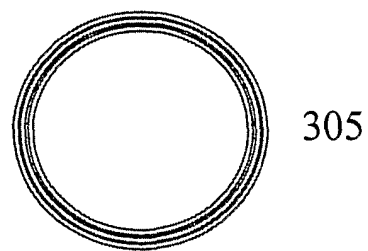


Fig. 3

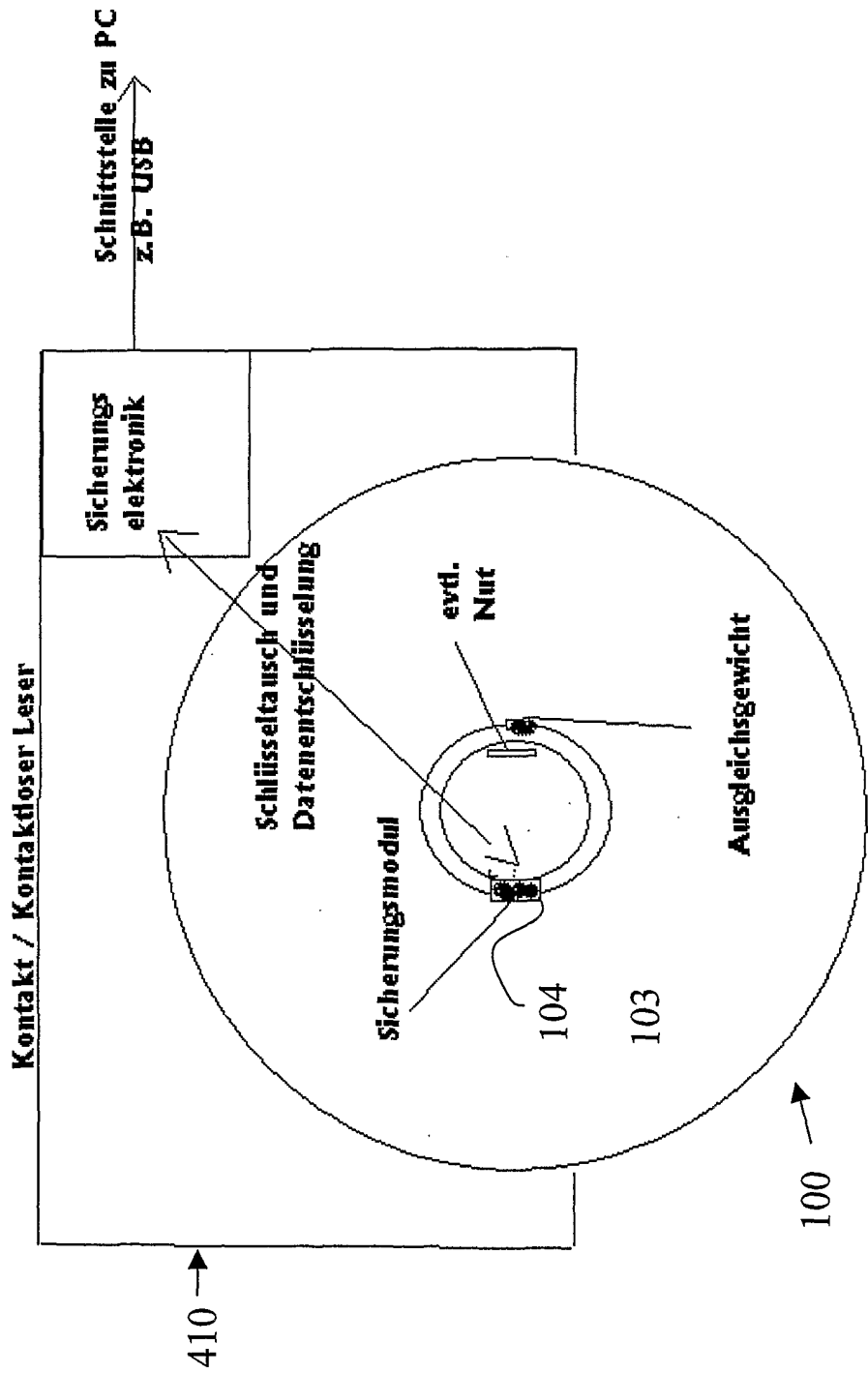


Fig. 4

3/3

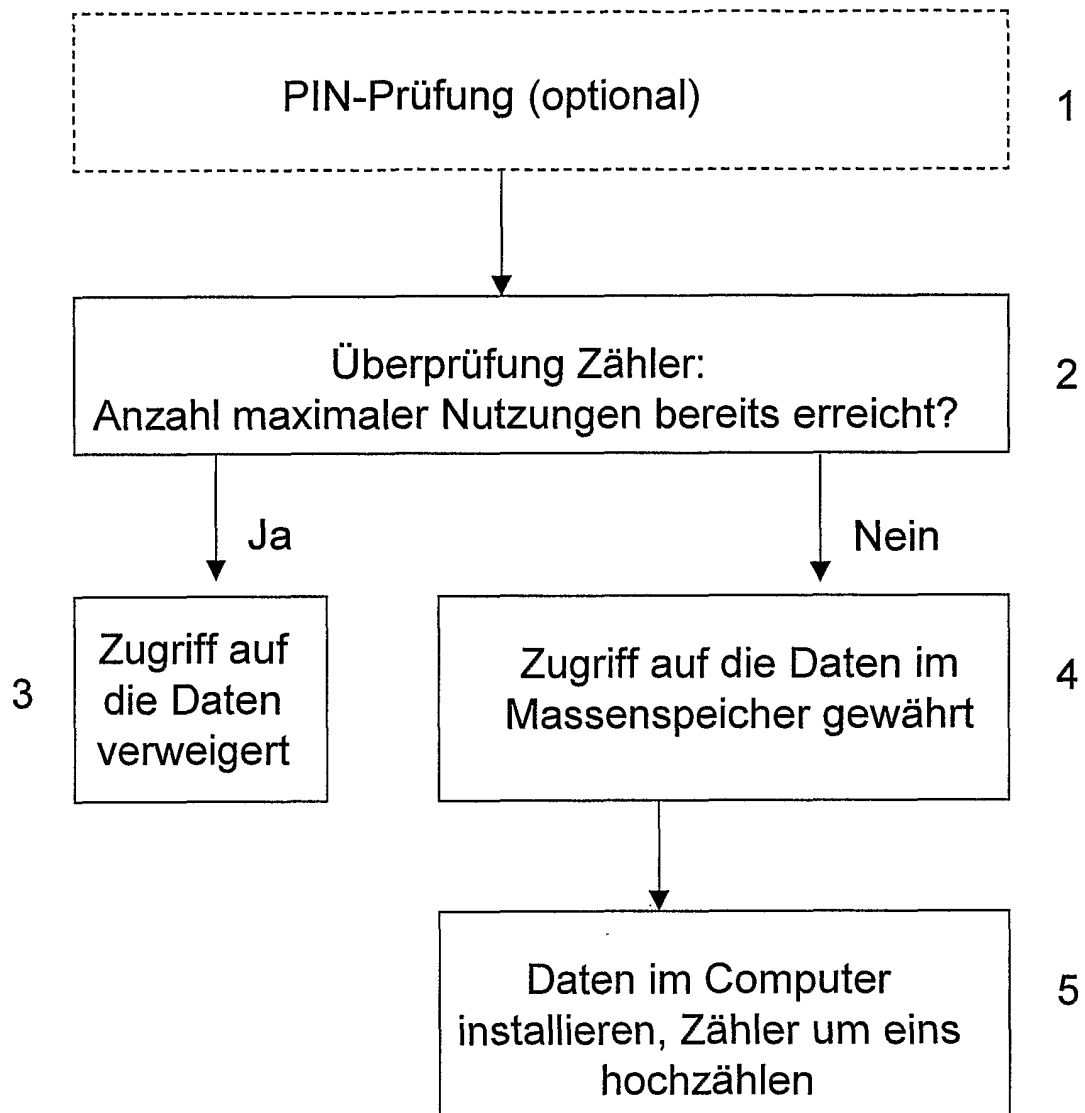


Fig. 5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/008996

A. CLASSIFICATION OF SUBJECT MATTER
G06F1/00

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.
X	WO 99/38162 A (NDS LTD; BAR-ON, GERSHON; ATLOW, SHABTAI) 29 July 1999 (1999-07-29) page 4, lines 1-18	1-20
X	US 6 542 444 B1 (RUETSCHKE MARIO) 1 April 2003 (2003-04-01) column 2, lines 25-42	1-20
A	US 2002/024905 A1 (KAHLMAN JOSEPHUS ARNOLDUS HENRICUS MARIA ET AL) 28 February 2002 (2002-02-28) paragraph '0027!	
A	DE 44 03 206 A1 (WALDORF, RALPH, 78333 STOCKACH, DE) 10 August 1995 (1995-08-10) the whole document	
	----- -/--	

☒ Further documents are listed in the continuation of box C.

☒ 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

8 December 2005

Date of mailing of the international search report

16/12/2005

Name and mailing address of the ISA

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

Authorized officer

Meződi, S

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/008996

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 02/11081 A (ORGA KARTENSYSTEME GMBH; BORMANN, FRANK, C; FISCHER, DIRK; FIEDLER, AL) 7 February 2002 (2002-02-07) page 8, line 21 – page 10, line 3 -----	
A	WO 96/29699 A (MEILLER COMCARD GMBH; LENDER, FRIEDWART; HORSTER, PATRICK) 26 September 1996 (1996-09-26) abstract -----	
A	US 6 357 005 B1 (DEVAUX FRANCOIS ET AL) 12 March 2002 (2002-03-12) abstract -----	
A	EP 1 089 156 A (M-SYSTEMS FLASH DISK PIONEERS LTD) 4 April 2001 (2001-04-04) paragraphs '0018!', '0019!', '0040! -----	
A	EP 0 818 748 A (MURAKOSHI, HIROMASA) 14 January 1998 (1998-01-14) abstract -----	
A	TECHNICAL STANDARD: "System Management: Software License Use Management (XSLM)" SOFTWARE LICENSE USE MANAGEMENT (XSLM), March 1999 (1999-03), pages 25-29,175, XP002271896 page 175 – page 180 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2005/008996

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9938162	A	29-07-1999	AU 1781099 A GB 2338586 A	09-08-1999 22-12-1999
US 6542444	B1	01-04-2003	AU 3185800 A EP 1043684 A1 WO 0058907 A1 JP 2002540547 T	16-10-2000 11-10-2000 05-10-2000 26-11-2002
US 2002024905	A1	28-02-2002	AU 9549601 A CN 1447970 A WO 0217316 A1 JP 2004507028 T	04-03-2002 08-10-2003 28-02-2002 04-03-2004
DE 4403206	A1	10-08-1995	NONE	
WO 0211081	A	07-02-2002	AU 6223601 A	13-02-2002
WO 9629699	A	26-09-1996	AU 5110596 A	08-10-1996
US 6357005	B1	12-03-2002	AT 193384 T CA 2261629 A1 DE 69702135 D1 DE 69702135 T2 DK 912920 T3 EP 0912920 A1 ES 2147016 T3 FR 2751767 A1 WO 9804966 A1 GR 3034219 T3 JP 2001502102 T	15-06-2000 05-02-1998 29-06-2000 09-11-2000 30-10-2000 06-05-1999 16-08-2000 30-01-1998 05-02-1998 29-12-2000 13-02-2001
EP 1089156	A	04-04-2001	AU 7712300 A IL 138661 A JP 2001160002 A TW 473664 B WO 0124054 A1 US 6324537 B1 US 6539380 B1	30-04-2001 17-05-2005 12-06-2001 21-01-2002 05-04-2001 27-11-2001 25-03-2003
EP 0818748	A	14-01-1998	AU 717988 B2 AU 2844497 A CA 2209596 A1 CN 1180201 A HK 1010258 A1 JP 2810033 B2 JP 10083298 A US 5943650 A	06-04-2000 15-01-1998 08-01-1998 29-04-1998 11-09-2003 15-10-1998 31-03-1998 24-08-1999

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2005/008996

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

G06F1/00

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.
X	WO 99/38162 A (NDS LTD; BAR-ON, GERSHON; ATLOW, SHABTAI) 29. Juli 1999 (1999-07-29) Seite 4, Zeilen 1-18	1-20
X	US 6 542 444 B1 (RUETSCHKE MARIO) 1. April 2003 (2003-04-01) Spalte 2, Zeilen 25-42	1-20
A	US 2002/024905 A1 (KAHLMAN JOSEPHUS ARNOLDUS HENRICUS MARIA ET AL) 28. Februar 2002 (2002-02-28) Absatz '0027!	
A	DE 44 03 206 A1 (WALDORF, RALPH, 78333 STOCKACH, DE) 10. August 1995 (1995-08-10) das ganze Dokument	

-/--

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ 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

8. Dezember 2005

Absendedatum des internationalen Recherchenberichts

16/12/2005

Name und Postanschrift der Internationalen Recherchenbehörde
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

Bevollmächtigter Bediensteter

Meződi, S

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 02/11081 A (ORGA KARTENSYSTEME GMBH; BORMANN, FRANK, C; FISCHER, DIRK; FIEDLER, AL) 7. Februar 2002 (2002-02-07) Seite 8, Zeile 21 - Seite 10, Zeile 3 -----	
A	WO 96/29699 A (MEILLER COMCARD GMBH; LENDER, FRIEDWART; HORSTER, PATRICK) 26. September 1996 (1996-09-26) Zusammenfassung -----	
A	US 6 357 005 B1 (DEVAUX FRANCOIS ET AL) 12. März 2002 (2002-03-12) Zusammenfassung -----	
A	EP 1 089 156 A (M-SYSTEMS FLASH DISK PIONEERS LTD) 4. April 2001 (2001-04-04) Absätze '0018!', '0019!', '0040! -----	
A	EP 0 818 748 A (MURAKOSHI, HIROMASA) 14. Januar 1998 (1998-01-14) Zusammenfassung -----	
A	TECHNICAL STANDARD: "System Management: Software License Use Management (XSLM)" SOFTWARE LICENSE USE MANAGEMENT (XSLM), März 1999 (1999-03), Seiten 25-29,175, XP002271896 Seite 175 - Seite 180 -----	

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2005/008996

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9938162	A	29-07-1999	AU GB	1781099 A 2338586 A	09-08-1999 22-12-1999
US 6542444	B1	01-04-2003	AU EP WO JP	3185800 A 1043684 A1 0058907 A1 2002540547 T	16-10-2000 11-10-2000 05-10-2000 26-11-2002
US 2002024905	A1	28-02-2002	AU CN WO JP	9549601 A 1447970 A 0217316 A1 2004507028 T	04-03-2002 08-10-2003 28-02-2002 04-03-2004
DE 4403206	A1	10-08-1995	KEINE		
WO 0211081	A	07-02-2002	AU	6223601 A	13-02-2002
WO 9629699	A	26-09-1996	AU	5110596 A	08-10-1996
US 6357005	B1	12-03-2002	AT CA DE DE DK EP ES FR WO GR JP	193384 T 2261629 A1 69702135 D1 69702135 T2 912920 T3 0912920 A1 2147016 T3 2751767 A1 9804966 A1 3034219 T3 2001502102 T	15-06-2000 05-02-1998 29-06-2000 09-11-2000 30-10-2000 06-05-1999 16-08-2000 30-01-1998 05-02-1998 29-12-2000 13-02-2001
EP 1089156	A	04-04-2001	AU IL JP TW WO US US	7712300 A 138661 A 2001160002 A 473664 B 0124054 A1 6324537 B1 6539380 B1	30-04-2001 17-05-2005 12-06-2001 21-01-2002 05-04-2001 27-11-2001 25-03-2003
EP 0818748	A	14-01-1998	AU AU CA CN HK JP JP US	717988 B2 2844497 A 2209596 A1 1180201 A 1010258 A1 2810033 B2 10083298 A 5943650 A	06-04-2000 15-01-1998 08-01-1998 29-04-1998 11-09-2003 15-10-1998 31-03-1998 24-08-1999