(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2006 037 493 A1** 2008.02.14

(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2006 037 493.2**
(22) Anmeldetag: **10.08.2006**
(43) Offenlegungstag: **14.02.2008**

(51) Int Cl.[8]: ***G06F 21/22*** (2006.01)
G06K 19/07 (2006.01)

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Spitz, Stephan, Dr., 81245 München, DE; Hinz, Walter, Dr., 85748 Garching, DE

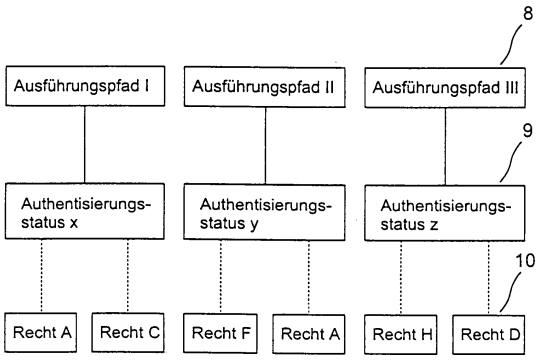
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:
FR 28 20 847 A1
US2005/00 05 079 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Rechercheantrag gemäß § 43 Abs. 1 Satz 1 PatG ist gestellt.

(54) Bezeichnung: **Tragbarer Datenträger**

(57) Zusammenfassung: Die Erfindung betrifft einen tragbaren Datenträger (1), der eine Prozessoreinheit (2) zur Ausführung von Programmcode und ein Betriebssystem zur quasi-parallelen Ausführung mehrerer Prozesse oder Ausführungspfade (8) mit Hilfe der Prozessoreinheit (2) aufweist. Das Betriebssystem weist einen Betriebssystem-Kern (12) auf, der den Zugriff auf Ressourcen (11) des tragbaren Datenträgers (1) steuert. Jedem Prozess oder Ausführungspfad (8) ist ein Authentisierungsstatus (9) zugeordnet, der auf einen Authentisierungsvorgang zurückgeht und an den während der Ausführung des Prozesses oder Ausführungspfads (8) verfügbare Berechtigungen (10) für den Zugriff auf die Ressourcen (11) geknüpft sind. Die zum jeweiligen Authentisierungsstatus (9) gehörigen Berechtigungen (10) werden vom Betriebssystem-Kern (12) verwaltet.



Beschreibung

[0001] Die Erfindung betrifft einen tragbaren Datenträger. Weiterhin betrifft die Erfindung ein Betriebssystem für einen tragbaren Datenträger und ein Verfahren zum Betreiben eines tragbaren Datenträgers.

[0002] Tragbare Datenträger, die insbesondere als Chipkarten ausgebildet sein können, werden beispielsweise im Bereich des Zahlungsverkehrs, im Mobilfunkbereich, als Ausweisdokumente, als sonstige Sicherheitsdatenträger usw. eingesetzt. Je nach Anwendungsfall können tragbare Datenträger sehr einfach ausgebildet sein und lediglich über einen Speicher verfügen oder als ein vergleichsweise komplexes System mit einem Mikroprozessor, der ein Betriebssystem aufweist. In vielen Fällen ist das Betriebssystem so ausgebildet, dass gleichzeitig nur ein einziger Prozess aktiv sein kann. Derartige Betriebssysteme werden als „single-threaded" bezeichnet. Darüber hinaus ist es auch bekannt, mehrere logische Kanäle vorzusehen, die eine quasi-parallele Ausführung mehrerer Prozesse ermöglichen. Insbesondere bei sicherheitsrelevanten Anwendungen besteht dabei das Problem, dass gewährleistet sein muss, dass es bei einer Ausführung der Prozesse nicht zu einer Überschreitung der jeweiligen Berechtigungen kommt.

[0003] Aus der EP 1 528 451 A1 ist ein Verfahren zur Erzwingung einer Benutzer-Validierung bei einer Smart Card bekannt, bei dem ein Applet für die Durchführung einer Benutzer-Authentisierung vorgesehen ist, welche zur Ausführung eines sicherheitsrelevanten Applets benötigt wird.

[0004] Aus der WO 2004/109754 A2 ist eine Multi-Modus-Architektur für einen Halbleiter-Schaltkreis bekannt, wobei der Zugang zu Ressourcen wie beispielsweise Speicher abhängig vom jeweiligen Modus begrenzt wird. Im Falle eines unberechtigten Zugriffsversuchs wird ein Interrupt generiert. Ebenso ist es auch möglich einen Interrupt zu generieren, falls es erforderlich ist, eine Ressource zu nutzen, die im derzeitigen Modus nicht verfügbar ist, insbesondere wenn in einem Benutzer-Modus auf eine Ressource eines Kernel-Modus zugegriffen werden soll.

[0005] Es ist Aufgabe der Erfindung, bei einem tragbaren Datenträger die quasi-parallele Ausführung von Prozessen oder Ausführungspfaden unter Beachtung der jeweiligen Berechtigung auf möglichst optimale Weise zu ermöglichen.

[0006] Diese Aufgabe wird durch einen tragbaren Datenträger gemäß Anspruch 1, ein Betriebssystem gemäß Anspruch 14 und ein Verfahren zum Betreiben eines tragbaren Datenträgers gemäß Anspruch 15 gelöst.

[0007] Der erfindungsgemäße tragbare Datenträger weist eine Prozessoreinheit zur Ausführung von Programmcode und ein Betriebssystem zur quasi-parallelen Ausführung mehrerer Prozesse oder Ausführungspfade mit Hilfe der Prozessoreinheit auf. Das Betriebssystem weist einen Betriebssystem-Kern auf, der den Zugriff auf Ressourcen des tragbaren Datenträgers steuert. Jedem Prozess oder Ausführungspfad ist ein Authentisierungsstatus zugeordnet, der auf einen Authentisierungsvorgang zurückgeht und an den während der Ausführung des Prozesses oder Ausführungspfads verfügbare Berechtigungen für den Zugriff auf die Ressourcen geknüpft sind. Die zum jeweiligen Authentisierungsstatus gehörigen Berechtigungen werden vom Betriebssystem-Kern verwaltet.

[0008] Die Erfindung hat den Vorteil, dass sie einen quasi-parallelen Betrieb des tragbaren Datenträgers ermöglicht und somit zu einer hohen Leistungsfähigkeit des tragbaren Datenträgers beiträgt. Dabei ist es besonders vorteilhaft, dass bei der quasi-parallelen Ausführung von Prozessen oder Ausführungspfaden unberechtigte Zugriffe zuverlässig unterbunden werden können. Da lediglich der Authentisierungsstatus geprüft werden muss, kann sehr schnell festgestellt werden, ob ein Zugriff auf eine Ressource zulässig ist.

[0009] Wenigstens einem der Prozesse oder Ausführungspfade kann nach erfolgreicher Durchführung einer Authentisierung ein Authentisierungsstatus zugeordnet werden. Dies bedeutet, dass ein hoher Sicherheitsstandard realisiert werden kann und verhindert werden kann, dass ein Authentisierungsstatus einem Prozess oder Ausführungspfad unberechtigter Weise zugeordnet wird.

[0010] Weiterhin kann der erfindungsgemäße tragbare Datenträger so ausgebildet sein, dass wenigstens einem der Prozesse oder Ausführungspfade der Authentisierungsstatus eines anderen Prozesses oder Ausführungspfads übertragen wird. Dies ermöglicht eine sehr flexible Handhabung des Authentisierungsstatus. Insbesondere kann bei der Erzeugung eines neuen Prozesses oder Ausführungspfads der Authentisierungsstatus des erzeugenden Prozesses oder Ausführungspfads übertragen werden. Somit weist der neue Prozess oder Ausführungspfad den gleichen Authentisierungsstatus wie der erzeugende Prozess oder Ausführungspfad auf. Eine nochmalige Durchführung der Authentisierung ist nicht erforderlich. Dies vereinfacht die Vorgehensweise und spart Zeit.

[0011] Vorzugsweise sind wenigstens einige der Prozesse oder Ausführungspfade verschiedenen Benutzern zugeordnet. Dies bedeutet, dass mehrere Benutzer gleichzeitig auf dem tragbaren Datenträger angemeldet sein können. Dabei können wenigstens

zeitweise Prozesse oder Ausführungspfade, die verschiedenen Benutzern zugeordnet sind, gleichzeitig aktiv sein.

[0012] Besonders vorteilhaft ist es, wenn wenigstens einem der Prozesse oder Ausführungspfade mehr als ein Authentisierungsstatus zugeordnet ist. Dies ermöglicht eine sehr flexible Vergabe von Berechtigungen.

[0013] Die Zuordnung zwischen einem Prozess oder Ausführungspfad und einem Authentisierungsstatus wird vorzugsweise vom Betriebssystem-Kern verwaltet. Dies trägt zur Erzielung eines hohen Sicherheitsstandards bei. Insbesondere kann vorgesehen sein, dass vor der Freigabe eines Zugriffs auf eine Ressource der Authentisierungsstatus des Prozesses oder Ausführungspfads geprüft wird. Die Freigabe des Zugriffs auf die Ressource kann dann erfolgen, wenn an den Authentisierungsstatus des Prozesses oder Ausführungspfads die für den Zugriff auf die Ressource benötigte Berechtigung geknüpft ist.

[0014] Der erfindungsgemäße tragbare Datenträger kann beispielsweise als ein Netz-Server betreibbar sein. Ebenso ist es auch möglich, dass der erfindungsgemäße tragbare Datenträger als ein Anwendungs-Server betreibbar ist. Vorzugsweise ist der erfindungsgemäße tragbare Datenträger als eine Chipkarte ausgebildet.

[0015] Die Erfindung bezieht sich weiterhin auf ein Betriebssystem eines tragbaren Datenträgers, der eine Prozessoreinheit zur Ausführung von Programmcode aufweist. Das erfindungsgemäße Betriebssystem ist für eine quasi-parallele Ausführung mehrerer Prozesse oder Ausführungspfade ausgelegt und weist einen Betriebssystem-Kern auf, der den Zugriff auf Ressourcen des tragbaren Datenträgers steuert. Jedem Prozess oder Ausführungspfad ist ein Authentisierungsstatus zugeordnet, der auf einen Authentisierungsvorgang zurückgeht und an den während der Ausführung des Prozesses oder Ausführungspfads verfügbare Berechtigungen für den Zugriff auf die Ressourcen geknüpft sind. Die zum jeweiligen Authentisierungsstatus gehörigen Berechtigungen werden vom Betriebssystem-Kern verwaltet.

[0016] Außerdem bezieht sich die Erfindung auf ein Verfahren zum Betreiben eines tragbaren Datenträgers, der eine Prozessoreinheit zur Ausführung von Programmcode aufweist. Beim erfindungsgemäßen Verfahren werden mehrere Prozesse oder Ausführungspfade von einem Betriebssystem des tragbaren Datenträgers quasi-parallel ausgeführt und der Zugriff auf Ressourcen des tragbaren Datenträgers von einem Betriebssystem-Kern gesteuert. Jedem Prozess oder Ausführungspfad wird ein Authentisierungsstatus zugeordnet, der auf einen Authentisierungsvorgang zurückgeht und an den während der Ausführung des Prozesses oder Ausführungspfads verfügbare Berechtigungen für den Zugriff auf die Ressourcen geknüpft sind. Die zum jeweiligen Authentisierungsstatus gehörigen Berechtigungen werden vom Betriebssystem-Kern verwaltet.

[0017] Die Erfindung wird nachstehend anhand der in der Zeichnung dargestellten Ausführungsbeispiele erläutert.

[0018] Es zeigen:

[0019] Fig. 1 ein stark vereinfachtes Blockschaltbild für ein Ausführungsbeispiel eines tragbaren Datenträgers,

[0020] Fig. 2 ein Ausführungsbeispiel für die erfindungsgemäße Realisierung einer Zugriffskontrolle,

[0021] Fig. 3 eine Prinzipdarstellung für eine mögliche Architektur des tragbaren Datenträgers und

[0022] Fig. 4 ein Flussdiagramm für eine mögliche Vorgehensweise bei der Auswertung des Authentisierungsstatus.

[0023] Fig. 1 zeigt ein stark vereinfachtes Blockschaltbild für ein Ausführungsbeispiel eines tragbaren Datenträgers **1**. Dabei ist als ein tragbarer Datenträger **1** im Sinn der Erfindung ein Rechnersystem anzusehen, bei dem die Ressourcen, d. h. Speicherressourcen und/oder Rechenkapazität (Rechenleistung) begrenzt sind, z. B. eine Chipkarte (Smart Card, Mikroprozessor-Chipkarte) oder ein Token oder ein Chipmodul zum Einbau in eine Chipkarte oder in ein Token. Der tragbare Datenträger **1** kann eine beliebige standardisierte oder nicht standardisierte Gestalt haben, beispielsweise die Gestalt einer flachen Chipkarte ohne Norm oder nach einer Norm wie z.B. ISO 7810 (z.B. ID-1, ID-00, ID-000) oder die eines volumigen Tokens.

[0024] Der tragbare Datenträger **1** weist eine Prozessoreinheit **2** auf, welche die Funktionsabläufe des tragbaren Datenträgers **1** steuert und auch als Central Processing Unit, abgekürzt CPU, bezeichnet wird. Weiterhin weist der tragbare Datenträger **1** eine Schnittstelle **3** zur Ein- und Ausgabe von Daten und einen Speicher **4** auf. Beim dargestellten Ausführungsbeispiel besteht der Speicher **4** aus einem Permanentspeicher **5**, einem nichtflüchtigen Speicher **6** und einem flüchtigen Speicher **7**. Alternativ dazu ist auch ein anderer Aufbau des Speichers **4** möglich. Die Prozessoreinheit **2** ist mit der Schnittstelle **3**, dem Permanentspeicher **5**, dem nichtflüchtigen Speicher **6** und dem flüchtigen Speicher **7** verbunden. Die Schnittstelle **3** dient der Kommunikation mit externen Geräten, die durch eine berührende Kontaktierung des tragbaren Datenträgers **1** und/oder kontaktlos abgewickelt werden kann.

[0025] Im Permanentspeicher **5** sind Daten abgelegt, die während der gesamten Lebensdauer des tragbaren Datenträgers **1** unverändert erhalten bleiben, beispielsweise Programme, Parameter, personenbezogene Angaben, Schlüssel usw. Insbesondere ist im Permanentspeicher **5** das Betriebssystem des tragbaren Datenträgers **1** gespeichert.

[0026] Der flüchtige Speicher **7** dient als Arbeitsspeicher für die Prozessoreinheit **2**, so dass geheime Daten beispielsweise bei der Durchführung von Berechnungen im flüchtigen Speicher **7** zwischengespeichert werden. Im flüchtigen Speicher **7** bleibt der Speicherinhalt nur solange erhalten, wie der tragbare Datenträger **1** mit einer Betriebsspannung versorgt wird.

[0027] Der nichtflüchtige Speicher **6** kann während der Lebensdauer des tragbaren Datenträgers **1** immer wieder neu beschrieben werden. Der jeweilige Speicherinhalt bleibt auch dann erhalten, wenn der tragbare Datenträger **1** nicht mit der Betriebsspannung versorgt wird. Im nichtflüchtigen Speicher **6** sind beispielsweise Ergänzungen zum Betriebssystem, Anwendungssoftware, Schlüssel, personenbezogene Daten usw. abgelegt.

[0028] Der in Fig. 1 dargestellte tragbare Datenträger **1** ist in der Lage, mehrere Aktionen quasi-parallel auszuführen. Dies kann im Rahmen eines Multitasking oder eines Multithreading erfolgen. Beim Multitasking sind mehrere Prozesse vorgesehen, die quasi-gleichzeitig ablaufen. Beim Multithreading wird nur ein einziger Prozess ausgeführt, der mehrere Ausführungspfade aufweist, welche quasi-parallel ausgeführt werden können. Die einzelnen Ausführungspfade werden auch als Threads bezeichnet. Auf die im folgenden beschriebene Weise wird jeweils sichergestellt, dass von den einzelnen Prozessen bzw. in den einzelnen Ausführungspfaden keine unberechtigten Zugriffe durchgeführt werden. Die folgenden Erläuterungen beziehen sich jeweils auf ein Multithreading-Betriebssystem, gelten jedoch in analoger Weise für ein Multitasking-Betriebssystem.

[0029] Fig. 2 zeigt ein Ausführungsbeispiel für die erfindungsgemäße Realisierung einer Zugriffskontrolle.

[0030] In Fig. 2 sind mehrere Ausführungspfade **8** dargestellt, die von der Prozessoreinheit **2** quasi-parallel ausgeführt werden können. Die folgenden Erläuterungen zu den Ausführungspfaden **8** gelten in analoger Weise für verschiedene Prozesse eines Multitasking-Betriebssystems.

[0031] Jedem Ausführungspfad **8** ist je ein Authentisierungsstatus **9** zugeordnet. Im einzelnen ist einem mit I bezeichneten Ausführungspfad **8** ein mit x bezeichneter Authentisierungsstatus **9**, einem mit II bezeichneten Ausführungspfad **8** ein mit y bezeichneter Authentisierungsstatus **9** und einem mit III bezeichneten Ausführungspfad **8** ein mit z bezeichneter Authentisierungsstatus **9** zugeordnet. Die Informationen, welchen Authentisierungsstatus **9** die Ausführungspfade **8** aufweisen, können beispielsweise in einem Steuerblock eines jeden Ausführungspfads **8** abgelegt sein.

[0032] Der Authentisierungsstatus **9** gibt jeweils an, über welche Berechtigungen **10** der Ausführungspfad **8** verfügt. Gemäß der Darstellung der Fig. 2 sind dem mit x bezeichneten Authentisierungsstatus **9** mit A und C bezeichnete Berechtigungen **10**, dem mit y bezeichneten Authentisierungsstatus **9** mit F und A bezeichnete Berechtigungen **10** und dem mit z bezeichneten Authentisierungsstatus **9** mit H und D bezeichnete Berechtigungen **10** zugeordnet. Konkrete Beispiele für einen Authentisierungsstatus **9** können sein:

– Betriebssystemmanager mit der Berechtigung **10**, Treiber im Betriebssystem des tragbaren Datenträgers **1** zu laden.
– Security Domain Manager mit der Berechtigung **10**, Rechte für das Laden von Applikationen zu vergeben.
– Load Manager mit der Berechtigung **10**, Applikationen zu laden.
– Standard-Benutzer mit der Berechtigung **10**, auf benutzerbezogene Daten zuzugreifen, wie beispielsweise auf ein Telefonbuch bei einem tragbaren Datenträger **1**, der als ein Sicherheitsmodul für ein Mobilfunktelefon ausgebildet ist oder auf Informationen über eine Person bei einem tragbaren Datenträger **1**, der als ein Ausweisdokument ausgebildet ist.

[0033] Ein Authentisierungsstatus **9** kann dadurch erlangt werden, dass eine Authentisierung durchgeführt wird. Hierzu kann beispielsweise eine persönliche Identifikationsnummer (PIN) von einem Benutzer eingegeben werden oder es kann eine Authentisierung mittels eines biometrischen Merkmals erfolgen. Ebenso ist es auch möglich, für die Authentisierung einen kryptographischen Schlüssel heranzuziehen. Der so erzeugte Authentisierungsstatus **9** bleibt erhalten und kann insbesondere auch an andere Ausführungspfade **8** weitergegeben werden. Insbesondere können bei einer Anwendung, die sich auf mehrere Ausführungspfade **8** verteilt, alle Prozesse den Authentisierungsstatus **9** des Ausführungspfads **8** aufweisen, mit dem die Anwendung gestartet wurde.

[0034] Die Information über den Authentisierungsstatus **9** wird ausgewertet, wenn ein Ausführungspfad **8** versucht, eine Aktion durchzuführen, für die eine Berechtigung **10** benötigt wird. Eine derartige Aktion kann eine logische Operation, wie beispielsweise eine Verwendung eines kryptographischen Schlüssels, eine Installation einer Applikation oder ei-

nes Treibers oder einen Zugriff auf eine Datei, beinhalten. Ebenso kann die Aktion einen Zugriff auf Betriebsmittel, wie beispielsweise den Speicher **4**, einer Kryptographie-Einrichtung, Schnittstellen **3** usw. beinhalten.

[0035] Die Auswertung der Information über den Authentisierungsstatus **9** kann mittels eines Interpreters, beispielsweise einer Java Virtual Machine oder in einer nativen Laufzeitumgebung, beispielsweise einem Betriebssystem-Kern, durchgeführt werden. Die diesbezügliche Vorgehensweise wird anhand der Fig. 3 und Fig. 4 erläutert.

[0036] Fig. 3 zeigt eine Prinzipdarstellung für eine mögliche Architektur des tragbaren Datenträgers **1**. Die als eine zentrale Scheibe dargestellte Prozessoreinheit **2** ist von einer Reihe von Ressourcen **11** umgeben, die als Ringsegmente dargestellt sind, welche in Umfangsrichtung nebeneinander angeordnet sind und insgesamt die Prozessoreinheit **2** umschließen. Bei den Ressourcen **11** kann es sich beispielsweise um verschiedene Speicherarten, um I/O- und Interrupt-Prozesse, um eine Kryptographieeinheit usw. handeln. Die Ressourcen **11** sind radial nach außen durch einen Ring, der einen Betriebssystem-Kern (Operating System Kernel) **12** darstellt, vollständig umschlossen. Radial außerhalb des Betriebssystem-Kerns **12** sind Ringsegmente in Umfangsrichtung nebeneinander angeordnet, die Ausführungspfade **8** darstellen, bei denen ein Zugriff auf eine oder mehrere der Ressourcen **11** erforderlich ist. Ein solcher Zugriff ist durch einen Pfeil dargestellt, der sich von einem Ausführungspfad **8** bis zu einer Ressource **11** erstreckt. Jeder Ausführungspfad **8** kann einem anderen Benutzer des tragbaren Datenträgers **1** zugeordnet sein.

[0037] Wie aus Fig. 3 unmittelbar hervorgeht, sind die Ausführungspfade **8** durch den Betriebssystem-Kern **12** von den Ressourcen **11** getrennt. Dies bedeutet, dass den Ausführungspfaden **8** jeweils nur dann ein Zugriff auf die Ressourcen **11** möglich ist, wenn der Zugriff vom Betriebssystem-Kern **12** nach Auswertung des Authentisierungsstatus **9** freigegeben wird. Die diesbezügliche Vorgehensweise wird anhand von Fig. 4 erläutert.

[0038] Fig. 4 zeigt ein Flussdiagramm für eine mögliche Vorgehensweise bei der Auswertung des Authentisierungsstatus **9**.

[0039] Der Durchlauf des Flussdiagramms beginnt mit einem Schritt S1, bei dem der Ausführungspfad **8** versucht, eine Aktion durchzuführen, für die eine Berechtigung **10** benötigt wird. An Schritt S1 schließt sich ein Schritt S2 an, bei dem vom Betriebssystem-Kern **12** ermittelt wird, welcher Authentisierungsstatus **9** für die Durchführung der Aktion benötigt wird. Danach wird in einem Schritt S3 abgefragt, ob der Ausführungspfad **8** über den in Schritt S2 ermittelten Authentisierungsstatus **9** verfügt. Falls die Abfrage zu einem positiven Ergebnis führt, d. h. falls der Ausführungspfad **8** über den erforderlichen Authentisierungsstatus **9** verfügt, wird im Anschluss an Schritt S3 ein Schritt S4 ausgeführt. Im Schritt S4 wird die gewünschte Aktion durchgeführt. Mit der Ausführung des Schritts S4 ist der Durchlauf des Flussdiagramms beendet.

[0040] Falls die Abfrage des Schritts S3 zu einem negativen Ergebnis führt, d. h. falls der Ausführungspfad **8** nicht über den erforderlichen Authentisierungsstatus **9** verfügt, wird im Anschluss an Schritt S3 ein Schritt S5 ausgeführt. Im Schritt S5 wird eine Verzeigung in eine Fehlerbehandlung (Exeption Handling) der Laufzeitumgebung oder virtuellen Maschine durchgeführt. Mit Schritt S5 ist der Durchlauf des Flussdiagramms beendet.

[0041] Die vorstehend beschriebene Vorgehensweise kann beispielsweise bei einem internetfähigen tragbaren Datenträger **1** angewendet werden, in dem ein Netz-Server (Web Server) implementiert ist. Verschiedene Clients können zum Beispiel über das HTTP-Protokoll Anfragen an den Netz-Server senden. Dabei können sich einzelne Clients mit Hilfe des SSL/TLS-Protokolls beim Netz-Server authentisieren (SSL-Client-Authentisierung). Durch die Authentisierung erlangen die den Clients zugeordneten Prozesse bzw. Ausführungspfade **8** des Netz-Servers jeweils einen Authentisierungsstatus **9**. Vom Authentisierungsstatus **9** hängt es ab, auf welche Daten ein Zugriff erfolgen kann. Dies bedeutet, dass jeder Client nur Zugriff auf die Daten hat, für die er gemäß dem erlangten Authentisierungsstatus **9** über eine Berechtigung **10** verfügt. Somit können mehrere Clients auf einen Netz-Server zugreifen, der auf einem einzigen tragbaren Datenträger **1** implementiert ist ohne Gefahr zu laufen, dass unberechtigte Datenzugriffe erfolgen, d. h. dass beispielsweise ein Client auf die Daten eines anderen Clients zugreift.

[0042] Weiterhin kann die Erfindung auch für den Betrieb eines Applikations-Servers genutzt werden. Anders als bei einem Netz-Server kann bei einem Applikation-Server ein Client auch die Ausführung von Programmen starten. Dies kann beispielsweise über eine CGI-Schnittstelle (Common Gateway Interface) erfolgen. Die von einem Client gestarteten Ausführungspfade **8** eines Programms verfügen jeweils über einen bestimmten Authentisierungsstatus **9**. Vom jeweiligen Authentisierungsstatus **9** hängt es ab, welche Aktionen die einzelnen Ausführungspfade **8** im Betriebssystem oder in der Laufzeitumgebung ausführen dürfen.

[0043] Ein Applikation-Server kann auch so eingesetzt werden, dass von den Clients keine Programme gestartet, sondern Prozeduren oder Funktionen auf-

gerufen werden. Der Aufruf der Prozeduren erfolgt mittels RPCs (Remote Procedure Calls). Beispielsweise können Netz-Dienste (Web Services) aufgerufen werden. Die Berechtigung **10** zum Aufruf der Prozeduren oder Funktionen kann wiederum über einen Authentisierungsstatus **9** erlangt werden, der dem Client aufgrund seiner Authentisierung zugewiesen wird. Beispielsweise kann eine in XML definierte Struktur für digitale Signaturen oder verschlüsselte Inhalte für die Erlangung eines Authentisierungsstatus **9** verwendet werden, der zum Aufrufen von Netz-Diensten berechtigt.

Patentansprüche

1. Tragbarer Datenträger, mit
– einer Prozessoreinheit (**2**) zur Ausführung von Programmcode,
– einem Betriebssystem zur quasi-parallelen Ausführung mehrerer Prozesse oder Ausführungspfade (**8**) mit Hilfe der Prozessoreinheit (**2**), wobei
– das Betriebssystem einen Betriebssystem-Kern (**12**) aufweist, der den Zugriff auf Ressourcen (**11**) des tragbaren Datenträgers (**1**) steuert,
– jedem Prozess oder Ausführungspfad (**8**) ein Authentisierungsstatus (**9**) zugeordnet ist, der auf einen Authentisierungsvorgang zurückgeht und an den während der Ausführung des Prozesses oder Ausführungspfads (**8**) verfügbare Berechtigungen (**10**) für den Zugriff auf die Ressourcen (**11**) geknüpft sind und
– die zum jeweiligen Authentisierungsstatus (**9**) gehörigen Berechtigungen (**10**) vom Betriebssystem-Kern (**12**) verwaltet werden.

2. Tragbarer Datenträger nach Anspruch 1, dadurch gekennzeichnet, dass wenigstens einem der Prozesse oder Ausführungspfade (**8**) nach erfolgreicher Durchführung einer Authentisierung ein Authentisierungsstatus (**9**) zugeordnet wird.

3. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass wenigstens einem der Prozesse oder Ausführungspfade (**8**) der Authentisierungsstatus (**9**) eines anderen Prozesses oder Ausführungspfads (**8**) übertragen wird.

4. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass bei der Erzeugung eines neuen Prozesses oder Ausführungspfads (**8**) der Authentisierungsstatus (**9**) des erzeugenden Prozesses oder Ausführungspfads (**8**) übertragen wird.

5. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass wenigstens einige der Prozesse oder Ausführungspfade (**8**) verschiedenen Benutzern zugeordnet sind.

6. Tragbarer Datenträger nach Anspruch 5, dadurch gekennzeichnet, dass wenigstens zeitweise Prozesse oder Ausführungspfade (**8**), die verschiedenen Benutzern zugeordnet sind, gleichzeitig aktiv sind.

7. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass wenigstens einem der Prozesse oder Ausführungspfade (**8**) mehr als ein Authentisierungsstatus (**9**) zugeordnet ist.

8. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Zuordnung zwischen einem Prozess oder Ausführungspfad (**8**) und einem Authentisierungsstatus (**9**) vom Betriebssystem-Kern (**12**) verwaltet wird.

9. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass vor der Freigabe eines Zugriffs auf eine Ressource (**11**) der Authentisierungsstatus (**9**) des Prozesses oder Ausführungspfads (**8**) geprüft wird.

10. Tragbarer Datenträger nach Anspruch 9, dadurch gekennzeichnet, dass der Zugriffs auf die Ressource (**11**) freigegeben wird, wenn an den Authentisierungsstatus (**9**) des Prozesses oder Ausführungspfads (**8**) die für den Zugriff auf die Ressource (**11**) benötigte Berechtigung (**10**) geknüpft ist.

11. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der tragbare Datenträger (**1**) als ein Netz-Server betreibbar ist.

12. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der tragbare Datenträger (**1**) als ein Anwendungs-Server betreibbar ist.

13. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der tragbare Datenträger (**1**) als eine Chipkarte ausgebildet ist.

14. Betriebssystem eines tragbaren Datenträgers (**1**), der eine Prozessoreinheit (**2**) zur Ausführung von Programmcode aufweist, wobei
– das Betriebssystem für eine quasi-parallele Ausführung mehrerer Prozesse oder Ausführungspfade (**8**) ausgelegt ist,
– das Betriebssystem einen Betriebssystem-Kern (**12**) aufweist, der den Zugriff auf Ressourcen (**11**) des tragbaren Datenträgers (**1**) steuert,
– jedem Prozess oder Ausführungspfad (**8**) ein Authentisierungsstatus (**9**) zugeordnet ist, der auf einen Authentisierungsvorgang zurückgeht und an den während der Ausführung des Prozesses oder Ausführungspfads (**8**) verfügbare Berechtigungen (**10**)

für den Zugriff auf die Ressourcen (**11**) geknüpft sind und
– die zum jeweiligen Authentisierungsstatus (**9**) gehörigen Berechtigungen (**10**) vom Betriebssystem-Kern (**12**) verwaltet werden.

15. Verfahren zum Betreiben eines tragbaren Datenträgers (**1**), der eine Prozessoreinheit (**2**) zur Ausführung von Programmcode aufweist, wobei
– mehrere Prozesse oder Ausführungspfade (**8**) von einem Betriebssystem des tragbaren Datenträgers (**1**) quasi-parallel ausgeführt werden,
– der Zugriff auf Ressourcen (**11**) des tragbaren Datenträgers (**1**) von einen Betriebssystem-Kern (**12**) gesteuert wird,
– jedem Prozess oder Ausführungspfad (**8**) ein Authentisierungsstatus (**9**) zugeordnet wird, der auf einen Authentisierungsvorgang zurückgeht und an den während der Ausführung des Prozesses oder Ausführungspfads (**8**) verfügbare Berechtigungen (**10**) für den Zugriff auf die Ressourcen (**11**) geknüpft sind und
– die zum jeweiligen Authentisierungsstatus (**9**) gehörigen Berechtigungen (**10**) vom Betriebssystem-Kern (**12**) verwaltet werden.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

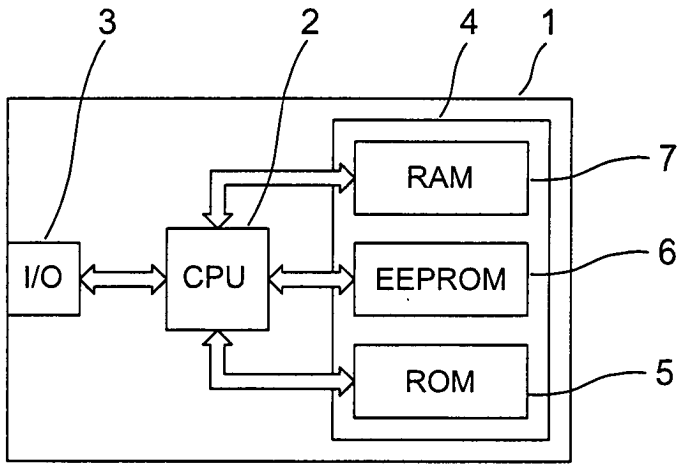


Fig. 1

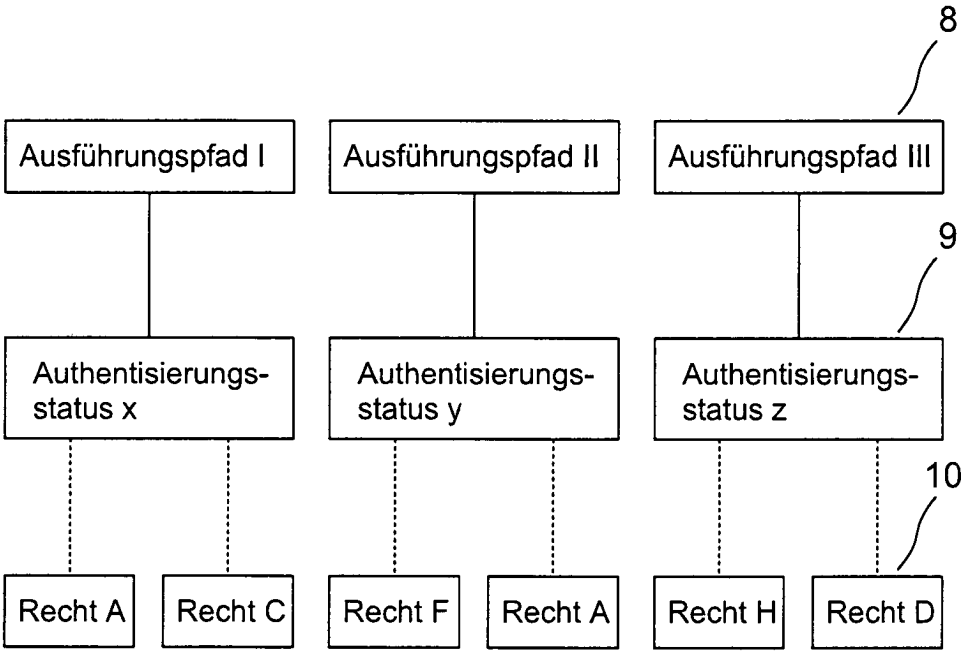


Fig. 2

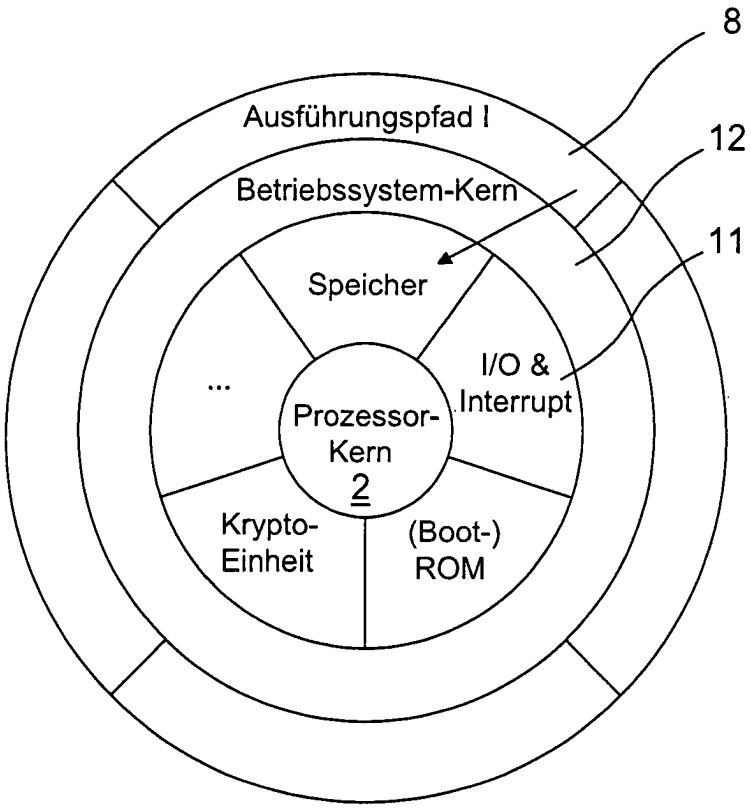

8
Ausführungspfad I
12
Betriebssystem-Kern
11
Speicher
I/O &
Interrupt
...
Prozessor-
Kern
2
Krypto-
Einheit
(Boot-)
ROM

Fig. 3

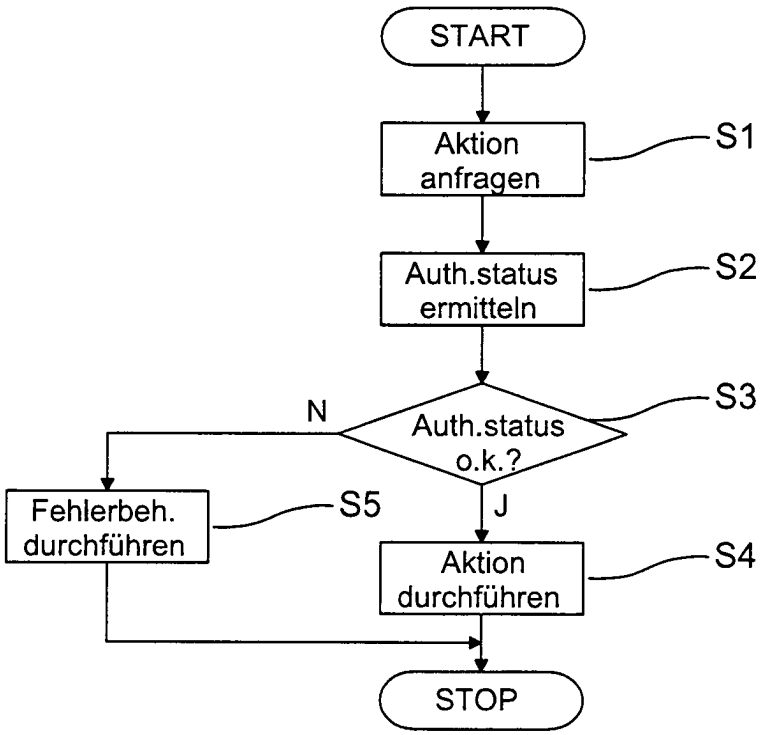

START
Aktion
anfragen
S1
Auth.status
ermitteln
S2
N
Auth.status
o.k.?
S3
Fehlerbeh.
durchführen
S5
J
Aktion
durchführen
S4
STOP

Fig. 4