(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
15. April 2010 (15.04.2010)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2010/040423 A1

(51) Internationale Patentklassifikation:
G06F 21/24 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2009/004336

(22) Internationales Anmeldedatum:
16. Juni 2009 (16.06.2009)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2008 028 703.2
9. Oktober 2008 (09.10.2008) 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)*: **GROBBEL, Hubertus** [DE/DE]; Caroline-Herschel-Straße 23, 81829 München (DE). **GUTER, Fabian** [DE/DE]; Oberndorfer Straße 23, 85622 Feldkirchen (DE).

(74) Anwalt: **KSNH Patentanwälte**; Klunker.Schmitt-Nilson.Hirsch, Destouchesstrasse 68, 80796 München (DE).

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

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

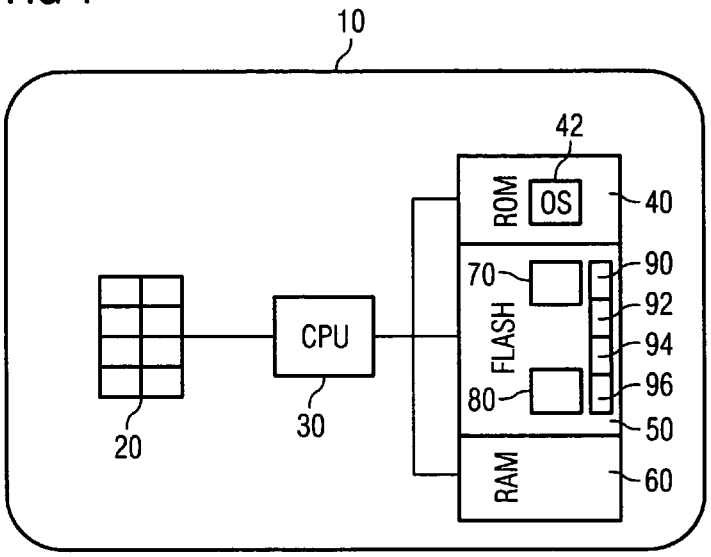
— *hinsichtlich der Berechtigung des Anmelders, die Priorität einer früheren Anmeldung zu beanspruchen (Regel 4.17 Ziffer iii)*

[Fortsetzung auf der nächsten Seite]

(54) **Title**: PERFORMING CRYPTOGRAPHIC OPERATIONS

(54) **Bezeichnung** : AUSFÜHREN KRYPTOGRAPHISCHER OPERATIONEN

FIG 1



(57) **Abstract**: The invention relates to a method for administering data on a portable medium (10) on which a file system (70) is set up, said method comprising the step of a user of the medium (10) accessing a directory of the file system (70). The directory (110, 120, 130, 140, 150, 160, 170) is thereby associated with at least one cryptographic operation, so that accessing the directory (110, 120, 130, 140, 150, 160, 170) initiates an execution of the cryptographic operation associated with the directory (110, 120, 130, 140, 150, 160, 170). The user can thereby be requested to be authenticated for the medium (10) upon accessing a directory (120, 130, 140, 150, 160, 170), which initiates data decoding or data signing by means of a cryptographic signature.

(57) **Zusammenfassung**: Ein Verfahren zum Verwalten von Daten auf einem portablen Datenträger (10), auf dem ein Dateisystem (70) eingerichtet ist, umfasst den Schritt des Zugreifens auf ein Verzeichnis des Dateisystems (70) durch einen Nutzer des Datenträgers (10). Dabei ist dem Verzeichnis (110, 120, 130, 140, 150, 160, 170) zumindest eine kryptographische Operation zugeordnet, so dass beim Zugreifen auf das Verzeichnis (110, 120, 130, 140, 150, 160, 170) eine Ausführung der dem Verzeichnis

[Fortsetzung auf der nächsten Seite]

WO 2010/040423 A1

— *Erfindererklärung (Regel 4.17 Ziffer iv)*

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(110, 120, 130, 140, 150, 160, 170) zugeordneten kryptographischen Operation ausgelöst wird. Hierbei kann der Nutzer bei einem Zugriff auf ein Verzeichnis (120, 130, 150, 160, 170), welches ein Entschlüsseln von Daten oder ein Signieren von Daten mittels einer kryptographischen Signatur auslöst, zur Authentisierung gegenüber dem Datenträger (10) aufgefordert werden.

Ausführen kryptographischer Operationen

Die vorliegende Erfindung betrifft die Ausführung kryptographischer Operationen auf einem portablen Datenträger, einen entsprechend eingerichteten Datenträger sowie die Einrichtung eines solchen Datenträgers.

Auf portablen Datenträgern, wie z.B. Chipkarten, Massenspeicherkarten, USB-Sticks und dergleichen, können z.B. Bild-, Audio-, oder Videodaten gespeichert werden, die auf verschiedenen Geräten betrachtet bzw. abgespielt werden können, aber auch persönliche geheime Daten, die zum Zugang zu verschiedenen Systemen berechtigen. Um solche sensiblen Daten vor unberechtigtem Zugriff, beispielsweise bei Verlust oder Diebstahl des Datenträgers, zu schützen, werden die Daten bevorzugt kryptographisch gesichert.

Die Verwendung derartiger Sicherheitsfunktionen, insbesondere kryptographischer Operationen, im Umgang mit persönlichen Daten wird dadurch erschwert, dass die Anwendung solcher Operationen meist eine zum Teil aufwendige Installation einer entsprechenden kryptographischen Software auf den jeweils genutzten Systemen erfordert. Des Weiteren wird die Portabilität kryptographisch gesicherter Daten dadurch erschwert, dass auf verschiedenen Systemen verschiedene Versionen bzw. auf manchen Systemen überhaupt keine entsprechende kryptographische Software installiert ist. Schließlich erfordert eine Nutzung von portablen Datenträgern, z.B. Chipkarten, zum sicheren Speichern persönlicher Daten in der Regel die Installation einer entsprechenden Middleware sowie das Vorhandensein angepasster Lesegeräte.

Aus der EP 1 722 336 A2 ist ein portabler Datenträger bekannt, der über eine USB-Schnittstelle Rohdaten empfängt und automatisch aus den Rohdaten mit Hilfe in dem Datenträger gespeicherter Geheimdaten Initialisierungsdaten zur Initialisierung von Sicherheitsdatenträgern erzeugt. Die Handhabung beliebiger Daten zum persönlichen Gebrauch wird in der EP 1 722 336 A2 nicht angesprochen.

Die WO 02/19582 A2 beschreibt, wie Daten in einem UNIX-System betriebssystemgesteuert beim Schreiben auf ein Speichermedium automatisch verschlüsselt bzw. beim Lesen von dem Speichermedium automatisch entschlüsselt werden. Zur Verschlüsselung und Entschlüsselung benötigte Schlüssel sind fest an das entsprechende System gebunden, wodurch z.B. eine Portierung gespeicherter verschlüsselter Daten zur Entschlüsselung an einem anderen System verhindert wird.

Aus der US 2008/0022132 A1 ist eine Speichereinrichtung bekannt, die unter anderem die Gestalt eine Chipkarte haben kann, mit einem hierarchisch strukturierten Speicher, wobei für bestimmte Hierarchieebenen definiert ist, daß Daten, die auf diesen Ebenen gehandhabt werden, automatisch ver- bzw. entschlüsselt werden. Die bekannte Lösung liefert eine konfigurierbar abgesicherte Speichereinrichtung. Soll sie variabel genutzt werden, setzt das aber eine zumindest hinreichend gute Kenntnis des Systems voraus, weshalb die bekannte Lösung letztlich nicht wirklich benutzerfreundlich ist.

Aus der EP 1 990 751 A1 ist eine treiberlos installierbare USB-Signier- und Verschlüsselungseinheit mit zwei Speichern bekannt, wovon auf einen nur schreibend und auf den anderen nur lesend zugegriffen werden kann. Bei einem Zugriff auf den ersten Speicher wird automatisch eine Signatur der Daten auslöst. Die signierten Daten werden anschließend jeweils in den

zweiten Speicher übertragen, von wo aus sie anschließend genutzt werden können. Dabei meldet sich jeweils zunächst der zweite Speicher gegenüber einem Host als „entfernt", nach Übertragen von signierten bzw. verschlüsselten Daten der erste Speicher. Bei Zugriff auf die Daten im zweiten Speicher verlangt die Einheit eine Authentisierung des Nutzers, z.B. durch Präsentation einer PIN.

Es ist Aufgabe der vorliegenden Erfindung, ein Verfahren zur sicheren und einfachen, nutzerfreundlichen Handhabung von Daten auf einem portablen Datenträger sowie einen entsprechenden Datenträger vorzuschlagen.

Diese Aufgabe wird durch ein Verfahren auf einem portablen Datenträger, einen portablen Datenträger und ein Verfahren zum Einrichten eines portablen Datenträgers mit den Merkmalen der unabhängigen Ansprüche gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen sind in den abhängigen Ansprüchen angegeben.

Die vorliegende Erfindung basiert auf dem Grundgedanken, einen Zugriff auf ein Verzeichnis in einem Dateisystem mit dem Ausführen einer kryptographischen Operation zu verknüpfen.

Demnach umfasst das erfindungsgemäße Verfahren auf einem portablen Datenträger, auf dem ein Dateisystem eingerichtet ist, den Schritt des Zugreifens auf ein Verzeichnis des Dateisystems durch einen Nutzer des Datenträgers. Dabei ist dem Verzeichnis zumindest eine kryptographische Operation zugeordnet und beim Zugreifen auf das Verzeichnis wird eine Ausführung der dem Verzeichnis zugeordneten kryptographischen Operation ausgelöst. Ein derartiges Verzeichnis wird im Rahmen der vorliegenden Erfindung nachstehend auch als Kryptographieoperationsverzeichnis bezeichnet.

Dementsprechend umfasst ein erfindungsgemäßer Datenträger zumindest einen Speicher mit einem darin eingerichteten Dateisystem, einen Prozessor und eine Steuereinrichtung. In dem Dateisystem ist zumindest ein erfindungsgemäßes Kryptographieoperationsverzeichnis angelegt, dem zumindest eine kryptographische Operation zugeordnet ist. Bei einem Zugriff auf das Kryptographieoperationsverzeichnis durch einen Nutzer des Datenträgers löst die Steuereinrichtung eine Ausführung der zumindest einen dem Kryptographieoperationsverzeichnis zugeordneten kryptographischen Operation aus.

Entsprechend wird in einem Dateisystem eines derartigen portablen Datenträgers zumindest ein Kryptographieoperationsverzeichnis angelegt. Dem zumindest einen Kryptographieoperationsverzeichnis wird dann zumindest eine kryptographische Operation derart zugeordnet, dass ein Zugriff eines Nutzers des Datenträgers auf das Kryptographieoperationsverzeichnis eine Ausführung der zumindest einen zugeordneten kryptographischen Operation auslöst. Dieses Verfahren zum erfindungsgemäßen Einrichten des Datenträgers wird vorzugsweise im Rahmen der Herstellung oder datentechnischen Ausgestaltung des Datenträgers durch einen Hersteller oder Herausgeber des Datenträgers durchgeführt werden.

Ein Nutzer des erfindungsgemäßen Datenträgers kann mittels des erfindungsgemäßen Verfahrens auf dem Datenträger auf einfache und sichere Weise sensible persönliche oder sonstige Daten verwalten und sichern. Eine komplizierte Installation oder Wartung einer kryptographischen Software kann entfallen. Weiterhin ist die Portabilität auf dem Datenträger gespeicherter Daten sichergestellt. Bereits durch den Zugriff auf in dem Dateisystem des Datenträgers angelegte Kryptographieoperationsverzeichnisse kann der

Nutzer auf einfache und für ihn transparente Weise Daten z.B. durch einfaches Ablegen in ein entsprechendes Verzeichnis kryptographisch sichern bzw. durch Auslesen aus dem Verzeichnis kryptographisch gesicherte Daten zurückgewinnen. Die erfindungsgemäße Verknüpfung eines Verzeichnisses mit einer kryptographischen Operation ermöglicht es dem Nutzer des Datenträgers also, die kryptographische Operation intuitiv und im Rahmen seiner üblichen Arbeit mit dem Datenträger einzusetzen. Auch wird ihm die persönliche Sicherstellung eines kryptographischen Schutzes sensibler Daten abgenommen, da alle in einem Kryptographieoperationsverzeichnis abgelegten Daten automatisch, d.h. ohne weitere Operationsaufrufe durch den Nutzer, entsprechend der jeweils zugeordneten kryptographischen Operation bearbeitet werden.

Schließlich lässt sich der Datenträger bei der Herstellung gemäß dem erfindungsgemäßen Verfahren zum Einrichten des portablen Datenträgers einfach und auf flexible Weise einrichten. Je nach gewünschter Anwendung können ein oder mehrere Kryptographieoperationsverzeichnisse in dem Dateisystem des Datenträgers angelegt werden. Es ist weiterhin möglich, jedem der angelegten Kryptographieoperationsverzeichnisse ein oder mehrere kryptographische Operationen in der vorstehend beschriebenen Weise zuzuordnen. Auch ist es möglich, dass Kryptographieoperationsverzeichnisse erst durch den Nutzer des Datenträgers eingerichtet werden, z.B. durch eine automatisierte Installation einer auf dem Datenträger vorinstallierten Krypto-Software.

Die beiden erfindungsgemäßen Verfahren und der erfindungsgemäße Datenträger stellen somit alle Mittel zur Verfügung, um eine einfache und sichere Handhabung von Daten auf einem portablen Datenträger zu ermöglichen.

Unter Zuordnung einer kryptographischen Operation zu einem Kryptographieoperationsverzeichnis ist im Rahmen der vorliegenden Erfindung eine Verknüpfung zu verstehen, die bewirkt, dass die Operation automatisch, d.h. ohne weitere Aktivierung durch den Nutzer, ausgeführt wird, wenn auf das entsprechende Verzeichnis zugegriffen wird, d.h. wenn Daten in dem Verzeichnis abgelegt werden oder daraus entnommen werden oder in dem Verzeichnis geöffnet und/oder angezeigt werden. Vorzugsweise wird die kryptographische Operation unmittelbar mit dem Zugriff ausgelöst, also vor dem eigentlichen Zugriff auf die entsprechenden Daten.

Als kryptographische Operationen, derer Ausführung bei einem Zugriff auf ein entsprechendes Kryptographieoperationsverzeichnis ausgelöst wird, werden dem Kryptographieoperationsverzeichnis vorzugsweise solche kryptographischen Operationen zugeordnet, die z.B. einem Verschlüsseln von Daten oder einem Entschlüsseln verschlüsselter Daten oder einem Signieren von Daten mittels einer kryptographischen Signatur oder einem Verifizieren einer kryptographischen Signatur entsprechen. Es ist möglich, einem Kryptographieoperationsverzeichnis mehr als eine kryptographische Operation zuzuordnen, z.B. das Verschlüsseln und das Signieren verschlüsselter Daten oder das Entschlüsseln und das Verifizieren signierter Daten. Auf diese Weise können sämtliche gebräuchlichen kryptographischen Operationen oder Kombinationen daraus allein durch den Zugriff auf entsprechend eingerichtete Kryptographieoperationsverzeichnisse ausgeführt werden.

Zusätzliche Daten, die eventuell zum Ausführen der kryptographischen Operationen benötigt werden, wie beispielsweise Empfängerlisten beim Verschlüsseln von Daten, können dem Datenträger als Parameterdaten übergeben werden. Solche Parameterdaten können z.B. als Dateiparameter der zu behandelten Datei oder als temporäre Konfigurationsdatei vorliegen, welche

dann von der entsprechenden kryptographischen Operation verarbeitet werden können.

Weiterhin kann eine einem Kryptographieoperationsverzeichnis zugeordnete kryptographische Operation ausschließlich bei einem lesenden Zugriff des Nutzers auf das Kryptographieoperationsverzeichnis ausgelöst wird, nicht aber bei einem schreibenden Zugriff. Umgekehrt kann eine kryptographische Operation einem Kryptographieoperationsverzeichnis derart zugeordnet sein, dass ausschließlich ein schreibender Zugriff auf das Verzeichnis ein Ausführen der Operation auslöst, nicht aber ein lesender Zugriff. Damit lässt sich beispielsweise erreichen, dass Daten automatisch beim Ablegen in ein Verzeichnis – d.h. bei einem schreibenden Zugriff – verschlüsselt werden, beim Auslesen aus dem Verzeichnis – d.h. bei einem lesenden Zugriff – jedoch nicht erneut verschlüsselt, sondern in der einfach verschlüsselten Form zurückgegeben werden. Schließlich ist es z.B. auch möglich, einem Kryptographieoperationsverzeichnis als kryptographische Operationen das Entschlüsseln und das Verschlüsseln von Daten in der Weise zuzuordnen, dass die Daten bei einem schreibenden Zugriff auf das Verzeichnis automatisch verschlüsselt und bei einem lesenden Zugriff auf das Verzeichnis automatisch entschlüsselt werden. Die komplementären Zugriffsarten des Schreibens und Lesens werden also mit entsprechenden komplementären kryptographischen Operationen verknüpft, z.B. Verschlüsseln und Entschlüsseln oder Signieren und Verifizieren.

Vorzugsweise wird der Nutzer des Datenträgers beim Zugreifen auf ein Kryptographieoperationsverzeichnis, das mit einem Entschlüsseln verschlüsselter Daten oder einem Signieren von Daten mittels einer kryptographischen Signatur verknüpft ist, aufgefordert, sich gegenüber dem Datenträger zu authentisieren. Das heißt, einem entsprechenden Kryptographieoperationsver-

zeichnis werden die kryptographischen Operationen des Entschlüsselns oder des Signierens derart zugeordnet, dass der Nutzer beim Zugriff auf das Verzeichnis automatisch zur Authentisierung gegenüber dem Datenträger aufgefordert wird. Eine solche Aufforderung kann seitens des Datenträgers durch die Steuereinrichtung erfolgen. Auf diese Weise kann beispielsweise sichergestellt werden, dass bei Verlust oder Diebstahl des Datenträgers verschlüsselt auf dem Datenträger gespeicherte Daten nicht von nicht autorisierter Seite entschlüsselt werden können. Es ist aber auch möglich, beim Auslösen weiterer oder anderer kryptographischer Operationen den Nutzer zu einer Authentisierung aufzufordern, beispielsweise um generell einen Zugriff auf ein Kryptographieoperationsverzeichnis zu ermöglichen. Vorzugsweise ist aber die automatische Authentisierungsaufforderung nur bei solchen kryptographischen Operationen notwendig, deren Ausführung einen geheimen kryptographischen Schlüssel erfordert, z.B. also das Entschlüsseln und das Signieren durch ein asymmetrisches Kryptographieverfahren.

Eine Authentisierung des Nutzers kann dabei beispielsweise durch direkte Eingabe eines zum Entschlüsseln oder Signieren benötigten kryptographischen Schlüssels erfolgen. Ebenso kann die Authentisierung durch Eingabe einer beliebigen geheimen Information erfolgen, z. B. einer PIN, oder durch Eingabe einer sonstigen Authentifikationsinformation, z.B. durch die Bereitstellung eines biometrischen Merkmals des Nutzers, wie beispielsweise eines Fingerabdrucks.

Eine einem Kryptographieoperationsverzeichnis zugeordnete Operation wird nach dem Auslösen eines Ausführens durch die Steuereinrichtung vorzugsweise auf einem Prozessor des Datenträgers ausgeführt, d.h. eine kryptographische Applikation, die die dem Kryptographieoperationsverzeichnis

zugeordnete kryptographische Operation bereitstellt, ist als eine auf dem Prozessor des Datenträgers ausführbare Applikation im Speicher des Datenträgers gespeichert. Der Datenträger vereint also Datenspeicher und Kryptographiefunktionalität in einer Einheit und die kryptographischen Operationen werden auf dem Datenträger selbst mit minimalem Aufwand und auf sichere Weise ausgeführt.

Es ist aber auch möglich, dass eine kryptographische Applikation, die eine entsprechende kryptographische Operation bereitstellt, welche einem Kryptographieoperationsverzeichnis zugeordnet ist, zwar in dem Speicher des Datenträgers gespeichert ist, jedoch nicht auf dem Prozessor des Datenträgers ausgeführt wird. Die Applikation kann beispielsweise als portable Software ausgebildet sein, die eingerichtet ist, auf einem Prozessor einer Datenverarbeitungseinrichtung, welche mit dem Datenträger über eine Datenkommunikationsschnittstelle des Datenträgers verbindbar ist, ausgeführt zu werden. Dazu ist in der Regel keine aufwendige Installation der Applikation im System der Datenverarbeitungseinrichtung notwendig ist. Auf diese Weise können auch solche Datenträger, die über weniger leistungsfähige Prozessoren oder allgemein über eingeschränkte Rechenkapazitäten verfügen, welche zum kryptographischen Bearbeiten größerer Datenmengen nicht ausreichend sind, und die lediglich über ausreichend Speicherkapazität zum Speichern vom kryptographisch behandelten Daten verfügen, als erfindungsgemäße Datenträger eingesetzt werden.

Schließlich ist es möglich, dass die Steuereinrichtung des Datenträgers beim Zugriff auf ein Kryptographieoperationsverzeichnis das Ausführen einer kryptographischen Applikation auslöst, die eine entsprechende, dem Kryptographieoperationsverzeichnis zugeordnete kryptographische Operation bereitstellt und nicht auf dem Datenträger gespeichert ist, sondern direkt auf

einer mit dem Datenträger verbundenen Datenverarbeitungseinrichtung gespeichert ist und auf Veranlassung der Steuereinrichtung auf einem Prozessor der Datenverarbeitungseinrichtung ausgeführt wird.

Als erfindungsgemäße Datenträger können nach einer entsprechenden Einrichtung mittels des erfindungsgemäßen Verfahrens verschiedene Datenträger eingesetzt werden, z.B. Chipkarten, Massenspeicherkarten, USB-Tokens, aber auch Festplatten und dergleichen. Die jeweiligen Datenträger sind dabei in der Regel derart ausgebildet, dass sie eine Datenkommunikationsschnittstelle umfassen, welche allgemein verbreitete Kommunikationsprotokolle unterstützt, z.B. USB, so dass eine einfache Portierung von auf dem Datenträger gespeicherten Daten sichergestellt ist.

Es ist möglich, dass der Controller des jeweiligen Datenträgers, der allgemein den Schreib- und Lesezugriff auf den Speicher des Datenträgers bzw. auf Verzeichnisse des darin eingerichteten Dateisystems überwacht und steuert, insbesondere also auch den Zugriff auf eingerichtete Kryptographieoperationsverzeichnisse, die Steuereinrichtung umfasst. Das heißt, jeder Zugriff auf ein Kryptographieoperationsverzeichnis wird automatisch vom Controller erkannt und löst mittels der Steuereinrichtung das Auslösen entsprechender, dem Kryptographieoperationsverzeichnis zugeordneter kryptographischer Operationen aus. Vorzugsweise wird auf Cache-Mechanismen im Controller verzichtet, um einen Zugriff auf in dem Datenträger gespeicherte Daten unmittelbar zu erkennen.

Die vorliegende Erfindung wird im Folgenden mit Bezug auf die beiliegenden Zeichnungen beispielhaft beschrieben. Darin zeigen:

Figur 1 eine bevorzugte Ausführungsform eines erfindungsgemäßen Datenträgers;

Figur 2 eine schematische Darstellung eines Dateisystems des Datenträgers aus Fig. 1; und

Figur 3. eine schematische Darstellung eines Dateisystems eines Datenträgers gemäß einer weiteren Ausführungsform.

Mit Bezug auf Figur 1 umfasst ein portabler Datenträger 10, der hier als Chipkarte ausgebildet ist, eine Datenkommunikationsschnittstelle 20, einen Prozessor (CPU) 30 und verschiedene Speicher 40, 50 und 60.

Die Kommunikationsschnittstelle 20 ist als Kontaktfeld gemäß ISO 7816 ausgebildet und unterstützt sowohl das T=0 / T=1 Kommunikationsprotokoll als auch das USB-Kommunikationsprotokoll. Es ist auch möglich, die Kommunikationsschnittstelle auf andere Weise auszubilden, beispielsweise nach dem SD-Standard. Über die Kommunikationsschnittstelle 20 kann der Datenträger 10 mit verschiedenen Datenverarbeitungseinrichtungen verbunden werden, die jeweils ihrerseits über eine geeignete Schnittstelle bzw. ein geeignetes Lesegerät verfügen, um die Kommunikationsschnittstelle 20 zu kontaktieren, und die ein von dem Datenträger 10 unterstütztes Kommunikationsprotokoll ebenfalls unterstützen. Der Datenträger 10 kann dabei auch als Massenspeicherkarte, (U)SIM-Mobilfunkkarte, USB-Token oder dergleichen, aber z.B. auch als - eventuell externe - Festplatte ausgebildet sein. Als Datenverarbeitungseinrichtungen, mit denen der Datenträger verbindbar ist, kommen ein Personal Computer (PC), ein Laptop, ein PDA, ein Mobilfunkendgerät und dergleichen in Frage.

Der nicht flüchtige, nicht wiederbeschreibbare ROM-Speicher 40 umfasst ein den Datenträger 10 steuerndes Betriebssystem (OS) 42. Teile des Betriebssystems 42, insbesondere so genannte Bibliotheksfunktionen, oder das gesamte Betriebssystem 42 können aber auch in dem nicht flüchtigen, wiederbeschreibbaren FLASH-Speicher 50 gespeichert sein. Der Speicher 50, der auch ein EEPROM-Speicher oder dergleichen sein kann, speichert weiterhin ein Dateisystem 70, eine Steuerapplikation 80 und kryptographische Applikationen 90, 92, 94 und 96. Diese Komponenten und Applikationen werden nachstehend mit Bezug auf Fig. 2 genauer beschrieben. Ein flüchtiger, wiederbeschreibbarer RAM-Speicher 60 dient dem Datenträger 10 als schneller Arbeitsspeicher.

Figur 2 veranschaulicht das Dateisystem 70 des Datenträgers 10, integriert in ein Dateisystem eines PCs, mit dem der Datenträger 10 verbunden ist. Der Datenträger 10 erscheint dabei als Wechseldatenträger E. Das Dateisystem 70 des Datenträgers 10 ist in Form eines Verzeichnisbaums gegliedert. Dieser umfasst auf der obersten Ebene die Verzeichnisse Kryptographie 100 und home 200, wobei für die vorliegende Erfindung vor allem das Verzeichnis 100 und seine nachstehend erläuterten Unterverzeichnisse relevant sind. Das Vorhandensein des Verzeichnisses 200 deutet an, dass der Datenträger 10 neben den erfindungsrelevanten Funktionen weitere Funktionalitäten umfassen kann, die vollständig unabhängig und unbeeinflusst von den nachstehend beschriebenen kryptographischen Operationen betrieben werden können, beispielsweise Funktionalitäten zum Unterstützen einer mobilen Kommunikation in einem Mobilfunknetz oder dergleichen.

Das Verzeichnis Kryptographie 100 umfasst das Unterverzeichnis Kryptographieoperationsverzeichnisse 105, welches seinerseits sieben Unterverzeichnisse Verschlüsseln 110, Entschlüsseln 120, Signieren 130, Verifizieren

140, Verschlüsseln+Entschlüsseln 150, Verschlüsseln+Signieren 160 und Entschlüsseln+Verifizieren 170 umfasst. In diesen Verzeichnissen können jeweils verschiedene, wie nachstehend beschrieben, auf definierte Weise kryptographisch behandelte Daten gespeichert sein. Der Inhalt des Verzeichnisses Verschlüsseln 110, welches eingerahmt dargestellt ist, ist auf der rechten Seite angedeutet. In dem Verzeichnis sind zwei verschlüsselte Dateien data1.txt.gpg und data2.pdf.gpg gespeichert.

Sämtliche in dem Unterverzeichnis Kryptographieoperationsverzeichnisse 105 angeordneten Unterverzeichnisse 110 bis 170 sind derart eingerichtet, dass jedem dieser Verzeichnisse 110 bis 170 eine oder mehrere kryptographische Operationen, die jeweils durch die Applikationen 90, 92, 94, 96 bereitgestellt werden, in einer Weise zugeordnet sind, dass ein Zugriff eines Nutzers des Datenträgers 10 auf das entsprechende Verzeichnis 110 bis 170 eine Ausführung der oder einer der zugeordneten Operationen auslöst. Die Namen der Verzeichnisse 110 bis 170 geben dabei bereits an, welche kryptographische(n) Operation(en) bei einem Zugriff auf das jeweilige Verzeichnis ausgelöst wird (werden). Dabei ist es möglich, dass ein Ausführen einer zugeordneten kryptographischen Operation ausschließlich bei einem lesenden Zugriff, ausschließlich bei einem schreibenden Zugriff oder bei einem lesenden und bei einem schreibenden Zugriff ausgelöst wird. Gleichfalls ist es möglich, dass bei verschiedenen Zugriffsarten verschiedene zugeordnete Operationen ausgelöst werden oder dass bei einem Zugriff mehrere Operationen ausgeführt werden.

Bei einem schreibenden Zugriff auf das Verzeichnis Verschlüsseln 110 wird automatisch die dem Verzeichnis 110 zugeordnete kryptographische Operation Verschlüsseln auf die bei dem schreibenden Zugriff in dem Verzeichnis 110 abgelegten Daten angewandt. Dabei erkennt die Steuerapplikation 80,

dass Daten in das entsprechende Verzeichnis 110 geschrieben werden sollen und veranlasst daraufhin eine entsprechende Applikation 90, die in dem Speicher 50 gespeichert und auf dem Prozessor 30 ausführbar ist, und die die Operation des Verschlüsselns bereitstellt, die in das Verzeichnis 110 zu schreibenden Daten zu verschlüsseln, bevor diese in dem Verzeichnis 110 in verschlüsselter Form gespeichert werden, wie z.B. die Datei data1.txt.gpg.

Es ist dabei möglich, dass die Steuereinrichtung 80 mit einem Controller des Datenträgers 10, der den Schreib- und Lesezugriff auf den Speicher 50 des Datenträgers 10 steuert, oder einer entsprechenden Funktion des Betriebssystems 42 derart gekoppelt ist, dass durch den Controller ein versuchter Zugriff auf das Verzeichnis 110 direkt erkannt und mittels der Steuereinrichtung 80 ein Auslösen des Verschlüsselns mittels der Applikation 90 direkt ausgelöst wird, so dass die Daten zu keiner Zeit in unverschlüsselter Form in dem Verzeichnis 110 vorliegen. Es ist aber auch möglich, dass, nachdem die Daten nach dem Ablegen in dem Verzeichnis 110 kurzzeitig unverschlüsselt vorlagen, die Steuereinrichtung 80 durch eine permanente Überwachung des Verzeichnisses 110 erkennt, dass neue, noch unverschlüsselte Daten vorliegen, und daraufhin die Applikation 90 veranlasst, eine Verschlüsselung dieser Daten vorzunehmen.

Um die Operation des Verschlüsselns durchzuführen, benötigt die Applikation 90 entsprechende Schlüssel, die zur Verschlüsselung verwendet werden sollen. Dabei ist es möglich, dass, falls keine weiteren Angaben vorliegen, die Daten mit dem öffentlichen Schlüssel (in Falle eines public-key-Kryptosystems) des Nutzers des Datenträgers 10 verschlüsselt werden. Es ist aber auch möglich, der Applikation 90 eine Empfängerschlüsselliste mit mehreren Schlüsseln zum Verschlüsseln der Daten bereitzustellen, beispielsweise mittels einer lokalen Konfigurationsdatei, die in dem Verzeichnis Temporäre

Konfiguration 195 als Datei Empfängerschlüssel 197 abgelegt sein kann. Verschiedene Schlüssel von anderen Kommunikationspartnern können in einem separaten Verzeichnis Schlüsselring 180 und darunter angelegten Unterverzeichnissen 182, 184 gespeichert und verwaltet werden.

Alternativ kann eine vorstehend beschriebene Konfigurationsdatei, die zum Durchführen einer kryptographischen Operation notwendige Informationen enthält, auch temporär jeweils in dem Verzeichnis, dem die entsprechende Operation zugeordnet ist, gespeichert und nach einem Ausführen der Operation automatisch wieder gelöscht werden. Vorstehend beschriebene und andere Konfigurationsdaten, wie beispielsweise eine Wahl eines Verschlüsselungsalgorithmus, falls mehrere zur Auswahl stehen, können alternativ oder zusätzlich den kryptographischen Applikationen 90 bis 96 auch mittels Dateiattributen oder Dateiparameter übergeben werden.

Bei einem lesenden Zugriff auf das Verzeichnis 110 werden die Daten nicht erneut verschlüsselt, sondern dem Nutzer in der einfach verschlüsselten Form zurückgeliefert.

Dem Verzeichnis Entschlüsseln 120 ist die kryptographische Operation des Entschlüsselns in der Weise zugeordnet, dass bei einem lesenden Zugriff auf das Verzeichnis 120 die ausgelesenen Daten automatisch mittels der Applikation 92, die die kryptographische Operation des Entschlüsselns bereitstellt, entschlüsselt werden, d.h. es wird angenommen, dass in dem Verzeichnis 120 verschlüsselte Daten gespeichert sind. Dabei ist die Zuordnung zusätzlich in der Weise vorgenommen, dass der Nutzer des Datenträgers 10 bei einem lesenden Zugriff automatisch aufgefordert wird, sich gegenüber dem Datenträger 10 zu authentisieren. Auf diese Weise wird sichergestellt, dass nur autorisierte Personen kryptographisch gesicherte, verschlüsselte und auf

dem Datenträger 10 gespeicherte Daten entschlüsseln können. Die Authentisierung kann dabei dadurch erfolgen, dass der Nutzer direkt den zum Entschlüsseln benötigten Schlüssel übergibt. Weitere Authentisierungsmöglichkeiten sind die Eingabe einer anderen geheimen Information, insbesondere einer PIN, oder die Bereitstellung einer andersartigen Authentifikationsinformation, insbesondere eines biometrischen Merkmals, z.B. eines Fingerabdrucks.

In ähnlicher Weise oder alternativ kann ein weiteres Kryptographieoperationsverzeichnis angelegt werden, dem die Operation des Entschlüsselns in der Weise zugeordnet ist, dass ein schreibender Zugriff auf das Verzeichnis die Operation des Entschlüsselns auslöst, d.h. dass in der Regel verschlüsselte Daten in das Verzeichnis geschrieben und dabei automatisch entschlüsselt werden. Als Voraussetzung für einen solchen schreibenden Zugriff kann dann ebenfalls eine Authentisierung des Nutzers gegenüber dem Datenträger 10 gefordert werden.

Dem Verzeichnis Signieren 130 ist die kryptographische Operation des Signierens mittels einer kryptographischen Signatur derart zugeordnet, dass bei einem schreibenden Zugriff auf das Verzeichnis die in dem Verzeichnis abgelegten Daten automatisch signiert werden. Die Applikation 94 stellt dabei die Operation des Signierens bereit. Analog zu der Zuordnung der Operation des Entschlüsselns zum Verzeichnis 120 wird der Nutzer des Datenträgers 10 auch bei einem schreibenden Zugriff auf das Verzeichnis Signieren 130 automatisch aufgefordert, sich gegenüber dem Datenträger zu authentisieren. Auch in diesem Fall ist es möglich, wie vorstehend mit Bezug auf das Verzeichnis Entschlüsseln 120 beschrieben, ein weiteres oder alternatives Kryptographieoperationsverzeichnis anzulegen, welchem die Operation des Signierens bei einem lesenden Zugriff zugeordnet ist.

Es ist gleichfalls möglich, dass der Nutzer sich unabhängig von einem Zugriff auf eines der Kryptographieoperationsverzeichnisse generell gegenüber dem Datenträger 10 authentisiert. Dazu ist ein Verzeichnis Authentisierung 190 in dem Dateisystem 70 angelegt, welchem eine Authentisierungsapplikation derart zugeordnet ist, dass der Nutzer des Datenträgers 10 bei einem Zugriff auf das Verzeichnis 190 automatisch zur Authentisierung gegenüber dem Datenträger 10 aufgefordert wird. Hat sich der Nutzer einmal gegenüber dem Datenträger 10 authentisiert, so kann eine weitere Authentisierung, z.B. bei einem lesenden Zugriff auf das Verzeichnis Entschlüsseln 120 oder bei einem schreibenden Zugriff auf das das Verzeichnis Signieren 130 entfallen, solange eine Sitzung auf dem Datenträger 10 andauert. Schließlich ist es auch möglich, eine Authentisierungsanforderung an weitere kryptographische Operationen zu binden oder aber gänzlich davon abzusehen.

Dem Verzeichnis Verifizieren 140 ist die kryptographische Operation des Verifizierens einer kryptographischen Signatur derart zugeordnet, dass bei einem lesenden Zugriff auf in dem Verzeichnis 140 gespeicherte Daten eine Signatur dieser Daten automatisch mittels der Applikation 96 verifiziert wird.

Dem Verzeichnis Verschlüsseln+Entschlüsseln 150 sind die beiden kryptographischen Operationen Verschlüsseln und Entschlüsseln jeweils in der Weise zugeordnet, wie es mit Bezug auf die Verzeichnisse 110 und 120 beschrieben worden ist, d.h. dass Daten beim Ablegen in dem Verzeichnis 150 automatisch verschlüsselt und beim Auslesen nach einer erfolgreichen Authentisierung des Nutzers automatisch wieder entschlüsselt werden.

Dem Verzeichnis Verschlüsseln+Signieren 160 sind die gleichnamigen Operationen in der Weise zugeordnet, wie es mit Bezug auf die Verzeichnisse 110 und 130 beschrieben worden ist. Dabei gilt, dass die Zuordnung der beiden Operationen dabei derart erfolgt, dass ein schreibender Zugriff auf das Verzeichnis 160 beide Operationen auslöst, d.h. dass in das Verzeichnis abgelegte Daten sowohl verschlüsselt als auch signiert werden. Zum Signieren der Daten wird der Nutzer des Datenträgers 10, wie vorstehend beschrieben, zur Authentisierung gegenüber dem Datenträger 10 aufgefordert.

Dem Verzeichnis Entschlüsseln+Verifizieren 170 schließlich sind die im Verzeichnisnamen angegebenen Operationen in einer mit Bezug auf die Verzeichnisse 120 und 140 beschriebenen Weise zugeordnet. Auch hier gilt, wie mit Bezug auf das Verzeichnis 160 beschrieben, dass ein Zugriff, diesmal ein lesender Zugriff, das Ausführen beider dem Verzeichnis zugeordneter Operationen, nämlich das Entschlüsseln der Daten und das Verifizieren der Signatur, auslöst.

Abschließend zu diesem Komplex sollte bemerkt werden, dass, falls irrtümlich Daten, die z.B. nicht verschlüsselt sind, in dem Verzeichnis Entschlüsseln 120 abgelegt werden und nachfolgend lesend auf diese Daten zugegriffen wird, die Steuerapplikation 80 erkennt, dass nichts zu Entschlüsseln ist und ein gewöhnliches Auslesen der Daten erlaubt. Sinngemäß gilt Gleiches für die Verzeichnisse 140 und 170.

Die in den Verzeichnissen 110 bis 170 gespeicherten Daten können auf dem Datenträger 10 selbst oder in einer mit dem Datenträger 10 verbundenen Datenverarbeitungseinrichtung weiterverarbeitet werden, beispielsweise können signierte Daten aus dem Verzeichnis 130 an eine e-Mail-Applikation der

Datenverarbeitungseinrichtung weitergeleitet und per e-Mail verschickt werden.

Gemäß einer weiteren Ausführungsform der Erfindung ist es möglich, dass die kryptographischen Applikationen 90, 92, 94, 96 auf dem Datenträger 10 als portable Software ("stickware") gespeichert sind und nicht auf dem Prozessor 30 des Datenträgers 10, sondern auf einem Prozessor einer mit dem Datenträger verbundenen Datenverarbeitungseinrichtung ausgeführt werden. Dabei ist die entsprechende Software in einer Weise ausgebildet, dass keine aufwendige Installation in dem System der Datenverarbeitungseinrichtung notwendig ist. Schließlich ist es möglich, dass die Steuereinrichtung 80 solche kryptographischen Operationen auslöst, die nur auf der Datenverarbeitungseinrichtung gespeichert und lauffähig sind.

Generell können Mittel, die es dem System der Datenverarbeitungseinrichtung möglich machen, auf das Dateisystem 70 des Datenträgers 10 zuzugreifen, mittels einfacher portabler Software bereitgestellt werden. Auf aufwendig zu installierende und zu wartende Middleware zu diesem Zweck kann dann verzichtet werden. Auf diese Weise können zum Beispiel sichere portable Banking-Applikationen, ein sicheres, automatisches Abspeichern bzw. Signieren von Daten in Digitalkameras und ein Abspielen von mittels DRM ("digital rights management", Digitale Rechteverwertung) gesicherten Inhalten ermöglicht werden.

Mit Bezug auf Figur 3 wird abschließend ein Dateisystem eines Datenträgers gemäß einer weiteren Ausführungsform der Erfindung exemplarisch dargestellt. Analog zu den vorstehend mit Bezug auf Figur 2 beschriebenen Kryptographieoperationsverzeichnissen 110, 120, 130, 140 160 und 170 umfasst das hier dargestellte Dateisystem die mit den entsprechenden englischen Be-

griffen bezeichneten Verzeichnisse encrypt, decrypt, sign, verify, encrypt-sign und decrypt-verify. Die Verzeichnisse APDU-in und APDU-out ermöglichen eine direkte Kommunikation des Nutzers mit dem Datenträger, einer Chipkarte gemäß ISO 7816, über entsprechende Kommando-APDUs ("Application Protocol Data Unit"). Diese Verzeichnisse erfüllen unter anderem analoge Funktionen wie das vorstehend mit Bezug auf Figur 2 beschriebene Verzeichnis Authentisierung 190. Ein Nutzer des Datenträgers kann sich beispielsweise mittels einer Applikation verify-APDU, die dem Verzeichnis ADPU-in zugeordnet sein kann, gegenüber dem Datenträger authentisieren und somit generell den Zugriff auf alle kryptographischen Operationen, die den oben bezeichneten Verzeichnissen zugeordnet sind, ermöglichen, ohne dass eine fallweise Authentisierung, beispielsweise beim lesenden Zugriff auf das Verzeichnis decrypt, notwendig wäre.

Gemäß der hier dargestellten Ausführungsform ist es z.B. beim Verschlüsseln (und Signieren) von Daten bei einem schreibenden Zugriff auf das Verzeichnis encrypt(-sign) vorgesehen, dass nach dem Verschlüsseln (und Signieren) neben den verschlüsselten (und signierten) Daten, die in Figur 3 mit to_be_encrypted.data.pgp bezeichnet sind, eine Berichtsdatei, to_be_encrypted.data_result, gespeichert wird, die beispielsweise beinhaltet, mit welchem Algorithmus und mit welchen Schlüsseln die entsprechende Datei to_be_encrypted.data verschlüsselt worden ist. Die Berichtsdatei kann weitere oder andere Informationen enthalten oder aber entfallen.

Patentansprüche

1. Verfahren auf einem portablen Datenträger (10) mit eingerichtetem Dateisystem (70), umfassend den Schritt des Zugreifens auf ein Verzeichnis des Dateisystems (70) durch einen Nutzer des Datenträgers (10), **dadurch gekennzeichnet**, dass dem Verzeichnis (110, 120, 130, 140, 150, 160, 170) zumindest eine kryptographische Operation zugeordnet ist, wobei beim Zugreifen auf das Verzeichnis (110, 120, 130, 140, 150, 160, 170) eine Ausführung der zugeordneten kryptographischen Operation ausgelöst wird und beim Auslösen der kryptographischen Operation der auf das Verzeichnis (120, 130, 150, 160, 170) zugreifende Nutzer aufgefordert wird, sich gegenüber dem Datenträger (10) zu authentisieren.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass beim Zugreifen auf das Verzeichnis (120, 130, 150, 160, 170) als zugeordnete kryptographische Operation ein Entschlüsseln verschlüsselter Daten oder ein Signieren von Daten mittels einer kryptographischen Signatur ausgelöst wird.

3. Verfahren nach Anspruch 2, **dadurch gekennzeichnet**, dass der Nutzer aufgefordert wird, dem Datenträger (10) einen zum Entschlüsseln oder Verifizieren benötigten kryptographischen Schlüssel oder eine geheime Information, insbesondere eine PIN, oder eine Authentifikationsinformation, insbesondere ein biometrisches Merkmal, bereitzustellen.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass der Datenträger (10) die Ausführung der zugeordneten krypto-

graphischen Operation auf einer mit dem Datenträger (10) verbundenen Datenverarbeitungseinrichtung veranlasst.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, dass die zugeordnete Operation ausschließlich bei einem lesenden Zugreifen oder ausschließlich bei einem schreibenden Zugreifen auf das Verzeichnis (110, 120, 130, 140, 160, 170) ausgelöst wird.

6. Portabler Datenträger (10), umfassend einen Speicher (50) mit einem darin eingerichteten Dateisystem (70), einen Prozessor (30) und eine Steuereinrichtung (80), **dadurch gekennzeichnet**, dass in dem Dateisystem (70) zumindest ein Kryptographieoperationsverzeichnis (110, 120, 130, 140, 150, 160, 170) angelegt ist, dem zumindest eine kryptographische Operation zugeordnet ist, wobei die Steuereinrichtung (80) eingerichtet ist, bei einem Zugriff auf das Kryptographieoperationsverzeichnis (110, 120, 130, 140, 150, 160, 170) durch einen Nutzer des Datenträgers (10) eine Ausführung der zumindest einen dem Kryptographieoperationsverzeichnis (110, 120, 130, 140, 150, 160, 170) zugeordneten Operationen auszulösen.

7. Datenträger (10) nach Anspruch 6, **dadurch gekennzeichnet**, dass dem Kryptographieoperationsverzeichnis (120, 130, 150, 160, 170) als kryptographische Operation ein Entschlüsseln verschlüsselter Daten oder ein Signieren von Daten mittels einer kryptographischen Signatur zugeordnet ist, und die Steuereinrichtung (80) eingerichtet ist, den auf das Kryptographieoperationsverzeichnis zugreifenden Nutzer beim Auslösen des Entschlüsselns oder des Signierens zur Authentisierung gegenüber dem Datenträger (10) aufzufordern.

8. Datenträger (10) nach Anspruch 6 oder 7, **gekennzeichnet durch** einen Controller, der schreibende oder lesende Zugriffe auf das Kryptographieoperationsverzeichnis (110, 120, 130, 140, 150, 160, 170) steuert und die Steuereinrichtung (80) umfasst.

9. Datenträger (10) nach einem der Ansprüche 6 bis 8, **gekennzeichnet durch** eine Datenkommunikationsschnittstelle (20) und dadurch, dass die Steuereinrichtung (80) eingerichtet ist, die Ausführung einer kryptographischen Applikation (90, 92, 94, 96), die die zugeordnete kryptographische Operation bereitstellt, auf einem Prozessor einer mit dem Datenträger (10) über die Datenkommunikationsschnittstelle (20) verbindbaren Datenverarbeitungseinrichtung zu veranlassen.

10. Datenträger (10) nach einem der Ansprüche 6 bis 9, **dadurch gekennzeichnet**, dass die Steuereinrichtung (80) eingerichtet ist, ein Verfahren nach einem der Ansprüche 2, 4 oder 6 auszuführen.

11. Verfahren zum Einrichten eines portablen Datenträgers (10) mit eingerichtetem Dateisystem (70), **gekennzeichnet durch** die Schritte:

- Anlegen zumindest eines Kryptographieoperationsverzeichnisses (110, 120, 130, 140, 150, 160, 170) in dem Dateisystem (70); und
- Zuordnen zumindest einer kryptographischen Operation zum Entschlüsseln von verschlüsselten Daten oder zum Signieren von Daten mittels einer kryptographischen Signatur zu zumindest einem Kryptographieoperationsverzeichnis (110, 120, 130, 140, 150, 160, 170) derart, dass ein Zugriff eines Nutzers des Datenträgers (10) auf das Kryptographieoperationsverzeichnis (110, 120, 130, 140, 150, 160, 170) eine Ausführung der zumindest einen zugeordneten kryptographischen Operationen auslöst und der zugreifende Nutzer beim Ausführen der krypto-

graphischen Operation zur Authentisierung gegenüber dem Datenträger (10) aufgefordert wird.

12. Verfahren nach Anspruch 11, **dadurch gekennzeichnet**, dass die Operation des Entschlüsseln oder des Signierens dem Kryptographieoperationsverzeichnis (120, 130, 150, 160, 170) derart zugeordnet wird, dass der auf das Kryptographieoperationsverzeichnis (120, 130, 150, 160, 170) zugreifende Nutzer aufgefordert wird, einen zum Ausführen des Entschlüsselns oder des Signierens benötigten kryptographischen Schlüssel oder eine geheime Information, insbesondere eine PIN, oder eine Authentifikationsinformation, insbesondere ein biometrisches Merkmal, bereitzustellen.

13. Verfahren nach Anspruch 11 , **dadurch gekennzeichnet**, dass die zumindest eine kryptographische Operation dem zumindest einen Kryptographieoperationsverzeichnis (110, 120, 130, 140, 150, 160, 170) derart zugeordnet wird, dass die Ausführung der kryptographischen Operation auf einer mit dem Datenträger (10) verbundenen Datenverarbeitungseinrichtung auslösbar ist.

14. Verfahren nach Anspruch 11, **dadurch gekennzeichnet**, dass die zumindest eine kryptographische Operation dem zumindest einen Kryptographieoperationsverzeichnis (110, 120, 130, 140, 160, 170) derart zugeordnet wird, dass ausschließlich bei einem lesenden Zugriff oder ausschließlich bei einem schreibenden Zugriff auf das Kryptographieoperationsverzeichnis (110, 120, 130, 140, 160, 170) eine Ausführung der kryptographischen Operation ausgelöst wird.

FIG 1

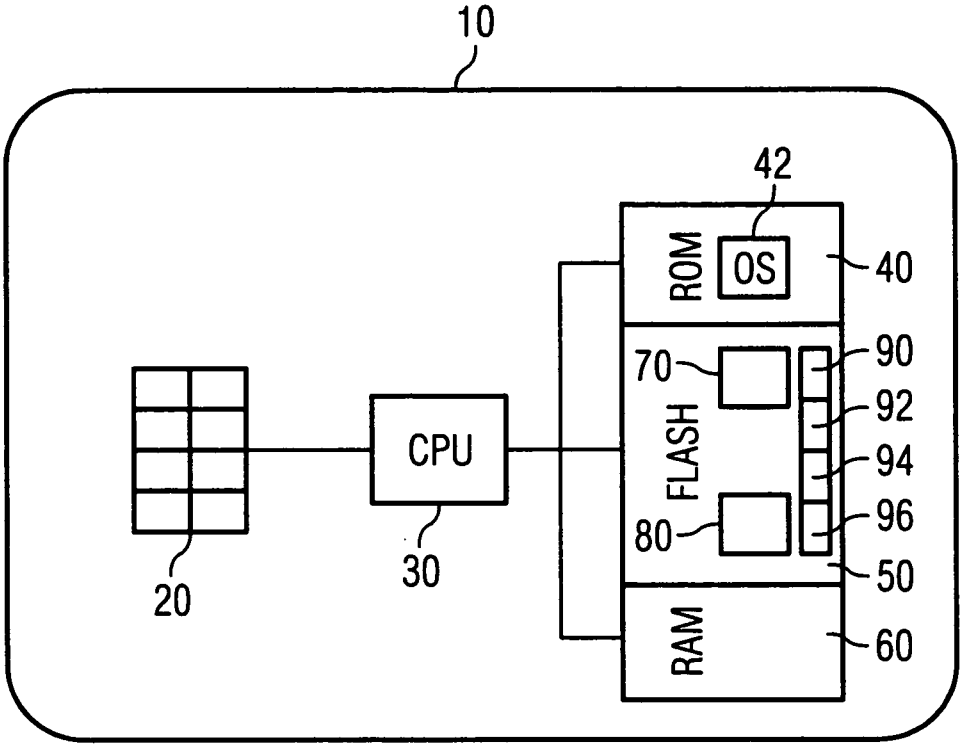


FIG 2

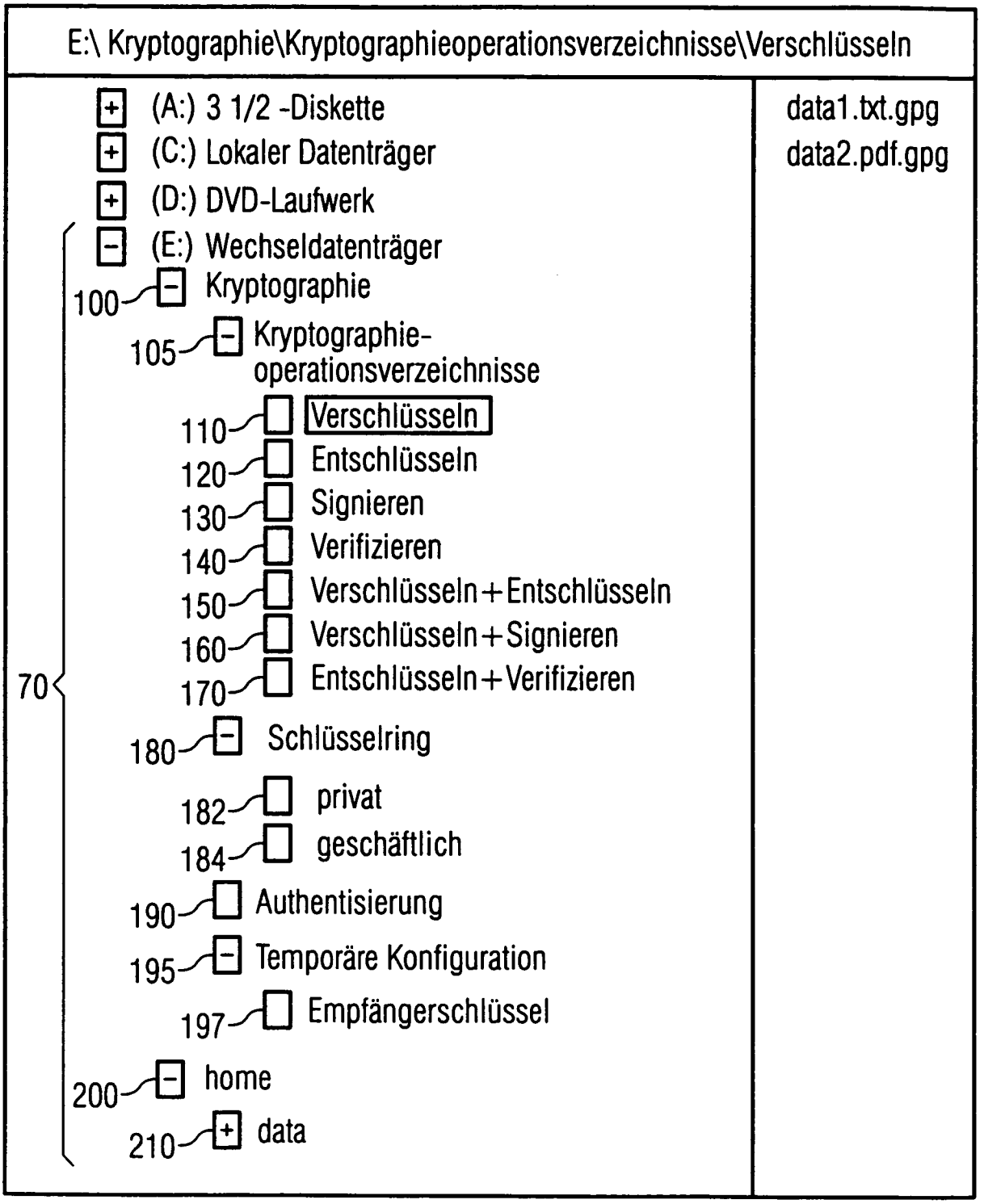
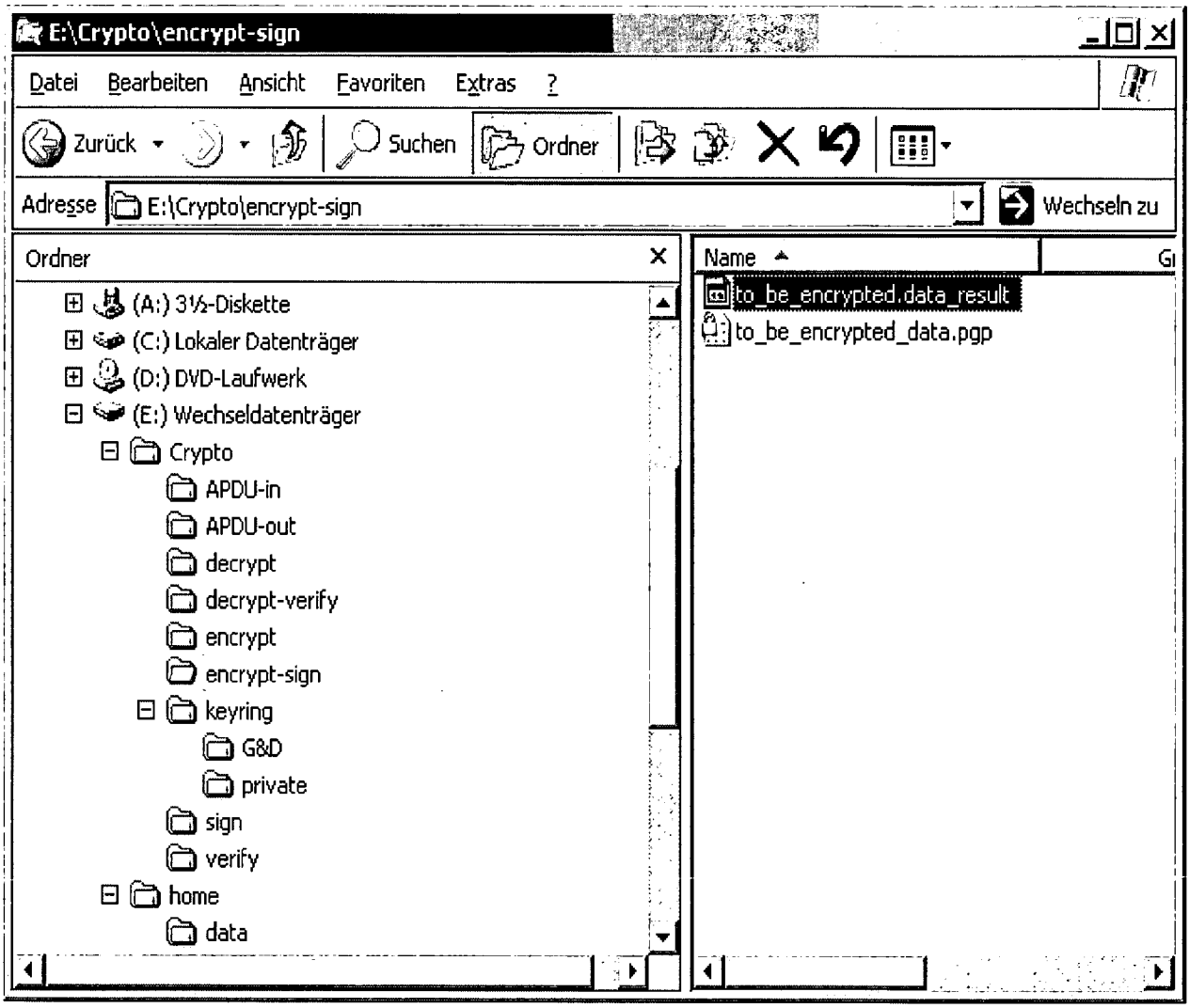

E:\ Kryptographie\Kryptographieoperationsverzeichnisse\Verschlüsseln
(A:) 3 1/2 -Diskette
(C:) Lokaler Datenträger
(D:) DVD-Laufwerk
(E:) Wechseldatenträger
100 Kryptographie
105 Kryptographie-operationsverzeichnisse
110 Verschlüsseln
120 Entschlüsseln
130 Signieren
140 Verifizieren
150 Verschlüsseln+Entschlüsseln
160 Verschlüsseln+Signieren
170 Entschlüsseln+Verifizieren
70
180 Schlüsselring
182 privat
184 geschäftlich
190 Authentisierung
195 Temporäre Konfiguration
197 Empfängerschlüssel
200 home
210 data
data1.txt.gpg
data2.pdf.gpg

FIG 3


E:\Crypto\encrypt-sign
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Ordner
Adresse E:\Crypto\encrypt-sign
Wechseln zu
Ordner
(A:) 3½-Diskette
(C:) Lokaler Datenträger
(D:) DVD-Laufwerk
(E:) Wechseldatenträger
Crypto
APDU-in
APDU-out
decrypt
decrypt-verify
encrypt
encrypt-sign
keyring
G&D
private
sign
verify
home
data
Name
to_be_encrypted.data_result
to_be_encrypted_data.pgp

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/004336

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/24

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

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, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98/55912 A (SPYRUS INC [US]) 10 December 1998 (1998-12-10) abstract page 1, line 19 - page 2, line 5; figures 1-8 page 5, line 11 - page 10, line 21 page 11, line 27 - page 31, line 16 page 37, line 30 - page 41, line 14	1-14
P,X	EP 1 990 751 A (SECUNET SECURITY NETWORKS AG [DE]) 12 November 2008 (2008-11-12) cited in the application abstract paragraphs [0002] - [0010], [0013]; figures 1-3	1-14
A	JP 2006 164096 A (HITACHI LTD) 22 June 2006 (2006-06-22) abstract	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family 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
11 September 2009	24/09/2009

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, Fax: (+31-70) 340-3016	Kleiber, Michael

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/004336

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9855912 A	10-12-1998	AU 7709498 A	21-12-1998
		US 6003135 A	14-12-1999
EP 1990751 A	12-11-2008	NONE	
JP 2006164096 A	22-06-2006	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2009/004336

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/24

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F

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, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 98/55912 A (SPYRUS INC [US]) 10. Dezember 1998 (1998-12-10) Zusammenfassung Seite 1, Zeile 19 - Seite 2, Zeile 5; Abbildungen 1-8 Seite 5, Zeile 11 - Seite 10, Zeile 21 Seite 11, Zeile 27 - Seite 31, Zeile 16 Seite 37, Zeile 30 - Seite 41, Zeile 14 -----	1-14
P,X	EP 1 990 751 A (SECUNET SECURITY NETWORKS AG [DE]) 12. November 2008 (2008-11-12) in der Anmeldung erwähnt Zusammenfassung Absätze [0002] - [0010], [0013]; Abbildungen 1-3 -----	1-14
A	JP 2006 164096 A (HITACHI LTD) 22. Juni 2006 (2006-06-22) Zusammenfassung -----	1-14

☐ 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	Absendedatum des internationalen Recherchenberichts
11. September 2009	24/09/2009

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kleiber, Michael

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2009/004336

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9855912	A	10-12-1998	AU	7709498 A	21-12-1998
			US	6003135 A	14-12-1999
EP 1990751	A	12-11-2008	KEINE		
JP 2006164096	A	22-06-2006	KEINE		