(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
6. November 2008 (06.11.2008)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2008/132129 A1

(51) **Internationale Patentklassifikation:**
G06F 21/00 (2006.01)

(21) **Internationales Aktenzeichen:** PCT/EP2008/054999

(22) Internationales Anmeldedatum:
24. April 2008 (24.04.2008)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2007 019 541.0 25. April 2007 (25.04.2007) DE

(71) **Anmelder** *(für alle Bestimmungsstaaten mit Ausnahme von US):* **WINCOR NIXDORF INTERNATIONAL GMBH** [DE/DE]; Heinz-Nixdorf-Ring 1, 33106 Paderborn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US):* **BLUME, Marco** [DE/DE]; Neuhäuserstrasse 132, 33102 Paderborn (DE). **NOLTE, Michael** [DE/DE]; Koberg Weg 2a, 33034 Brakel (DE).

(74) Anwalt: SCHAUMBURG, THOENES, THURN, LANDSKRON; Postfach 86 07 48, 81634 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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND SYSTEM FOR AUTHENTICATING A USER

(54) Bezeichnung: VERFAHREN UND SYSTEM ZUM AUTHENTIFIZIEREN EINES BENUTZERS

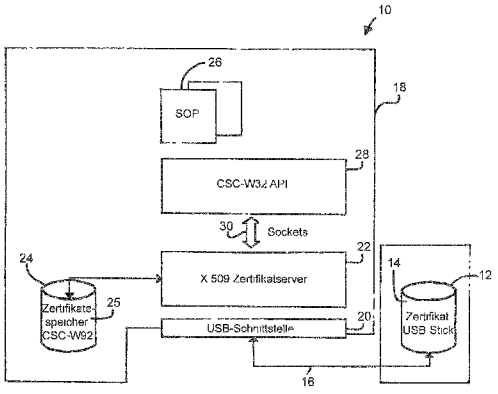

Fig. 1

22... X.509 Certificate Server
25... Certificate memory CSC-W92
20... USB interface
14... Certificate USB stick

(57) Abstract: The invention relates to a System and a method for authenticating a user. A removable memory means (12) comprises at least one memory region, in which identification data for the identification of the removal memory means (12) is stored, wherein in said memory region, or in a further memory region of the removable memory means (12), data of a digital certificate (14) is stored. Furthermore, a data processing System (18) is provided, to which the removable memory means (12) is connected via a data transmission connection. The identification data and the data of the digital certificate (14) are transmitted by the removable memory means to the data processing System (18). The data processing System (18) processes the identification data and the data of the digital certificate (14) and authenticates the user.

(57) Zusammenfassung: Die Erfindung betrifft ein System und ein Verfahren zum Authentifizieren eines Benutzers. Ein Wechselspeichermedium (12) weist mindestens einen Speicherbereich auf, in dem Identifizierungsdaten zum Identifizieren des Wechselspeichermediums (12) gespeichert sind, wobei in diesem Speicherbereich oder in einem weiteren Speicherbereich des

[Fortsetzung auf der nächsten Seite]

WO 2008/132129 A1

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 verfugbare 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), europaisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FT, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, 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)

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist, Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Wechselspeichermediums (12) Daten eines digitalen Zertifikats (14) gespeichert sind Ferner ist eine Datenverarbeitungsanlage (18) vorgesehen, mit der das Wechselspeichermedium (12) über eine Datenubertragungsverbindung verbunden ist Die Identifïzierungsdaten und die Daten des digitalen Zertifikats (14) werden vom Wechselspeichermedium zur Datenverarbeitungsanlage (14) übertragen Die Datenverarbeitungsanlage (18) verarbeitet die Identifïkationsdaten und die Daten des digitalen Zertifikats (14) und authentifiziert den Benutzer

Verfahren und System zum Authentifizieren eines Benutzers

Die Erfindung betrifft ein Verfahren und ein System zum Authentifizieren eines Benutzers bei einer Datenverarbeitungsanlage. Insbesondere dient die Erfindung zum Authentifizieren eines Benutzers an einem Geldmitteltransaktionsgerät. Bei Datenverarbeitungsanlagen, insbesondere bei Datenverarbeitungsanlagen, die Bestandteil eines Geldmitteltransaktionsgerätes sind, müssen eine Vielzahl von Sicherheitsaspekten berücksichtigt werden, um sicherzustellen, dass diese Datenverarbeitungsanlagen nicht von Unbefugten manipuliert werden können. Besonders die Übertragung von Daten, insbesondere von Programmdaten, von einem Wechseldatenträger zur Datenverarbeitungsanlage sowie von Daten von der Datenverarbeitungsanlage zu einem mit dieser Datenverarbeitungsanlage verbundenen Wechseldatenträger sollte bei unbefugten Benutzern sicher verhindert werden.

Bei Geldmitteltransaktionsgeräten ist eine solche Datenübertragung schon aus Sicherheitsgründen für dazu nicht befugte Benutzer zu unterbinden, um Datenschutzerfordernisse einzuhalten und Manipulationen zu unterbinden. Bekannte Geldmitteltransaktionsgeräte können insbesondere Selbstbedienungssysteme sein, die eine Vielzahl elektronischer Komponenten umfassen. Solche Komponenten sind beispielsweise in einer Geldausgabeeinheit, einer Tastatur, einem Kartenlese- und -Schreibgerät sowie in weiteren Peripheriegeräten enthalten. Diese einzelnen Komponenten sind mit der Datenverarbeitungsanlage des Geldmitteltransaktionsgerätes über

Kommunikationsschnittstellen und Datenleitungen verbunden. Jede dieser Komponente verarbeitet und erzeugt Daten, insbesondere Betriebsprotokolle, Tracedaten und Fehlerinformationen. Üblicherweise werden diese Daten in einen Speicherbereich eines Permanentspeichers der Datenverarbeitungsanlage, insbesondere eines Festplattenspeichers der Datenverarbeitungsanlage, gespeichert. Aus vielfältigen Gründen ist es sinnvoll, diese Daten auf einer weiteren Datenverarbeitungsanlage, insbesondere zentral beim Hersteller des Geldmitteltransaktionsgerätes zu verarbeiten und dabei zu analysieren. Eine Analyse dieser Daten kann beispielsweise auch auf einem Laptop-Computer eines Servicetechnikers mit geeigneter Software durchgeführt werden. Dabei kann es erforderlich sein, diese Daten mit Hilfe eines steckbaren Flashspeichers, wie einem Flashspeicher mit einer integrierten USB-Schnittstelle, einem sogenannten USB-Stick, von der Datenverarbeitungsanlage eines Geldmitteltransaktionsgerätes zu der weiteren Datenverarbeitungsanlage, wie dem Laptop-Computer des Servicetechnikers, zu übertragen. Dazu werden die relevanten Daten von der Datenverarbeitungsanlage des Geldmitteltransaktionsgerätes in einen Speicherbereich des steckbaren Flashspeichers kopiert oder bewegt. Jedoch ist eine solche Datenübertragung bei herkömmlichen Datenverarbeitungssystemen nicht gesichert, sodass jede Bedienperson, die Zugang zur Datenverarbeitungsanlage des Geldmitteltransaktionsgerätes hat, diese Daten kopieren kann. Dadurch kann eine missbräuchliche Nutzung dieser Daten nicht ausgeschlossen werden. Ferner sollte auch beim Übertragen von in einem Speicherbereich des steckbaren Flashspeichers gespeicherten Daten zur Datenverarbeitungsanlage des Geldmitteltransaktionsgerätes sichergestellt werden, dass diese Datenübertragung nur für autorisiert Be-

nutzer gestattet ist. Gleiche Probleme treten auf, wenn anstelle des steckbaren Flashspeichers andere Wechseldatenträger genutzt werden. Auch zum Einräumen weiterer Benutzerrechte bei einer Datenverarbeitungsanlage ist eine sichere Authentifizierung eines Benutzers erforderlich, um diesem Benutzer voreingestellte Benutzerrechte einzuräumen. Diese Benutzerrechte können insbesondere das Ausführen von Anwendungsprogrammen, mit denen sicherheitsrelevante Einstellungen des Geldmitteltransaktionsgerätes geändert werden können oder die auf andere Art und Weise eine Manipulation des Geldmitteltransaktionsgerätes bewirken und/oder den sicheren Betrieb des Geldmitteltransaktionsgerätes beeinträchtigen können, verhindern.

Aufgabe der Erfindung ist es, ein System und ein Verfahren zum Authentifizieren eines Benutzers anzugeben, durch die ein Benutzer einfach und sicher authentifiziert werden kann .

Diese Aufgabe wird durch ein System mit den Merkmalen des Patentanspruchs 1 und durch ein Verfahren mit den Merkmalen des Patentanspruchs 18 gelöst. Vorteilhafte Weiterbildungen der Erfindung sind in den abhängigen Patentansprüchen angegeben .

Durch ein System mit den Merkmalen des Patentanspruchs 1 und durch ein Verfahren mit den Merkmalen des Patentanspruchs 18 ist es auf einfache Art und Weise möglich einer Bedienperson, wie beispielsweise einem Servicetechniker, in

der Datenverarbeitungsanlage voreingestellte Benutzerrechte zuzuweisen und die Bedienperson sicher als Benutzer dieser Benutzergruppe zu authentifizieren. Dadurch können nicht autorisierten Bedienpersonen insbesondere sicherheitsrelevante Bedienfunktionen nicht bereitgestellt werden. Durch die Verbindung eines Zertifikats mit dem Identifizierungscode zum Identifizieren des Wechselspeichermediums ist die Authentifizierung des Benutzers an das Vorhandensein des dem Zertifikat zugeordneten Wechselspeichermediums gebunden. Dies bietet eine relativ hohe Sicherheit beim Authentifizieren des Benutzers, sodass Zugriffe von unbefugten Benutzern auf sicherheitsrelevante Funktionen wirkungsvoll verhindert werden können. Als Wechselspeichermedium können übliche kostengünstige Wechseldatenträger, wie USB-Speichersticks und/oder Wechselfestplatten eingesetzt werden, die über die erforderlichen Identifizierungsinformationen verfügen. Das Wechselspeichermedium muss somit keinen Controller zum Ausführen eines Verwaltungsprozesses haben der digitale Zertifikate verwaltet, Zufallszahlen sowie Pseudozuf auszahlen erzeugt und Verschlüsselungen von Zufallszahlen und Daten durchführt. Ein einfaches kostengünstiges Wechselspeichermedium ohne Kontroller, wie ein einfacher Massenspeicher, mit gespeicherten Identifikationsdaten und gespeichertem Zertifikat ist somit für die Erfindung ausreichend.

Bei einer Weiterbildung der Erfindung wird der Benutzer identifiziert und der identifizierte Benutzer authentifiziert, wobei für den Benutzer und/oder für eine Benutzergruppe, zu der der Benutzer zugeordnet ist, in der Datenverarbeitungsanlage Benutzerrechte voreingestellt sind, die

durch das Authentifizieren des Benutzers für diesen Benutzer aktiviert werden. Dabei kann das Identifizieren des Benutzers ebenfalls mit Hilfe des Identifizierungscodes zum Identifizieren des Wechselspeichermediums und/oder mit Hilfe des digitalen Zertifikats, das in dem Speicherbereich des Wechselspeichermediums gespeichert ist, ermittelt werden .

Vorzugsweise ist das Zertifikat ein Attributzertifikat, wobei der Identifikationscode und/oder ein Passwort, das über eine Bedienoberfläche der Datenverarbeitungsanlage eingebbar ist, als Attribute dienen, die von einer Zertifizierungsstelle mit einem Zertifikat verbunden werden. Das Attributzertifikat verweist vorzugsweise auf das Attribut bzw. die Attribute und auf ein weiteres Zertifikat.

Ferner ist es vorteilhaft, im Speicherbereich des Wechselspeichermediums als Identifikationscode einen Herstelleridentifikationscode und einen Seriennummeridentif ikationscode zu speichern. Der Herstelleridentifikationscode und der Seriennummeridentif ikationscode sind vorzugsweise Attribute des Zertifikats.

Das Zertifikat hat vorzugsweise eine festgelegte Gültigkeitsdauer, wobei das Zertifikat mit Ablauf dieser Gültigkeitsdauer ungültig wird und von der Datenverarbeitungsanlage nicht mehr akzeptiert wird. Die Echtheit des Zertifikats sowie die Gültigkeit des Zertifikats können von der Datenverarbeitungsanlage geprüft werden, wobei nach einer

erfolgreichen Prüfung der Benutzer authentifiziert wird. Dadurch kann insbesondere ein dauerhafter Missbrauch des Wechselspeichermediums zum Authentifizieren eines Benutzers wirkungsvoll vermieden werden.

Mit Hilfe des Zertifikats kann ein öffentlicher Schlüssel eines asymmetrischen Schlüsselpaars des Benutzers zertifiziert werden, mit dessen Hilfe Daten verschlüsselt werden, die mit dem privaten Schlüssel des Schlüsselpaares entschlüsselbar sind. Vorzugsweise werden Daten, die von der Datenverarbeitungsanlage zum Wechselspeichermedium übertragen werden, vor dem Übertragen mit Hilfe des zertifizierten öffentlichen Schlüssels verschlüsselt.

Die Datenverarbeitungsanlage ist bei einem bevorzugten Ausführungsbeispiel Bestandteil eines Geldmitteltransaktionsgerätes, wobei das Geldmitteltransaktionsgerät vorzugsweise ein Geldeinzahlautomat, ein Geldauszahlautomat, ein Geldrecyclingautomat, eine automatische Tresorkasse, ein automatisches Kassensystem und/oder ein Registrierkassensystem ist.

Das Wechselspeichermedium ist vorzugsweise eine externe Festplatte und/oder ein externer Flashspeicher, wobei das Wechselspeichermedium über eine Datenleitung und vorzugsweise über eine Standardschnittstelle mit der Datenverarbeitungsanlage verbindbar ist. Die Standardschnittstelle ist vorzugsweise eine USB-Schnittstelle und der Flashspeicher ist vorzugsweise eine Speicherkarte und/oder ein

steckbarer USB-Speicher. Dadurch kann zum Authentifizieren des Benutzers ein Wechselspeichermedium genutzt werden, das einen ausreichend großen Speicherbereich aufweist, um auch große Datenmengen von der Datenverarbeitungsanlage auf das Wechselspeichermedium zu speichern als auch große Datenmengen vom Wechselspeichermedium zur Datenverarbeitungsanlage zu übertragen. Auf diese Weise lassen sich auch Daten zur Systemaktualisierung des Betriebssystems und/oder von Anwendungssoftware der Datenverarbeitungsanlage sicher übertragen .

Bei einer weiteren bevorzugten Ausführungsform der Erfindung ist erst nach einer erfolgreichen Authentifizierung des Benutzers das Übertragen von Daten von der Datenverarbeitungsanlage zum Wechselspeichermedium und/oder zum Übertragen von weiteren Daten vom Wechselspeichermedium zur Datenverarbeitungsanlage möglich. Dadurch kann die Datenübertragung verhindert werden, wenn keine Authentifizierung des Benutzers erfolgt ist, die die jeweilige Datenübertragung zulässt. Dadurch wird sowohl sichergestellt, dass sicherheitsrelevante Daten von der Datenverarbeitungsanlage nicht von nicht dazu autorisierten Bedienpersonen auf das Wechselspeichermedium übertragbar sind als auch dass ungewünschte Daten, insbesondere schädliche Programmcodes, wie Viren, nicht vom Wechselspeichermedium zur Datenverarbeitungsanlage übertragen werden.

Das Zertifikat kann bei einem Initialisierungsvorgang erstellt und in einem Speicherbereich des Wechseldatenträgers gespeichert werden. Vorzugsweise ist das Zertifikat nach

einem Standard für digitale Zertifikate erstellt, insbesondere nach dem X.509 Standard. Dieser X.509 Standard liegt zum Zeitpunkt der Anmeldung in der Version 3 vor.

Der Identifikationscode bzw. die Identifikationscodes des Wechselspeichermediums werden durch den Hersteller in einem nachträglich nicht mehr veränderbaren Speicherbereich des Wechselspeichermediums, vorzugsweise bei dessen Herstellungsprozess, als nur lesbare Daten gespeichert. Das Zertifikat kann ebenfalls in einen solchen nicht mehr veränderbaren Speicherbereich als nur lesbare Daten oder alternativ vorzugsweise in einen weiteren wiederbeschreibbaren Speicherbereich des Wechselspeichermediums gespeichert werden, der wiederbeschreibbar ist und in dem weitere Daten speicherbar sind. Bei dieser bevorzugten Ausführungsform, bei der die Daten des Zertifikats in einem weiteren wiederbeschreibbaren Speicherbereich des Wechselspeichermediums gespeichert sind, kann das Zertifikat auf einfache Art und Weise erneuert werden, indem das bestehende Zertifikat gelöscht und durch ein neues Zertifikat ersetzt wird.

Das Attributzertifikat kann einen Benutzer zum Ausführen mindestens eines Anwendungsprogramms durch die Datenverarbeitungsanlage autorisieren. Dazu kann insbesondere das Anwendungsprogramm oder ein weiteres Programmmodul überprüfen, ob eine entsprechende Autorisierung des Benutzers durch eine erfindungsgemäße Authentifizierung des Benutzers erfolgt ist und/oder beim Start des Programms eine solche Authentifizierung des Benutzers zum Autorisieren veranlassen.

Durch die Erfindung können erst nach einer erfolgreichen Prüfung der Autorisierung der Bedienperson bzw. des angemeldeten Benutzers sicherheitsrelevante Funktionen einer Anwendungssoftware oder sicherheitsrelevante Anwendungssoftware aktiviert und/oder ausgeführt werden. Insgesamt wird durch die Erfindung der Datenschutz und die Datensicherheit erhöht.

Ein Verfahren zum Authentifizieren eines Benutzers kann in gleicher Weise weitergebildet werden, wie für das System zum Authentifizieren eines Benutzers insbesondere durch die Merkmale der unabhängigen Patentansprüche angegeben ist.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung, welche in Verbindung mit den beigefügten Figuren die Erfindung anhand eines Ausführungsbeispiels näher erläutert.

Es zeigen:

Figur 1 ein Blockdiagramm mit Komponenten zum Authentifizieren eines Benutzers;

Figur 2 einen Ablauf zum Anfordern, Erzeugen und Speichern eines Zertifikats für einen Benutzer auf einem USB-Speicherstick; und

Figur 3 einen Ablauf zum Verifizieren eines auf einem USB-Speicherstick gespeicherten Zertifikats.

In Figur 1 ist ein Blockdiagramm eines Systems zum Authentifizieren eines Benutzers dargestellt, mit dessen Hilfe ein Servicetechniker als Benutzer der Benutzergruppe "Techniker" durch ein auf einem USB-Speicherstick 12 gespeichertes Zertifikat 14 von einer Datenverarbeitungsanlage authentifiziert werden kann. Der USB-Speicherstick 12 ist über eine Datenleitung 16 mit einer USB-Schnittstelle 20 der Datenverarbeitungsanlage 18 verbunden. Von der Datenverarbeitungsanlage 18 wird mit Hilfe eines Programmmoduls ein Zertifikatserver 22 nach dem Zertifikatstandard X.509 bereitgestellt. Der Zertifikatserver 22 hat Zugriff auf einen Permanentspeicherbereich 24, wie z. B. einen Festplattenspeicherbereich, in dem Zertifikate 25 gespeichert sind. Mit Hilfe der Zertifikate 25 können verschiedene auf unterschiedlichen USB-Speichersticks, USB-Festplatten oder anderen USB-Wechselspeichermedien gespeicherte Zertifikate überprüft werden. Insbesondere enthält der Permanentspeicherbereich 24 mindestens ein Zertifikat 25, auf das das im USB-Speicherstick 12 gespeicherte Zertifikat 14 verweist.

Der Servicetechniker startet über eine grafische Bedienoberfläche mindestens ein Service- und Operatinganwen-

dungsprogramm 26. Dieses Service- und Operatinganwendungsprogramm 26 übergibt eine definierte Anfrage in Form eines Textfeldes an ein CSC-W32 API-Programmmodul 28, dass eine Anwendungsschnittstelle für das Service- und Operatinganwendungsprogramm 26 und weitere Programme bereitstellt. Das CSC-W32 API-Programmmodul 28 ist ein Client, der über mindestens eine Socketverbindung 30 Dienste des X.509-Zertifikatservers 22 in Anspruch nimmt. Das CSC-W32 API-Programmmodul 28 leitet die Anfrage des Service- und Operatinganwendungsprogramms 26 an den Zertifikatserver 22 als Anfrage weiter.

Aufgrund dieser Anfrage überprüft der Zertifikatserver 22, ob der angemeldete aktuelle Benutzer als Benutzer der Benutzergruppe "Techniker" authentifiziert werden kann, indem der Zertifikatserver 22 mit Hilfe der im Permanentspeicherbereich 24 gespeicherten Zertifikate 25 überprüft, ob das Zertifikat 14 des mit der USB-Schnittstelle 20 der Datenverarbeitungsanlage 18 verbundenen USB-Speichersticks 12 gültig ist und den Benutzer tatsächlich als gültigen Benutzer der Benutzergruppe "Techniker" authentifiziert. Ergibt die Überprüfung des Zertifikatservers 22, dass das Zertifikat 14 in Verbindung mit der Seriennummer des USB-Speichersticks 12 und optional einem Passwort, dass der Servicetechniker über eine Benutzeroberfläche der Datenverarbeitungsanlage 18 eingegeben hat, authentifiziert, teilt der Zertifikatserver 22 dem CSC-W32 API-Programmmodul 28 mit, dass die Authentifizierung des Benutzers erfolgreich war und das Service- und Operatinganwendungsprogramm 26 weiter abgearbeitet werden kann bzw. eine von diesem Service- und Operatinganwendungsprogramm 26 bereitgestellte si-

cherheitsrelevante Funktion aktiviert werden kann. Bei einem ungültigen Zertifikat 14 bzw. bei einer nicht erfolgreichen Authentifizierung des Benutzers erzeugt der Zertifikatserver 22 eine entsprechende Antwort auf die Anfrage des CSC-W32 API-Programmmoduls 28, wodurch eine weitere Abarbeitung des Service- und Operatinganwendungsprogramms 26 bzw. das Bereitstellen einer sicherheitsrelevanten Funktion, das bzw. die die Überprüfung veranlasst hat, nicht aktiviert wird.

In Figur 2 ist ein Ablauf zum Anfordern, Erzeugen und Speichern eines Zertifikats 14 für einen Benutzer zum Personalisieren und Aktivieren des USB-Speichersticks 12 beispielhaft dargestellt. Gleiche Elemente haben gleiche Bezugszeichen. Wie bereits im Zusammenhang mit Figur 1 beschrieben, dient das Zertifikat 14 zum Authentifizieren eines Benutzers durch die Datenverarbeitungsanlage 18 sowie durch weitere Datenverarbeitungsanlagen. Der USB-Speicherstick 12 wird mit Hilfe einer Client-Server-Applikation für einen speziellen Benutzer, beispielsweise für den bereits erwähnten Servicetechniker, personalisiert. In einem nicht dargestellten Vorverarbeitungsschritt muss eine Beantragung der Registrierung bei einer Registrierungsstelle erfolgen. Die Registrierungsstelle kann beispielsweise vom Hersteller des Geldmitteltransaktionsgerätes bereitgestellt werden, in dem die Datenverarbeitungsanlage 18 enthalten ist.

Die Beantragung der Registrierung wird von der Zertifizierungsstelle manuell durch administrative Tätigkeit abgearbeitet und ist mit dem Freischalten eines neuen Benutzers

in einem Netzwerk vergleichbar. Der Antragsteller wird dabei als Benutzer in einer Datenbank registriert. Der Antragsteller stellt den Antrag beispielsweise per E-Mail oder per Telefon. Alternativ kann der Antrag automatisch von einem Programmmodul erzeugt werden, wenn ein Servicetechniker eingestellt worden ist und/oder ein Servicetechniker oder ein anderer Benutzer neu registriert worden ist, für den eine Autorisierung zum Aktivieren von Service- und Operatinganwendungsprogrammen und/oder anderen sicherheitsrelevanten Programmen und/oder Funktionen erfolgen soll. Daraufhin wird dieser Antrag zum Zertifizieren geprüft. Erforderlichenfalls erfolgt ein telefonischer Rückruf oder eine Kommunikation per E-Mail, um sicherzustellen, dass die Anfrage tatsächlich vom betreffenden Servicetechniker kommt. Anschließend wird überprüft, ob dem Antragsteller, d.h. dem Servicetechniker, die gewünschten Benutzerrechte zugeteilt werden können. Alternativ oder zusätzlich werden aufgrund der Stellung des Servicetechnikers im Unternehmen und seiner Funktion automatisch geeignete Benutzerrechte festgelegt, die dem Servicetechniker dann zugewiesen und durch ein Zertifikat bestätigt werden. Dem Servicetechniker werden vorzugsweise die allgemeinen Benutzerrechte der voreingestellten Benutzergruppe "Techniker" und erforderlichenfalls weitere Benutzerrechte zugewiesen.

Wird bei der Prüfung des Antrags festgestellt, dass diesem Antrag des Antragstellers stattgegeben wird und ihm entsprechende Nutzungsrechte zugewiesen werden sollen, so wird ein Stammdatensatz in einer Datenbank angelegt und ein für die Zertifizierung erforderlicher Zertifizierungsprozess durch einen Datenbankeintrag freigeschaltet. Sowohl der

Stammdatensatz als auch der Zertifizierungsprozess können auch zum Erzeugen weiterer Zertifikate für den betreffenden Servicetechniker genutzt werden.

In Figur 2 ist der Kommunikationsablauf zwischen einer Kommunikationseinrichtung 40 des Servicetechnikers, dem als Frontend 42 dienenden Callcenters der Zertifizierungsstelle und einer Datenbank 44 zum Registrieren von zu zertifizierenden und zertifizierten Benutzern dargestellt. In Schritt SO werden der Datenbank Identifizierungsinformationen von vorzugsweise mehreren Technikern übergeben, die in eine in einer Datei gespeicherte Liste mit diesen dem jeweiligen Techniker zugeordneten Informationen umfassen. Mit Hilfe dieser Identifizierungsinformationen können die Servicetechniker identifiziert werden, für die ein Zertifikat 14 ausgestellt werden darf. Diese Liste kann beispielsweise in Form einer mit dem Softwareprogramm Microsoft Excel erstellten Tabelle gespeichert und von der Datenbank 44 importiert werden.

Im Schritt Sl erfolgt eine Anforderung des Servicetechnikers, mit der er einen Antrag auf Zertifizierung stellt und eine gewünschte bzw. mit Hilfe der Identifizierungsdaten voreingestellte Benutzerrolle beantragt. Die Benutzerrolle korrespondiert mit den für eine Benutzergruppe zugewiesenen Benutzerrechten, wenn der Servicetechniker Mitglied der Gruppe werden soll. Allgemein korrespondiert die Benutzerrolle mit den dem jeweiligen Benutzer (Servicetechniker) zugewiesenen Benutzerrechten. Die Datenbank 44 erzeugt für jeden Listeneintrag der importierten Liste, d. h. für jeden

zu registrierenden Benutzer, einen separaten Datensatz. Im Schritt Sl. 1 wird vom Frontend 42 eine Anforderung an die Datenbank 44 gestellt, der Datensatz für den Servicetechniker angefordert und aus der Datenbank ausgelesen.

Die Authentizität des Servicetechnikers wird beispielsweise durch die Abfrage eines Authenifizierungscodes wie z. B. seines Geburtstags, im Schritt Sl. 1.1 festgestellt. Ferner werden die dem Servicetechniker zugewiesenen Berechtigungen im Schritt Sl. 1.2 aktiviert. Dann wird vom Frontend 42 ein Verifikationscode (vc) erzeugt. Dieser Verifikationscode wird in den Datensatz des Servicetechnikers in der Datenbank 44 eingetragen. Der Verifikationscode kann beispielsweise ein kryptografischer Wert sein, der über den Datensatz des Servicetechnikers gebildet ist. Anschließend wird im Schritt Sl. 2 der Datensatz und/oder die geänderten Daten des Datensatzes in die Datenbank 44 geschrieben. Im Schritt Sl. 3 wird dem Servicetechniker der Verifikationscode übermittelt. Dies kann beispielsweise per Telefon oder per Datenübertragung, insbesondere per E-Mail, erfolgen. Alternativ kann ihm der Verifikationscode auch postalisch zugestellt werden. Dieser Verifikationscode wird zu einem späteren Zeitpunkt zur weiteren Authetifikation des Benutzers benötigt, insbesondere um zu einem späteren Zeitpunkt ein oder mehrere Zertifikate anzufordern. Im Schritt Sl. 3.1 notiert sich der Servicetechniker der Verifikationscode bzw. speichert ihn zur weiteren Verfügung.

In Figur 3 ist ein Ablauf zum Erzeugen und Übermitteln eines Nutzerzertifikats dargestellt. Ein Zertifizierungs-

Clientanwendungsprogramm 48 wird beispielsweise auf einem Desktop-PC oder einem Notebook-Computer ausgeführt, mit dessen Hilfe ein Zertifikat bei einem Zertifizierungsserver 46 angefordert wird. Das Clientanwendungsprogramm kann beispielsweise über ein Netzwerk, wie ein Intranet oder das Internet, zum Desktop-Computer oder Notebook-Computer übertragen werden, mit dessen Hilfe das Zertifikat angefordert wird. Auf diesem Computer wird das Clientanwendungsprogramm ausgeführt. Erforderlichenfalls wird das Clientanwendungsprogramm vor dem Ausführen auf dem Computer installiert und bei den notwenigen Komponenten des Betriebssystems entsprechend registriert. Ein solches Clientanwendungsprogramm hat vorzugsweise folgende Funktionen:

- Erzeugen eines RSA-Schlüsselpaares
- Personalisieren eines Wechselspeichermediums
- eine weitere Funktion zum Nachpersonalisieren
- Passwort ändern.

Beispielsweise kann das Clientanwendungsprogramm auch eine browserbasierte und/oder eine plattformunabhängige Java-Applikation sein.

Der Zertifizierungsserver 46 ist über eine Datenverbindung mit der Datenbank 44 verbunden. Der Zertifizierungsserver 46 und die Datenbank 44 können durch verschiedene Software--

applikationen auch mit Hilfe einer einzigen Datenverarbeitungsanlage bereitgestellt werden.

Im Schritt A1 wird durch das Clientanwendungsprogramm ein Schlüsselpaar für den Servicetechniker erzeugt. Anschließend erzeugt das Clientanwendungsprogramm 48 im Schritt A2 eine Zertifizierungsanforderung. Zum Erzeugen der Anfrage wird ein Wechselspeichermedium, vorzugsweise ein USB-Speicherstick 12 des Servicetechnikers mit der Datenverarbeitungsanlage verbunden, die das Zertifizierungsclientanwendungsprogramm 48 abarbeitet. Das Zertifizierungsclientanwendungsprogramm 48 liest die Seriennummer und vorzugsweise die Hersteller-ID des Wechselspeichermediums aus und integriert diese in die Zertifizierungsanforderung. Ferner legt der Servicetechniker ein Passwort fest, das ebenfalls in die Serviceanforderung integriert wird. Diese Zertifizierungsanforderung wird im Schritt A3 vom Zertifizierungsclientanwendungsprogramm 48 zum Zertifizierungsserver 46 übertragen, der den Datensatz für den Techniker, für den das Zertifikat erstellt werden soll lädt. Ausgehend von den zum Servicetechniker in der Datenbank 44 gespeicherten Informationen wird im Schritt A3.1.1 vom Zertifikatserver 46 ein Zertifikat 14 entsprechend den für diesen Servicetechniker in der Datenbank 44 gespeicherten Berechtigungsinformationen erzeugt. Der Zertifizierungsserver 46 erzeugt im Schritt A3.1.1 ein Attributzertifikat, wobei die Seriennummer, der Hersteller-ID-Code des USB-Speichersticks, das Passwort und/oder biometrische Daten des Servicetechnikers als Attribute zum Erzeugen des Attributzertifikats dienen. Das erzeugte Attributzertifikat legt die Benutzerberechtigungen des Servicetechnikers auf einer Datenverarbeitungs-

anläge fest, wie beispielsweise auf der Datenverarbeitungsanlage, die das Clientzertifizierungsprogramm 48 abarbeitet oder auf der Datenverarbeitungsanlage des Geldmitteltransaktionsgerätes. Ferner können durch die Nutzungsrechte die Berechtigung zum Starten und Ausführen bestimmter Anwendungsprogramme und/oder sicherheitsrelevanter Funktionen dienen, wie bereits im Zusammenhang mit Figur 1 ausführlich erläutert .

Vorzugsweise umfasst die Zertifikatsanforderung auch den Verifikationscode, der dem Techniker zuvor, wie in Verbindung mit Figur 2 beschrieben, übermittelt worden ist. Alternativ kann dieser Verifikationscode in einer gesonderten Kommunikation zwischen Zertifizierungsclientanwendungsprogramm 48 und Zertifizierungsserver 46 übermittelt werden. Im Schritt A3.2. wird ein Vermerk in den Datensatz des Servicetechnikers in die Datenbank 44 geschrieben, dass ein entsprechendes Zertifikat erzeugt worden ist. Vorzugsweise wird der gesamte Datensatz des Servicetechnikers neu in die Datenbank 44 geschrieben.

Im Schritt A3.3 wird das erzeugte Zertifikat von dem Zertifizierungsserver 46 zum Zertifizierungsclientanwendungsprogramm 48 übertragen. Das Zertifikat wird vom Zertifizierungsclient 48 in einen Speicherbereich des USB-Speichersticks 12 geschrieben, der mit einer USB-Schnittstelle der Datenverarbeitungsanlage verbunden ist, die das Zertifizierungsclientanwendungsprogramm 48 abarbeitet. Das Attributzertifikat hat vorzugsweise ein Ablauf da-

tum, dass in dem im Schritt A3.1.1 erzeugten Zertifikat enthalten ist.

In der Datenbank 44 werden nach dem Erzeugen des Zertifikats Informationen des Antragstellers, d.h. des Servicetechnikers, zugelassene Benutzerrechte bzw. Benutzerrollen, das Zertifikat selbst, die Seriennummer des USB-Speichersticks 12 und/oder der aktuelle Status des Zertifikats gespeichert. Der Status kann beispielsweise "beantragt", "ausgestellt" oder "zurückgezogen" sein. Sowohl die Zertifizierungsclientapplikation 48 als auch die Zertifizierungsserverapplikation 46 können grafische Benutzeroberflächen aufweisen. Der Server hat weiterhin folgende Funktionen:

- Administration eines Schlüsselspeichers und mindestens eines Route-Zertifikates
- Administration von Benutzern
- Verarbeitung von Zertifikatsanfragen
- Protokollierung von Zertifizierungsvorgängen in der Datenbank 44.

Vorzugsweise wird mit der Anforderung des Zertifikats oder in einer gesonderten Kommunikation zumindest der öffentliche Schlüssel des im Schritt A1 erzeugten Schlüsselpaars zum Zertifizierungsserver 42 übertragen. Der übertragene Schlüssel selbst kann dem Benutzer zugeordnet oder in einem

Schlüsselspeicher der Datenbank 44 oder in einem Speicherbereich des Zertifizierungsservers 46 gespeichert werden.

Das Service- und Operatinganwendungsprogramm 26 der Datenverarbeitungsanlage 18 kann Funktionen bereitstellen, die nur dann ausgeführt werden können, wenn ein Benutzer authentifiziert wird, dem dafür erforderliche Benutzerrechte, also eine spezielle Benutzerrolle zugeordnet ist.

Das Wechselspeichermedium kann vorzugsweise auch verwendet werden, um die durch die Datenverarbeitungsanlage 18 erzeugten Log- und Tracedaten automatisch als so genanntes Bündel abzuholen. Dadurch kann sichergestellt werden, dass alle erforderlichen Log- und Tracedateien zu Auswertungszwecken auf das Wechselspeichermedium kopiert worden sind. Die Berechtigung zum Kopieren und der Kopiervorgang selbst kann automatisch mit Hilfe des auf dem Wechselspeichermedium gespeicherten Zertifikats sowie den Identifizierungsinformationen des Wechselspeichermediums überprüft und angestoßen werden.

Insbesondere werden Schreib- und Lesezugriffe auf das Wechselspeichermedium nur dann gestattet, wenn auf dem Wechselspeichermedium ein gültiges Zertifikat gespeichert ist, das einen Benutzer authentifiziert, der eine solche Schreib- und Leseberechtigung hat. Aus Sicherheitsgründen kann eine andere Schreib- und Lesemöglichkeit von und auf Wechselspeichermedien nicht zugelassen werden.

Ferner können auf dem Wechselspeichermedium Programmdaten von Service- und Anwendungsprogrammen gespeichert sein, die vorzugsweise nur dann von der Datenverarbeitungsanlage 18 ausgeführt werden können, wenn auf dem Wechselspeichermedium ein gültiges Zertifikat gespeichert ist, das zusammen mit den Identifizierungsinformationen des Wechselspeichermediums eine Berechtigung für diese Schreib- und Lesezugriffe bestätigt.

Sollen Daten auf dem Wechselspeichermedium gespeichert werden, werden diese vorzugsweise komprimiert und/oder in einer geschützten Datei gespeichert. Vorzugsweise werden die Daten mit Hilfe eines öffentlichen Schlüssels eines RSA-Schlüsselpaares verschlüsselt gespeichert.

Im Dateinamen der gespeicherten Datei kann vorzugsweise eine Seriennummer eines Geldmitteltransaktionsgerätes, in dem die Datenverarbeitungsanlage 18 angeordnet ist, enthalten sein. Die Datenverarbeitungsanlage 18 kann insbesondere ein geeigneter Personalcomputer und/oder eine geeignete Steuereinheit sein

Die Datenbank 44 ist vorzugsweise eine SQL-Datenbank, in der für jeden zu zertifizierenden und/oder zertifizierten Benutzer Name, Anschrift, Firma, Abteilung, Telefonnummer, E-Mail-Adresse, Seriennummer des Wechselspeichermediums, vergebene Zertifikate, Gültigkeit der Zertifikate, Bearbei-

ter, Datum und Status gespeichert sind. Vorzugsweise wird auch die Historie einzelner Daten erfasst, sodass Änderungen auch zu einem späteren Zeitpunkt nachvollzogen werden können. Die Datenbank 44 und/oder der Zertifizierungsserver 46 erzeugt bei folgenden Ereignissen eine Information, insbesondere schickt die Datenbank 44 und/oder der Zertifizierungsserver 46 automatisiert eine E-Mail:

- an die Zertifizierungsstelle über eingehende Anträge;
- an den Antragsteller nach Freischaltung des Antrags zur Aufforderung, die Zertifikate abzuholen;
- an den Antragsteller vor Ablauf einzelner Zertifikate als Hinweise zur Beantragung einer Verlängerung und/oder eines neuen Zertifikats und
- an den Antragsteller, wenn neue und/oder verlängerte Zertifikate vorliegen.

Durch die Verknüpfung der Seriennummer des Wechselspeichermediums, der Hersteller-ID des Wechselspeichermediums und/oder eines frei wählbaren Passworts in einem Standard X.509 Attributzertifikat können Standardwechselspeichermedien, wie USB-Wechselspeichermedien, zum Authentifizieren eines Benutzers genutzt werden, die relativ preiswert sind. Mit Hilfe dieser Benutzerauthentifizierung können Datenschutz und Datensicherheit erhöht werden.

Ansprüche

1. System zum Authentifizieren eines Benutzers,

mit einem Wechselspeichermedium (12), das mindestens einen Speicherbereich aufweist, in dem Identifizierungsdaten zum Identifizieren des Wechselspeichermediums (12) gespeichert sind, wobei in diesem Speicherbereich oder in einem weiteren Speicherbereich des Wechselspeichermediums (12) Daten eines digitalen Zertifikats (14) gespeichert sind,

mit einer Datenverarbeitungsanlage (18), mit der das Wechselspeichermedium (12) über eine Datenübertragungsverbindung verbunden ist,

wobei die Identifizierungsdaten und die Daten des digitalen Zertifikats (14) vom Wechselspeichermedium (12) zur Datenverarbeitungsanlage (18) übertragen werden, und

wobei die Datenverarbeitungsanlage (18) die Identifikationsdaten und die Daten des digitalen Zertifikats verarbeitet und den Benutzer authentifiziert.

2. System nach Anspruch 1, dadurch gekennzeichnet, dass der Benutzer identifiziert und der identifizierte Benutzer authentifiziert wird, und dass für den Benutzer und/oder eine Benutzergruppe, zu der der Benutzer zugeordnet ist, Rechte voreingestellt sind, die durch das Authentifizieren des Benutzers für diesen Benutzer aktiviert werden.

3. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Benutzer durch die Eingabe eines Benutzernamens, durch die Seriennummer des Wechseldatenträgers (12) und/oder das Zertifikat (14) identifiziert wird.

4. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Zertifikat (14) ein Attributzertifikat ist, wobei die Identifikationsdaten und/oder ein Passwort als Attribute dienen, die von einer Zertifizierungsstelle (44, 46) mit einem Zertifikat (14) verbunden werden, wobei das Attributzertifikat vorzugsweise auf das Attribut bzw. die Attribute und auf ein weiteres Zertifikat verweist.

5. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Datenverarbeitungsanlage (18) die Gültigkeit und/oder Echtheit des Zertifikats (14) prüft.

6. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass mit Hilfe des Zertifikats (14) ein öffentlicher Schlüssel eines asymmetrischen Schlüsselpaars des Benutzers zertifziert ist, mit dessen Hilfe Daten verschlüsselt werden, die mit dem privaten Schlüssel des Schlüsselpaars entschlüsselbar sind, wobei Daten von der Datenverarbeitungsanlage (18) zum Wechselspeichermedium (12) vorzugsweise mit Hilfe des zertifizierten öffentlichen Schlüssels verschlüsselt übertragen werden.

7. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass im Speicherbereich des Wechselspeichermediums (12) als Identifikationsdaten Herstelleridentifikationsdaten und ein Seriennummerinformationscode gespeichert sind, wobei die Herstelleridentifikationsdaten und der Seriennummerinf ormationscode vorzugsweise Attribute des Zertifikats (14) sind.

8. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Datenverarbeitungsanlage (18) Bestandteil eines Geldmitteltransaktionsgerätes ist, wobei das Geldmitteltransaktionsgerät vorzugsweise ein Geldeinzahlautomat, ein Geldauszahlautomat, ein Geldrecyclingautomat, ein automatisches Kassensystem und/oder ein Registrierkassensystem ist.

9. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Zertifikat (14) eine

festgelegte Gültigkeitsdauer hat und dass das Zertifikat (14) mit Ablauf der Gültigkeitsdauer ungültig wird und von der Datenverarbeitungsanlage (18) nicht mehr akzeptiert wird.

10. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Wechselspeichermedium (12) eine externe Festplatte und/oder ein externer Flashspeicher ist, wobei das Wechselspeichermedium (12) über eine Datenleitung, vorzugsweise über eine Standardschnittstelle (20), mit der Datenverarbeitungsanlage (18) verbindbar ist, wobei die Standardschnittstelle (20) vorzugsweise eine USB-Schnittstelle und der Flashspeicher vorzugsweise eine Speicherkarte und/oder ein steckbarer USB-Speicher ist.

11. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass erst nach einer erfolgreichen Authentifizierung des Benutzers das Übertragen von Daten von der Datenverarbeitungsanlage (18) zum Wechselspeichermedium (12) und/oder das Übertragen von weiteren Daten vom Wechselspeichermedium (12) zur Datenverarbeitungsanlage (18) ermöglicht werden.

12. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Zertifikat (14) bei einem Initialisierungsvorgang erstellt und in dem und/oder einem weiteren Speicherbereich des Wechseldatenträgers (12) gespeichert wird.

13. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Zertifikat (14) nach einem Standard für digitale Zertifikate erstellt ist, vorzugsweise nach dem X.509 Standard, insbesondere in dessen aktueller Version 3.

14. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Identifikationsdaten durch den Hersteller in einen nachträglich nicht mehr veränderbaren Speicherbereich des Wechselspeichermediums (12), vorzugsweise beim dessen Herstellungsprozess, als nur lesbare Daten gespeichert werden, und dass die Daten des Zertifikats in einem weiteren wiederbeschreibbaren Speicherbereich des Wechselspeichermediums (12) gespeichert sind, in dem weitere Daten speicherbar sind.

15. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Attributzertifikat den Benutzer zum Ausführen mindestens eines Anwendungsprogramms (26) durch die Datenverarbeitungsanlage (18) autorisiert .

16. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Datenverarbeitungsanlage (18) prüft, ob der Benutzer zum Aktivieren einer durch ein Programm der Datenverarbeitungsanlage (18)

bereitgestellten Funktion autorisiert ist und erst nach einer erfolgreichen Überprüfung die Funktion durch die Datenverarbeitungsanlage (18) aktiviert und/oder ausgeführt wird.

17. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine Registrierungsinstanz eine Anfrage nach einem Zertifikat verarbeitet und die Anfrage prüft, wobei nach positiver Prüfung ein Prozess zur Zertifizierung gestattet wird.

18. Verfahren zum Authentifizieren eines Benutzers,

bei dem in mindestens einem Speicherbereich eines Wechselspeichermediums (12) Identifizierungsdaten zum Identifizieren des Wechselspeichermediums (12) gespeichert sind,

in dem Speicherbereich oder in einem weiteren Speicherbereich des Wechselspeichermediums (12) Daten eines digitalen Zertifikats (14) gespeichert sind,

die Identifizierungsdaten und die Daten des digitalen Zertifikats aus dem Speicherbereich des Wechselspeichermediums (12) ausgelesen und über eine Datenüber-

tragungsverbindung zu einer Datenverarbeitungsanlage (18) übertragen werden, und

bei dem mit Hilfe der Datenverarbeitungsanlage (18) die Identifikationsdaten und die Daten des digitalen Zertifikats (14) verarbeitet und zum Authentifizieren des Benutzers genutzt werden.

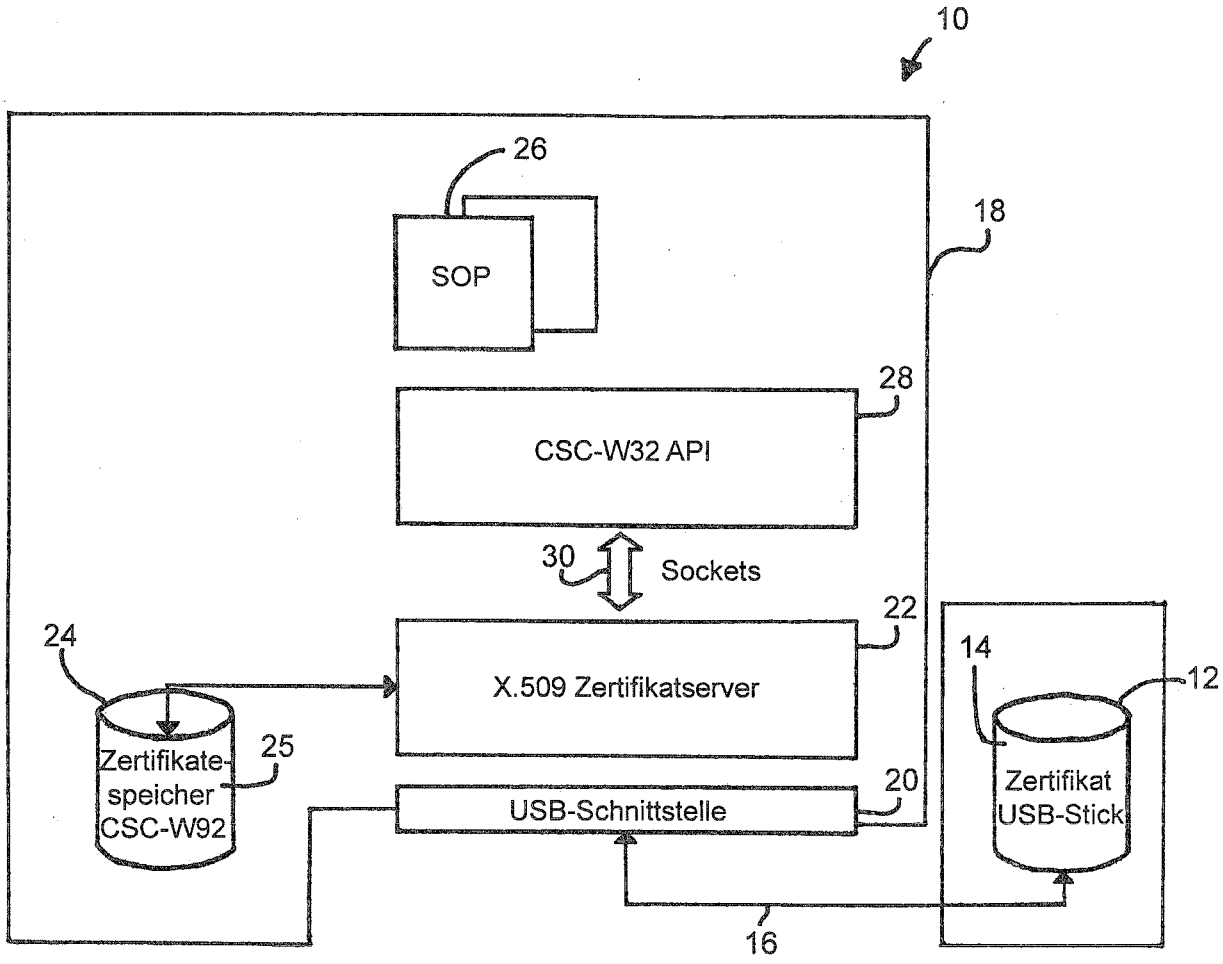
10
26
SOP
18
28
CSC-W32 API
30
Sockets
22
X.509 Zertifikatserver
24
Zertifikate-
speicher
CSC-W92
25
20
USB-Schnittstelle
14
12
Zertifikat
USB-Stick
16

Fig. 1

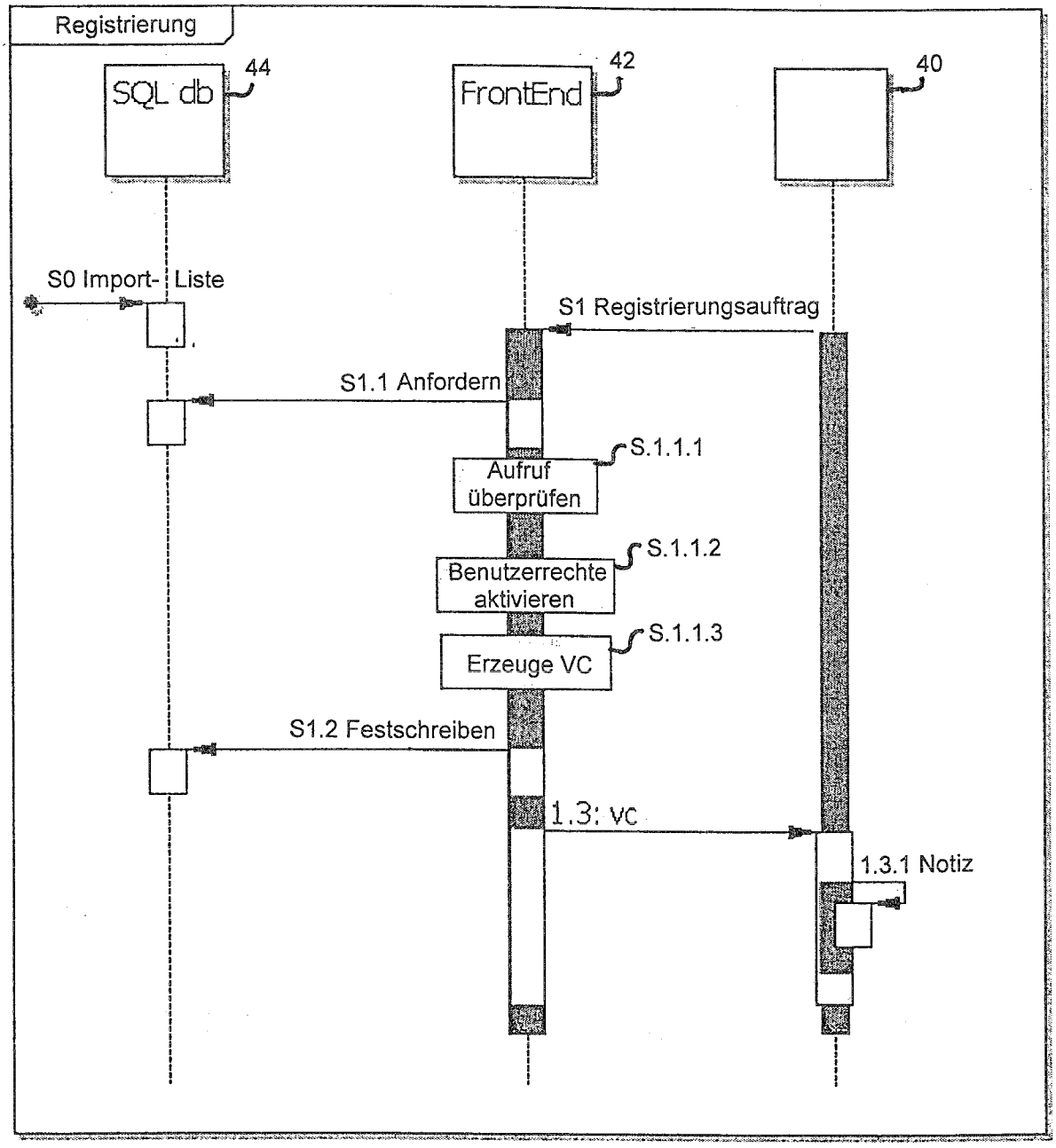
Registrierung
SQL db
44
FrontEnd
42
40
S0 Import- Liste
S1 Registrierungsauftrag
S1.1 Anfordern
S.1.1.1
Aufruf überprüfen
S.1.1.2
Benutzerrechte aktivieren
S.1.1.3
Erzeuge VC
S1.2 Festschreiben
1.3: VC
1.3.1 Notiz

Fig. 2

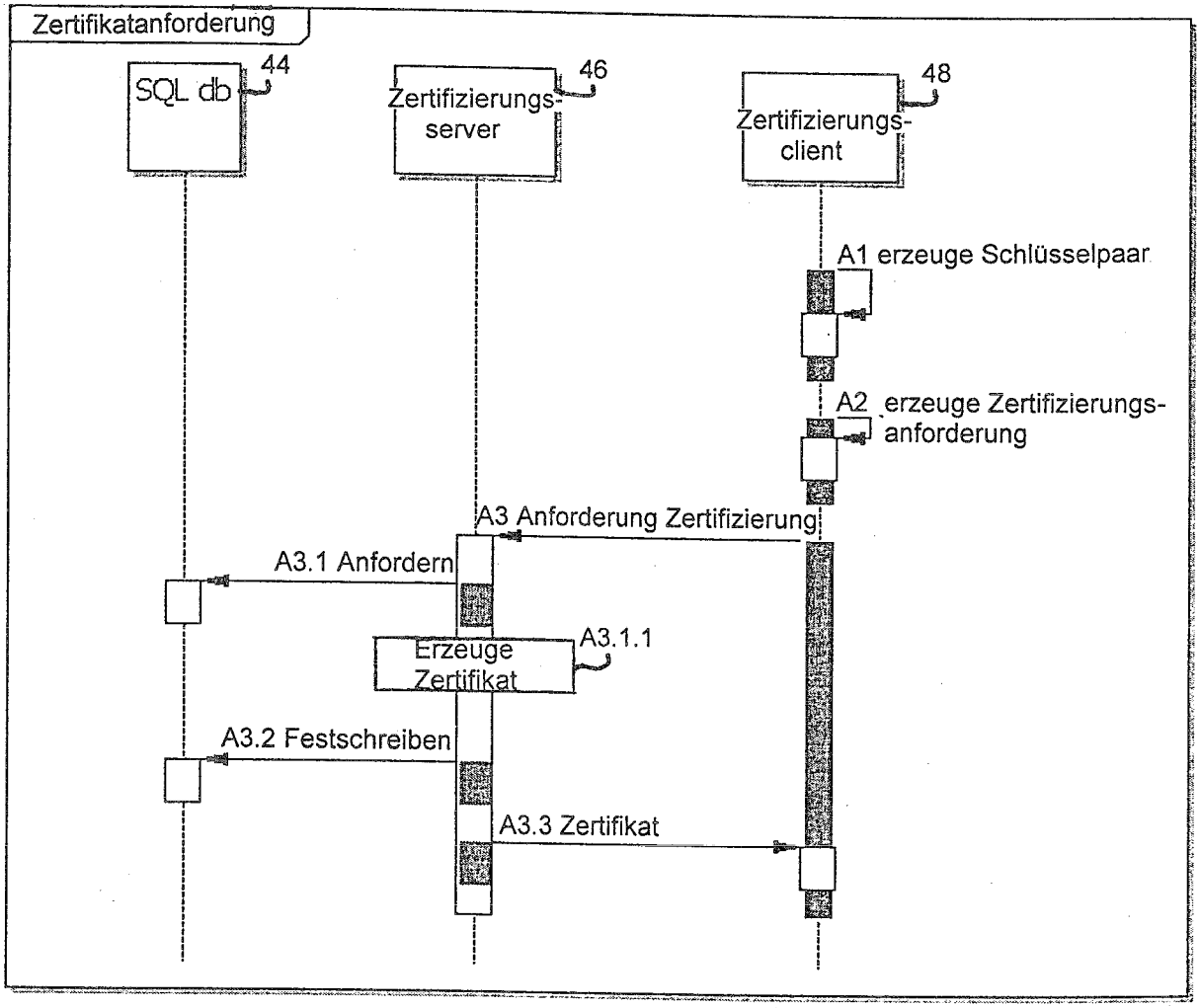
Zertifikatanforderung
SQL db
44
Zertifizierungs-server
46
Zertifizierungs-client
48
A1 erzeuge Schlüsselpaar
A2 erzeuge Zertifizierungs-anforderung
A3 Anforderung Zertifizierung
A3.1 Anfordern
Erzeuge Zertifikat
A3.1.1
A3.2 Festschreiben
A3.3 Zertifikat

Fig. 3

INTERNATIONAL SEARCH REPORT

International appllcation No
PCT/EP2008/054999

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

Accordingio International Patent Classification (IPC) orto both national Classification and IPC

B. FIELDS SEARCHED

Minimum documentallön searcned (Classification System followed by Classification Symbols)
G06F

Docume ntation searched other than mlnimum documentatlon 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 , WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category"	Citation of document, with indication, where appropnate, of the relevant passages	Relevant Io Claim No.
Y	US 2004/064708 Al (ANGELO MICHAEL F [US] ET AL) 1 April 2004 (2004-04-01) abstract figuxes 2,4 paragraphs [0004], [0017], [0-30]	1-18
Y	US 2006/234797 Al (DAVIS HEDLEY C [US] ET AL) 19 October 2006 (2006-10-19) abstract	1-18
A	USB IMPLEMENTERS FORUM: "Universal Serial Bus Mass Storage Class" 19990930, 30 September 1999 (1999-09-30), XP002489594 page 9 - , page 10	1-18

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

'A" document defming the general State of the art which Is not considered to be of particular relevance

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

'L1 document which may throw doubts on priority daim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O* document reterring 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 prin Cple or theory undertying 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 docu¬ments, 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 August 2008	01/09/2008

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/054999

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document with indication, where appropriate, of the relevant passages	Relevant to Claim No
A	BALL E ET AL: "Role-based access control with X.509 attribute certificates" IEEE INTERNET COMPUTING, IEEE SERVICE CENTER, NEW YORK, NY, US, vol. 7, no. 2, 1 March 2003 (2003-03-01), pages 62-69, XP011095972 ISSN: 1089-7801 page 63 - page 66	4,15,16
A	US 6 968 459 B1 (MORGAN JEFFREY A [US] ET AL) 22 November 2005 (2005-11-22) abstract figure 2 columns 1,3,4	6
A	"Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks; X.509 (08/05)" ITU-T STANDARD IN FORCE (I), INTERNATIONAL TELECOMMUNICATION UNION, GENEVA, CH, no. X.509 (08/05), 29 August 2005 (2005-08-29), XP017405086 page 62 - page 67	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/054999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004064708 **A1**	01-04-2004	**NONE**	
US 2006234797 **A1**	19-10-2006	**EP** 1869821 **A2**	26-12-2007
		KR 20080005497 **A**	14-01-2008
		WO 2006113160 **A2**	26-10-2006
US 6968459 B1	22-11-2005	**NONE**	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2008/054999

A.. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/00

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, **WPI Data**

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 2004/064708 Al (ANGELO MICHAEL F [US] ET AL) 1. April 2004 (2004-04-01) Zusammenfassung Abbildungen 2,4 Absätze [0004], [0017], [0-30]	1-18
Y	US 2006/234797 Al (DAVIS HEDLEY C [US] ET AL) 19. Oktober 2006 (2006-10-19) Zusammenfassung	1-18
A	USB IMPLEMENTERS FORUM: "Universal Serial Bus Mass Storage Class" 19990930, 30. September 1999 (1999-09-30), XP002489594 Seite 9 - Seite 10.	1-18

-/--

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

* Besondere Kategorien von angegebenen Veröffentlichungen :
'A' Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
'E' älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
'L' Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
'P' Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
'T' Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
'X' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
'&' Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
11. August 2008	01/09/2008

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

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2008/054999

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr Anspruch Nr
A	**BALL E ET AL: "Role-based access control with X.509 attribute certificates"** **IEEE INTERNET** COMPUTING, **IEEE SERVICE** CENTER, **NEW** YORK, NY, US, **Bd.** 7, **Nr.** 2, 1. **März 2003** (2003-03-01), **Seiten** 62-69, **XP011095972** **ISSN: 1089-7801** **Seite 63 - Seite 66**	4,15,16
A	**US 6 968 459 Bl (MORGAN JEFFREY A [US] ET AL) 22. November 2005 (2005-11-22)** **Zusammenfassung** **Abbildung 2** Spalten 1,3,4	6
A	**"Information technology - Open Systems Interconnection - The Directory:** Public-key **and attribute certificate främeworks; X.509 (08/05)"** **ITU-T STANDARD IN FORCE (I), INTERNATIONAL TELECOMMUNICATION** UNION, GENEVA, CH, **Nr.** **X.509** (08/05), **29. August 2005** (2005-08-29), **XP017405086** **Seite 62 - Seite 67**	**1-18**

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2008/054999

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2004064708 **A1**	01-04-2004	**KEINE**	
US 2006234797 **A1**	19-10-2006	EP 1869821 **A2**	26-12-2007
		KR 20080005497 **A**	14-01-2008
		WO 2006113160 A2	26-10-2006
US 6968459 **B1**	22-11-2005	**KEINE**	