(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 601 05 326 T2** 2005.09.22

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 117 207 B1**
(21) Deutsches Aktenzeichen: **601 05 326.5**
(96) Europäisches Aktenzeichen: **01 300 224.1**
(96) Europäischer Anmeldetag: **11.01.2001**
(97) Erstveröffentlichung durch das EPA: **18.07.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **08.09.2004**
(47) Veröffentlichungstag im Patentblatt: **22.09.2005**

(51) Int Cl.[7]: **H04L 9/32**

(30) Unionspriorität:
483356 **14.01.2000** **US**

(73) Patentinhaber:
Hewlett-Packard Development Co., L.P., Houston, Tex., US

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler & Zinkler, 82049 Pullach

(84) Benannte Vertragsstaaten:
DE, FR, GB

(72) Erfinder:
Corella, Francisco, Hayward, California 94541, US

(54) Bezeichnung: **Infrastruktur für öffentliche Schlüssel**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf Öffentlicher-Schlüssel-Kryptosysteme und insbesondere auf eine leichte Öffentlicher-Schlüssel-Infrastruktur, die kurzfristige Einmalzertifikate für Authentifizierung und/oder Autorisierung verwendet.

[0002] Öffentlicher-Schlüssel-Kryptosysteme werden weltweit im World Wide Web verwendet, und auch bei einer wachsenden Anzahl von Firmennetzwerken, für die Einrichtung sicherer Kommunikationskanäle. Jeder Nutzer in einem Öffentlicher-Schlüssel-Kryptosystem hat ein Paar von Schlüsseln, einschließlich einem öffentlichen Schlüssel und einem privaten Schlüssel. Der öffentliche Schlüssel wird anderen Benutzern offenbart, während der private Schlüssel geheimgehalten wird. Ein Öffentlicher-Schlüssel-Kryptosystem hat typischerweise eine bestimmte Hauptverwendung, wie z. B. für Verschlüsselung, digitale Signatur oder Schlüsselübereinstimmung. Öffentlicher-Schlüssel-Kryptosysteme werden auch für Benutzerauthentifizierung verwendet. Beispielsweise kann sich ein Benutzer selbst für andere Benutzer authentifizieren durch Nachweisen seiner Kenntnis seines privaten Schlüssels, den andere Benutzer unter Verwendung des entsprechenden öffentlichen Schlüssels verifizieren können.

[0003] Bei einer Anwendung eines Öffentlicher-Schlüssel-Kryptosystems zum Authentifizieren eines Benutzers muss der öffentliche Schlüssel der Identität des Benutzers sicher zugeordnet sein, der den öffentlichen Schlüssel besitzt, durch Authentifizieren des öffentlichen Schlüssels selbst. Typischerweise werden Öffentlicher-Schlüssel-Zertifikate verwendet, um den öffentlichen Schlüssel zu authentifizieren. Ein Öffentlicher-Schlüssel-Zertifikat ist ein digitales Dokument, das durch eine Zertifikatautorität unterzeichnet ist, das einen öffentlichen Schlüssel mit einem oder mehreren Attributen verbindet, die den Besitzer des öffentlichen Schlüssels eindeutig identifizieren. Das Öffentlicher-Schlüssel-Zertifikat kann unter Verwendung des öffentlichen Schlüssels der Zertifikatautorität verifiziert werden, von dem angenommen wird, dass es gut bekannt ist oder rekursiv durch eine höhere Autorität zertifiziert. Beispielsweise kann in einer Firma ein Öffentlicher-Schlüssel-Zertifikat einen öffentlichen Schlüssel mit einer Angestelltennummer verbinden.

[0004] Eine Öffentlicher-Schlüssel-Infrastruktur (PKI = public key infrastructure) bezieht sich auf die Sammlung von Entitäten, Datenstrukturen und Prozeduren, die verwendet werden, um öffentliche Schlüssel zu authentifizieren. Eine traditionelle PKI umfasst eine Zertifikatautorität, Öffentlicher-Schlüssel-Zertifikate und Prozeduren zum Verwalten und Verwenden der Öffentlicher-Schlüssel-Zertifikate.

[0005] Ein Typ eines Benutzers einer PKI besitzt den öffentlichen Schlüssel, der in einem Öffentlicher-Schlüssel-Zertifikat enthalten ist und verwendet das Zertifikat, um die Identität des Benutzers nachzuweisen. Dieser Typ von Benutzer wird als das Subjekt des Zertifikats bezeichnet oder allgemeiner als das Subjekt. Ein weiterer Typ von Benutzer verlässt sich auf ein Öffentlicher-Schlüssel-Zertifikat, das durch einen anderen Benutzer präsentiert wird, um zu verifizieren, dass der andere Benutzer das Subjekt des Zertifikats ist und dass die Attribute, die in dem Zertifikat enthalten sind, für den anderen Benutzer gelten. Dieser Typ von Benutzer, der sich auf das Zertifikat verlässt, wird als ein Verifizierer oder eine Vertrauenspartei bezeichnet.

[0006] Die Zuordnung zwischen einem öffentlichen Schlüssel und einer Identität kann ungültig werden, wenn die Attribute, die die Identität definieren, nicht mehr für den Besitzer des öffentlichen Schlüssels gelten, oder weil der öffentliche Schlüssel, der dem öffentlichen Schlüssel entspricht, beeinträchtigt wurde. Eine PKI verwendet typischerweise zwei komplementäre Techniken zum Trennen eines öffentlichen Schlüssels von einer Identität. Bei der ersten Technik hat jeder öffentliche Schlüssel jedes Öffentlicher-Schlüssel-Zertifikat eine Gültigkeitsperiode, die durch ein Ablaufdatum definiert ist, das eine wesentliche Periode von dem Ausgabedatum entfernt ist, wie z. B. ein Jahr ab dem Ausgabedatum. Bei der zweiten Technik hebt die Zertifikatautorität ein Öffentlicher-Schlüssel-Zertifikat auf, falls die Bindung des Öffentlicher-Schlüssel-Zertifikats vor dem Ablaufdatum ungültig wird. Eine Möglichkeit zum Aufheben eines Öffentlicher-Schlüssel-Zertifikats ist das Aufnehmen einer Seriennummer des Öffentlicher-Schlüssel-Zertifikats in eine Zertifikat-Aufhebungsliste (CRL = certificate revocation list), die durch die Zertifikatautorität in bekannten regelmäßigen Intervallen, wie z. B. alle paar Stunden oder einmal am Tag, unterzeichnet und ausgegeben wird. Eine Entität, die sich auf ein Zertifikat verlässt, ist verantwortlich für das Erhalten der neuesten Version der CRL und für das Verifizieren, dass die Seriennummer des Öffentlicher-Schlüssel-Zertifikats nicht auf der Liste ist.

[0007] CRLs werden typischerweise sehr schnell sehr lang. Wenn die CRLs lang werden, ist die Leistungsfähigkeit stark beeinträchtigt. Zunächst verbraucht die CRL-Wiedergewinnung große Mengen an Netzwerkbandbreite. Zweitens muss jede Anwendung die CRL regelmäßig wiedergewinnen, die CRL syntaktisch analysieren und Speicher für die CRL zuweisen. Dann muss die Anwendung eine lineare Suche der CRL durchführen, nach der Öffentlicher-Schlüssel-Zertifikat-Seriennummer, wenn die Anwendung jedes Öffentlicher-Schlüssel-Zertifikat verifiziert. Als Folge steigen herkömmliche PKIs nicht über einige tausend Benutzer an.

[0008] Eine Lösung, die vorgeschlagen wurde, um das lineare Suchproblem zu lindern, ist das Unterteilen der CRLs. Die Seriennummer des Öffentlicher-Schlüssel-Zertifikats bestimmt, wo die CRL-Unterteilung positioniert ist, wenn das Öffentlicher-Schlüssel-Zertifikat aufgehoben wird. Mit unterteilten CRLs muss die Anwendung nach wie vor die gesamte CRL wiedergewinnen und speichern, oder andernfalls muss die Anforderung eine CRL-Unterteilung abrufen, um ein Zertifikat zu verifizieren. Da eine Zertifikats-Verifizierung ein wahrscheinlich kritischer Weg ist, beeinträchtigt das Abrufen einer CRL-Unterteilung die Zeit, die benötigt wird, um die Anwendung auszuführen.

[0009] Ein On-Line-Zertifikat-Statusprotokoll (OCSP; OCSP = online certificate status protocol) arbeitet, indem es dem Verifizierer des Öffentlicher-Schlüssel-Zertifikat ermöglicht, die Zertifikatautorität zu fragen, ob das Zertifikat aktuell gültig ist. Die Zertifikatautorität antwortet mit einer unterzeichneten Erklärung. Die OCSP ermöglicht es, dass CRLs umgangen werden, erfordert jedoch, dass der Verifizierer die Zertifikatautorität abfragt, als Teil der Transaktion, die die Öffentlicher-Schlüssel-Zertifikate verwendet. Der Verifizierer, der die Zertifikatautorität abfragt, erhöht die Zeit, die notwendig ist, um die Transaktion durchzuführen. Das OCSP-Schema ist stark anfällig für einen Dienstverweigerungsangriff, bei dem der Angreifer die Zertifikatautorität mit Abfragen überflutet. Das Antworten auf jede Abfrage ist rechentechnisch aufwendig, weil jede Antwort eine digitale Signatur erfordert.

[0010] Bei einem Zertifikat-Statusbeweisschema behält die Zertifikatautorität eine Datenstruktur bei, die den Satz von gültigen und ungültigen Zertifikaten in dem Verzeichnis beschreibt. Für jedes Öffentlicher-Schlüssel-Zertifikat, das noch nicht abgelaufen ist, kann ein kurzer kryptographischer Beweis von der Datenstruktur des aktuellen Status des Zertifikats (d. h. gültig oder ungültig) extrahiert werden. Eine CRL kann im wesentlichen als ein kryptographischer Beweis der Ungültigkeit für die Öffentlicher-Schlüssel-Zertifikate in der CRL gesehen werden, und ein Beweis für die Gültigkeit für diejenigen, die nicht in der CRL sind. Die CRL ist jedoch kein kurzer Beweis. Der kurze kryptographische Beweis kann durch den Verifizierer von dem Verzeichnis erhalten werden, oder derselbe kann durch das Subjekt erhalten werden und dem Verifizierer zusammen mit dem Öffentlicher-Schlüssel-Zertifikat präsentiert werden.

[0011] Die SPKI-Arbeitsgruppe (SPKI = Simple Public Key Infrastructure = einfache Öffentlicher-Schlüssel-Infrastruktur) der Internetgesellschaft (Internet Society) und der Internetarbeitsgruppe (Internet Engineering Task Force) hat die Möglichkeit vorgeschlagen, kurzlebige Zertifikate als ein Verfahren zum Erreichen einer dichten Steuerung über das Gültigkeitsintervall eines Zertifikats zu erhalten. Siehe C.M. Ellison, B. Frantz, B. Lampson, R. Rivest, B.M. Thomas and T. Ylonen, SPKI Certificate Theory, Request for Comments 2560 of the Internet Engineering Task Force, September 1999. Die SPKI-Zertifikats-Theorie-Referenz gibt an, dass es Fälle gibt, in denen ein kurzlebiges Zertifikat weniger Signaturen und weniger Netzwerkverkehr erfordert als verschiedene On-Line-Testoptionen. Die Verwendung eines kurzlebigen Zertifikats erfordert immer weniger Signaturverifizierungen als die Verwendung eines Zertifikats plus On-Line-Testergebnis.

[0012] Die internationale Patentanmeldung von Hur u. a., internationale Veröffentlichungs-Nr. WO99/35783 offenbart ein Clientseiten-Öffentlicher-Schlüssel-Authentifizierungsverfahren und eine Vorrichtung mit kurzlebigen Zertifikaten. Die Patentanmeldung von Hur u. a. offenbart ein Schlüsselverteilungszentrum, das das Privater/Öffentlicher-Schlüssel-Paar des Benutzers in Zusammenhang mit einem Identifizierer des Benutzers speichert und auf Anforderung kurzlebige Zertifikate ausgibt, die den öffentlichen Schlüssel des Benutzers zertifizieren und neu zertifizieren. Gemäß diesem Schema muss der Benutzer das Privater/Öffentlicher-Schlüssel-Paar mit dem Schlüsselverteilungszentrum gemeinsam verwenden, was das Senden des privaten Schlüssels des Benutzers über das Netzwerk umfasst. Damit ein solches gemeinschaftlich verwendetes Schlüssel-Paar-Paradigma praktisch ist, muss dasselbe Sicherheitsprobleme adressieren, die sich auf das Übertragen des privaten Schlüssels des Benutzers über das Netzwerk beziehen.

[0013] Das U.S.-Patent 5,982,898 von Hsu u. a. offenbart einen Zertifizierungsprozess, der eine Registrierungsautorität mit einer Zertifizierungsautorität kombiniert, die kurzlebige Zertifikate für einen Benutzer ausgibt. Die Registrierungsautorität prüft den Identitätsbeweis des Benutzers zum Bestätigen, dass der Benutzer vertrauenswürdig ist, und gibt dann ein Passwort für den Benutzer aus, das es dem Benutzer ermöglicht, auf die Zertifizierungsautorität zuzugreifen. Wenn der vertrauenswürdige Benutzer ein kurzlebiges Zertifikat von einer Zertifizierungsautorität wünscht, müssen der Benutzer und die Zertifizierungsautorität einen Passwortverifizierungsprozess abschließen. Als nächstes schreitet die Zertifizierungsautorität fort, um das kurzlebige Zertifikat zu entwickeln und zu unterzeichnen. Die Verwendung von Passwortschutz zum Zugreifen auf die Zertifizierungsautorität und dass die Zertifizierungsautorität das kurzlebige Zertifikat entwickeln muss, erhöhen die Komplexität des Authentifizierungsprozesses und können einen Engpass in dem Zertifizierungsprozess erzeugen.

[0014] Trotzdem wurde kein praktisches Verfahren zum Ausgeben kurzlebiger Zertifikate vorgeschla-

gen. Traditionelle Zertifikate werden off-line erstellt, als Teil eines Prozesses, der Subjektregistrierung umfasst, bei der Geschwindigkeit von einem pro Jahr pro Benutzer. Im Gegensatz dazu müssten kurzlebige Zertifikate on-line bei einer Geschwindigkeit von zumindest einem pro Tag pro Benutzer ausgegeben werden, und vielleicht auch so oft wie alle paar Minuten für jeden Benutzer.

[0015] Der Begriff On-Line und der Begriff Off-Line haben im Zusammenhang einer PKI bestimmte Definitionen. Der Begriff On-Line bezieht sich hierin auf die alltägliche Verwendung von Öffentlicher-Schlüssel-Zertifikaten und Schlüsselpaaren für Authentifizierung. Der Begriff Off-Line bezieht sich hierin auf die weniger häufige Herstellung oder Auflösung von Öffentlicher-Schlüssel-Bindungen, die zu dem Ausgeben oder Aufheben von Öffentlicher-Schlüssel-Zertifikaten führen kann. Beispielsweise ist die traditionelle Zertifikatautorität off-line, erteilt CRLs off-line und platziert die CRLs in ein Verzeichnis für eine On-Line-Wiedergewinnung. Das Schema, das Zertifikat-Statusbeweise umfasst, verwendet auch Off-Line-Zertifikatautoritäten. Das OCSP ist das einzige Schema, das oben beschrieben wurde, das eine On-Line-Zertifikatautorität verwendet.

[0016] Aus oben genannten Gründen und aus anderen Gründen, die bei der Beschreibung des bevorzugten Ausführungsbeispiels der vorliegenden Beschreibung näher präsentiert sind, gibt es einen Bedarf an einer verbesserten leichten PKI, die die oben beschriebenen Aufhebungsprobleme überwindet und effizient weit mehr als einige tausend Benutzer aufnehmen kann, und die für Authentifizierung und/oder Autorisierung verwendet werden kann.

[0017] Die vorliegende Erfindung liefert eine Öffentlicher-Schlüssel-Infrastruktur (PKI), die ein Subjekt, eine Off-Line-Registrierungsautorität, einen On-Line-Berechtigungsnachweisserver und einen Verifizierer aufweist. Die Registrierungsautorität gibt ein erstes nichtunterzeichnetes Zertifikat off-line an das Subjekt aus, das einen öffentlichen Schlüssel des Subjekts an langfristige Identifikationsinformationen bindet, die sich auf das Subjekt beziehen. Die Registrierungsautorität behält eine Zertifikatdatenbank von nicht-unterzeichneten Zertifikaten bei, in der dieselbe das erste nicht-unterzeichnete Zertifikat speichert. Der Berechtigungsnachweisserver gibt ein kurzfristiges Einmalzertifikat on-line an das Subjekt aus. Das kurzfristige Einmalzertifikat bindet den öffentlichen Schlüssel des Subjekts von dem ersten nicht-unterzeichneten Zertifikat an die langfristigen Identifikationsinformationen, die sich auf das Subjekt des ersten nichtunterzeichneten Zertifikats beziehen. Der Berechtigungsnachweisserver behält eine Tabelle bei, die Einträge enthält, die gültigen, nicht-unterzeichneten Zertifikaten entsprechen, die in der Zertifikatdatenbank gespeichert sind.

[0018] Das Subjekt präsentiert das kurzfristige Einmalzertifikat dem Verifizierer für eine Authentifizierung und zeigt, dass das Subjekt Kenntnis eines privaten Schlüssels hat, der dem öffentlichen Schlüssel in dem kurzfristigen Einmalzertifikat entspricht.

[0019] Fig. 1 ist ein Blockdiagramm einer leichten Öffentlicher-Schlüssel-Infrastruktur (PKI) gemäß der vorliegenden Erfindung, die kurzfristige Einmalzertifikate verwendet.

[0020] Fig. 2 ist ein Diagramm eines nicht-unterzeichneten Zertifikats, das von einer Registrierungsautorität der PKI von Fig. 1 ausgegeben wurde.

[0021] Fig. 3 ist ein Flussdiagramm eines Off-Line-Protokolls zum Ausgeben eines nicht-unterzeichneten Zertifikats von einer Registrierungsautorität der PKI von Fig. 1.

[0022] Fig. 4 ist ein Diagramm eines nicht-strukturierten kurzfristigen Einmalzertifikats, wie es durch den Berechtigungsnachweisserver des PKI von Fig. 1 ausgegeben wird.

[0023] Fig. 5 ist ein Flussdiagramm, das ein On-Line-Protokoll zum Ausgeben eines kurzfristigen Einmalzertifikats von einem Berechtigungsnachweisserver der PKI von Fig. 1 darstellt.

[0024] Fig. 6 ist ein Flussdiagramm, das ein On-Line-Protokoll für ein Subjekt darstellt, zum Nachweisen seiner Identität an einen Verifizierer der PKI von Fig. 1.

[0025] Fig. 7 ist ein Flussdiagramm, das ein Protokoll für eine Registrierungsautorität darstellt, zum Aufheben eines nicht-unterzeichneten Zertifikats für den PKI von Fig. 1.

[0026] Fig. 8 ist ein Blockdiagramm einer leichten PKI, die kurzfristige Einmalzertifikate für eine Autorisierung gemäß der vorliegenden Erfindung verwendet.

[0027] Fig. 9 ist ein Diagramm eines strukturierten kurzfristigen Einmalzertifikats, wie es durch einen Berechtigungsnachweisserver der PKI von Fig. 8 ausgegeben wird.

[0028] Fig. 10 ist ein Flussdiagramm, das ein On-Line-Protokoll zum Ausgeben eines strukturierten kurzfristigen Einmalzertifikats von einem Berechtigungsnachweisserver der PKI von Fig. 8 darstellt.

[0029] Fig. 11 ist ein Flussdiagramm, das ein On-Line-Protokoll darstellt, das durch ein Subjekt verwendet wird, um seine Identität einem Verifizierer der PKI von Fig. 8 nachzuweisen.

[0030] Fig. 12 ist ein Blockdiagramm einer verteilten Zertifikatautorität mit verteilten Berechtigungsnachweisservern gemäß der vorliegenden Erfindung.

[0031] Fig. 13 ist eine PKI für Webserver-Zertifikatsanwendungen gemäß der vorliegenden Erfindung.

[0032] Fig. 14 ist ein Flussdiagramm, das ein Protokoll für Webserver-Zertifikatsanwendungen für die PKI von Fig. 13 darstellt.

[0033] Fig. 15 ist ein Blockdiagramm einer Unternehmens-PKI gemäß der vorliegenden Erfindung.

[0034] Fig. 16 ist ein Flussdiagramm, das ein Autorisierungs-Protokoll für die Unternehmens-PKI von Fig. 17 darstellt.

[0035] Fig. 17 ist ein Blockdiagramm eines Computersystems und eines entsprechenden computerlesbaren Mediums, das ein oder mehrere Hauptsoftware-Programmkomponenten einer PKI gemäß der vorliegenden Erfindung umfasst.

[0036] Bei der folgenden detaillierten Beschreibung der bevorzugten Ausführungsbeispiele wird auf die beiliegenden Zeichnungen Bezug genommen, die einen Teil derselben bilden, und in der durch die Darstellung spezifische Ausführungsbeispiele gezeigt sind, in denen die Erfindung praktiziert werden kann. Es ist klar, dass andere Ausführungsbeispiele verwendet werden können und strukturelle oder logische Änderungen durchgeführt werden können, ohne von dem Schutzbereich der vorliegenden Erfindung abzuweichen. Die folgende detaillierte Beschreibung ist daher nicht in beschränkendem Sinne zu sehen und der Schutzumfang der vorliegenden Erfindung ist durch die angehängten Ansprüche definiert.

[0037] Eine leichte Öffentlicher-Schlüssel-Infrastruktur (PKI) gemäß der vorliegenden Erfindung ist allgemein bei **30** in Fig. 1 dargestellt. Die PKI **30** umfasst mehrere Hauptkomponenten, die jeweils ein Softwareprogramm sind. Die Hauptsoftware-Programmkomponenten der PKI **30** laufen auf einem oder mehreren Computersystemen. Bei einem Ausführungsbeispiel läuft jede der Hauptsoftware-Programmkomponenten auf ihrem eigenen Computersystem.

[0038] Eine Zertifikatautorität **32** gibt kurzfristige Einmalzertifikate an ein oder mehrere Subjekte aus, wie z. B. das Subjekt **34**. Das Subjekt **34** ist ein Benutzer, der einen öffentlichen Schlüssel besitzt, der in dem kurzfristigen Einmalzertifikat enthalten ist und verwendet das kurzfristige Einmalzertifikat, um die Identität des Subjekts einem oder mehreren Verifizierern, wie z. B. dem Verifizierer **36**, nachzuweisen, durch Nachweisen, dass das Subjekt Kenntnis eines privaten Schlüssels hat, der dem öffentlichen Schlüssel in dem kurzfristigen Einmalzertifikat entspricht. Der Verifizierer **36** ist ein Benutzer, der sich auf das kurzfristige Einmalzertifikat verlässt, das durch das Subjekt **34** präsentiert wird, um zu verifizieren, dass das Subjekt **34** das Subjekt des kurzfristigen Einmalzertifikats ist und dass die Attribute, die in dem kurzfristigen Einmalzertifikat enthalten sind, für das Subjekt **34** gelten. Bei einigen Ausführungsbeispielen der PKI **30** kann der gleiche Benutzer in unterschiedlichen Situationen die Rolle des Subjekts **34** und des Verifizierers **36** spielen.

[0039] Die PKI **30** gibt keine traditionellen langfristigen Zertifikate aus, wie sie z. B. durch herkömmliche PKIs ausgegeben werden. Traditionelle langfristige Zertifikate haben typischerweise eine Gültigkeitsperiode, die durch ein Ablaufdatum definiert ist, das eine wesentliche Periode von dem Ausgabedatum entfernt ist, wie z. B. ein Jahr ab dem Ausgabedatum. Eine herkömmliche Zertifikatautorität muss ein traditionelles langfristiges Zertifikat aufheben, falls die Bindung des Öffentlicher-Schlüssel-Zertifikats vor dem Ablaufdatum ungültig wird. Wie es in der Beschreibungseinleitung der vorliegenden Beschreibung erörtert wird, wurden eine Vielzahl von Verfahren verwendet, um traditionelle langfristige Zertifikate aufzuheben, wie z. B. durch Verwenden einer Zertifikats-Aufhebungsliste (CHL) oder eines On-Line-Zertifikats-Statusprotokolls (OCSP).

[0040] Im Gegensatz zu traditionellen langfristigen Zertifikaten sind die kurzfristigen Einmalzertifikate, die durch die Zertifikatautorität **32** gemäß der vorliegenden Erfindung ausgegeben werden, keiner Aufhebung unterworfen. Die kurzfristigen Einmalzertifikate werden als einmalig bezeichnet, weil das Subjekt **34** dieselben nach einigen Benutzungen wegwerfen kann. Als Folge werden bei einem Ausführungsbeispiel der vorliegenden Erfindung die kurzfristigen Einmalzertifikate in einem flüchtigen Speicher gespeichert und nicht auf einer Platte gespeichert. Die PKI **30** wird als eine leichte PKI bezeichnet, weil dieselbe wesentlich einfacher und effizienter ist als eine herkömmliche PKI.

[0041] Ein kurzfristiges Einmalzertifikat ist hierin definiert als ein Öffentlicher-Schlüssel-Zertifikat, das den öffentlichen Schlüssel des Subjekts an einen oder mehrere Namen oder Identifizierer bindet und eine kurze Gültigkeitsperiode hat, die durch ein Ablaufdatum/-zeit bestimmt ist. Eine beispielhafte Gültigkeitsperiode für ein kurzfristiges Einmalzertifikat ist ein Tag, einige Stunden oder sogar einige wenige Minuten. Da die Gültigkeitsperiode recht kurz ist, ist eine Aufhebung nicht notwendig. Das Subjekt **34** fordert nach Bedarf ein neues kurzfristiges Einmalzertifikat an, und legt es dem Verifizierer **36** vor. Der Verifizierer **36** muss nur das Ablaufdatum/-zeit prüfen,

um zu verifizieren, dass das kurzfristige Einmalzertifikat gültig ist.

[0042] Aus der Sicht des Verifizierers **36** ist die Verwendung von kurzfristigen Einmalzertifikaten ein viel besseres Schema als das Verwenden traditioneller langfristiger Zertifikate, weil der Verifizierer **36** nur eine Signatur des kurzfristigen Einmalzertifikats verifizieren muss und das Ablaufdatum/-zeit des kurzfristigen Einmalzertifikats prüfen muss. Da die Zertifikatvalidierungsarbeit des Verifizierers **36** höchstwahrscheinlich ein kritischer Weg bei der Gesamtarbeit des Verifizierers **36** ist, sind kurzfristige Einmalzertifikate eine gute Lösung für den Verifizierer. In vielen Fällen ist der Verifizierer ein Leistungsfähigkeitsengpass und somit sind kurzfristige Einmalzertifikate eine gute Gesamtlösung für die PKI **30**.

[0043] Die Zertifikatautorität **32** umfasst eine Registrierungsautorität **38**, die eine Zertifikatdatenbank (DB) **40** beibehält, die nicht-unterzeichnete Zertifikate enthält. Die Zertifikatautorität **32** umfasst auch einen Berechtigungsnachweisserver **42**, der eine Hash-Tabelle (HAT) **44** beibehält, die kryptographische Hash-Werte von nicht-unterzeichneten Zertifikaten enthält.

[0044] Die Registrierungsautorität **38** ist eine Off-Line-Komponente der Zertifikatautorität **32** und ist verantwortlich für Subjektregistrierung und für das Beibehalten einer Zertifikatdatenbank **40**. Jedes nicht-unterzeichnete Zertifikat in einer Zertifikatdatenbank **40** bindet einen öffentlichen Schlüssel eines Subjekts an ein oder mehrere Attribute, die das Subjekt eindeutig identifizieren.

[0045] Der Berechtigungsnachweisserver **42** ist eine On-Line-Komponente der Zertifikatautorität **32** und ist verantwortlich für das Ausgeben der kurzfristigen Einmalzertifikate und für das Beibehalten der Liste von kryptographischen Hash-Werten von aktuell gültigen nicht-unterzeichneten Zertifikaten in der Hash-Tabelle **44**. Jeder kryptographische Hash-Wert in der Hash-Tabelle **44** wird von einem nichtunterzeichneten Zertifikat berechnet, unter Verwendung einer vereinbarten kollisionsresistenten Hash-Funktion, wie z. B. SHA-1 oder MD5. Die Hash-Tabelle **44** ist im wesentlichen eine Liste der aktuell gültigen nicht-unterzeichneten Zertifikate, die durch den kryptographischen Hash-Wert mit einem Schlüssel versehen wird. Kryptographische Hash-Werte funktionieren gut als Schlüssel für die Hash-Tabelle **44**, weil sich kryptographische Hash-Werte statistisch als Zufallsgrößen verhalten.

[0046] Das Subjekt **34** hat einen privaten Schlüssel **46**, der in einem sicheren Speichermedium **48** gespeichert ist, wie z. B. einer Smartcard oder einer sicheren Softwaretasche. Das Subjekt **34** hat auch einen öffentlichen Schlüssel, der mathematisch dem privaten Schlüssel **46** zugeordnet ist. Das Subjekt **34** registriert den öffentlichen Schlüssel, der dem privaten Schlüssel **46** entspricht, bei der Registrierungsautorität **38**, durch Senden des öffentlichen Schlüssels und eines oder mehrerer Attribute, die die Identität des Subjekts **34** eindeutig identifizieren, an die Registrierungsautorität **38** und Nachweisen, dass die Identifikations-Attribute für das Subjekt **34** gelten. Beispiele solcher Identifikationsattribute umfassen den Namen, die Sozialversicherungsnummer und die Angestelltennummer.

[0047] Die Komponenten der PKI **30** sind durch ein oder mehrere Computernetzwerke verbunden. Eine Netzwerkverbindung **50** koppelt den Berechtigungsnachweisserver **42** und das Subjekt **34**. Eine Netzwerkverbindung **52** koppelt das Subjekt **34** und den Verifizierer **36**. Netzwerkverbindungen **50** und **52** sind in Fig. 1 als durchgezogene Linien gezeigt und werden für On-Line-Kommunikation verwendet. Eine Netzwerkverbindung **54** koppelt die Registrierungsautorität **38** und das Subjekt **34**. Eine Netzwerkverbindung **56** koppelt die Registrierungsautorität **38** und den Berechtigungsnachweisserver **42**. Netzwerkverbindungen **54** und **56** sind in Fig. 1 als gestrichelte Linien dargestellt und werden für Off-Line-Kommunikation verwendet. Die Registrierungsautorität **38** ist nur bei Off-Line-Kommunikation beteiligt und kommuniziert durch Off-Line-Netzwerkverbindungen **54** und **56**. Andererseits ist der Berechtigungsnachweisserver **42** durch die Netzwerkverbindung **50** bei der On-Line-Kommunikation beteiligt.

[0048] Ein Ausführungsbeispiel eines nicht-unterzeichneten Zertifikats, das durch die Registrierungsautorität **38** ausgegeben wird, ist in Fig. 2 allgemein bei **60** dargestellt. Das nicht-unterzeichnete Zertifikat **60** umfasst ein Metadaten- (MD-) Feld **61**, das Daten über nicht- unterzeichnete Zertifikate **60** selbst anstatt Daten enthält, die sich auf das Subjekt beziehen. Beispiele von Daten, die in dem Metadatenfeld **61** gespeichert sind, umfassen Seriennummer und Ausgebername. Das nicht-unterzeichnete Zertifikat **60** umfasst einen öffentlichen Schlüssel (PK) **62** des Subjekts. Das nicht-unterzeichnete Zertifikat **60** umfasst ein Langfristige-Identifikationsinformationen- (LTI-) Feld **63**, das Attribute enthält, die das Subjekt **34** eindeutig identifizieren, wie z. B. den Namen des Subjekts, die Sozialversicherungsnummer des Subjekts oder die Angestelltennummer des Subjekts.

[0049] Das nicht-unterzeichnete Zertifikat **60** umfasst optional ein Langfristiger-Ablauf- (EXP-) Feld **64**, das ein Datum/eine Zeit des Ablaufs für das nicht-unterzeichnete Zertifikat **60** enthält. Das Ablaufdatum/-zeit, die in dem Langfristiger-Ablauf-Feld **64** enthalten ist, ist für Verwaltungszwecke sinnvoll, aber ist für eine ordnungsgemäße Funktion der PKI **30** nicht erforderlich. Im Gegensatz dazu ist bei einer herkömmlichen PKI das Ablaufdatum erforderlich,

um die Größe der CRL zu reduzieren, wenn aufgehobene Zertifikate ihre Ablaufdaten erreichen. Das nicht-unterzeichnete Zertifikat **60** umfasst optional ein Dauer- (DUR-) Feld **65**, das eine Dauer für die Gültigkeitsperiode aller kurzfristigen Einmalzertifikate spezifiziert, die für das nichtunterzeichnete Zertifikat **60** ausgegeben wurden.

[0050] Ein Off-Line-Protokoll zum Ausgeben eines nichtunterzeichneten Zertifikats **60** von der Registrierungsautorität **38** ist in Fig. 3 allgemein bei **100** dargestellt. Bei Schritt **102** sendet das Subjekt **34** seinen öffentlichen Schlüssel und ein oder mehrere Attribute, die das Subjekt **34** eindeutig identifizieren, an die Registrierungsautorität **38**.

[0051] Bei Schritt **103** demonstriert das Subjekt **34** Kenntnis des privaten Schlüssels **46**, der dem öffentlichen Schlüssel des Subjekts **34** zugeordnet ist. Schritt **103** wird auf eine Weise durchgeführt, die von dem Kryptosystem abhängt, für das das Privater-Öffentlicher-Schlüssel-Paar durch das Subjekt **34** erzeugt wurde. Beispielsweise weist das Subjekt **34** bei einem digitalen Signaturkryptosystem Kenntnis des privaten Schlüssels **46** nach durch Verwenden des privaten Schlüssels **46** zum digitalen Unterzeichnen einer Menge, die von einer Zufallsmenge abgeleitet wird, die durch die Registrierungsautorität **38** erzeugt wird. Die Registrierungsautorität **38** verifiziert dann diese digitale Signatur unter Verwendung des öffentlichen Schlüssels des Subjekts **34**.

[0052] Bei Schritt **104** weist das Subjekt **34** der Registrierungsautorität **38** durch eine Außerbandverwaltungs-Einrichtung nach, dass die Identifikations-Attribute, die in Schritt **102** gesendet werden, für das Subjekt **34** gelten.

[0053] Bei Schritt **106** erzeugt die Registrierungsautorität **38** ein nicht-unterzeichnetes Zertifikat **60** und speichert das nicht-unterzeichnete Zertifikat **60** in der Zertifikatdatenbank **40**. Bei Schritt **108** sendet die Registrierungsautorität **38** das nicht-unterzeichnete Zertifikat **60** an das Subjekt **34**.

[0054] Bei Schritt **110** berechnet die Registrierungsautorität **38** einen kryptographischen Hash-Wert des nicht-unterzeichneten Zertifikats **60** unter Verwendung einer vereinbarten kollisionsresistenten Hash-Funktion, wie z. B. SHA-1 oder MD5. Bei Schritt **110** sendet die Registrierungsautorität **38** den berechneten kryptographischen Hash-Wert des nichtunterzeichneten Zertifikats **60** an den Berechtigungsnachweisserver **42** über die Netzwerkverbindung **56**, die Datenintegritätsschutz liefert, wie z. B. mit einer SSL-Verbindung (SSL = Secure Sockets Layer = Sicherheitssockelschicht).

[0055] Bei Schritt **112** speichert der Berechtigungsnachweisserver **42** den kryptographischen Hash-Wert des nichtunterzeichneten Zertifikats **60**, das in Schritt **110** berechnet wird, in der Hash-Tabelle **44**.

[0056] Ein Ausführungsbeispiel eines kurzfristigen Einmalzertifikats, wie es durch den Berechtigungsnachweisserver **42** ausgegeben wird, ist in Fig. 4 allgemein bei **70** dargestellt. Das kurzfristige Einmalzertifikat **70** umfasst ein Metadaten- (MD-) Feld **71**, das Daten über das kurzfristige Einmalzertifikat **70** enthält, anstatt über das Subjekt des kurzfristigen Einmalzertifikats **70**. Das kurzfristige Einmalzertifikat **70** umfasst einen öffentlichen Schlüssel (PK) **72**, der der gleiche öffentliche Schlüssel ist wie der öffentliche Schlüssel **62** des nicht-unterzeichneten Zertifikats **60**. Das Subjekt des nicht-unterzeichneten Zertifikats **60** und des kurzfristigen Einmalzertifikats **70** hat nur ein Privater-Öffentlicher-Schlüssel-Paar, das dem privaten Schlüssel **46** zugeordnet ist, der in der Smartcard oder der sicheren Softwaretasche **48** gespeichert ist. Das kurzfristige Einmalzertifikat **70** umfasst ein Langfristige-Identifikationsinformationen-(LTI-) Feld **73**, das Attribute enthält, die das Subjekt **34** eindeutig identifizieren. Das Langfristige-Identifikationsinformationen-Feld **73** ist identisch mit dem Langfristige-Identifikationsinformatione-Feld **63** des nicht-unterzeichneten Zertifikats **60**.

[0057] Das kurzfristige Einmalzertifikat **70** umfasst auch ein Kurzfristiger-Ablauf- (EXP-) Feld **76**, das ein Datum und eine Zeit des Ablaufs für ein kurzfristiges Einmalzertifikat **70** spezifiziert. Bei einem Ausführungsbeispiel, bei dem das nicht-unterzeichnete Zertifikat **60** ein Dauerfeld **65** enthält, das eine Dauer für die Gültigkeitsperiode der kurzfristigen Einmalzertifikate spezifiziert, die von demselben ausgegeben werden, werden das Datum und die Zeit, die durch das Kurzfristiger-Ablauf-Feld **56** spezifiziert sind, erhalten durch Hinzufügen der Dauer, die durch das Dauerfeld **65** spezifiziert wird, zu dem Datum und der Zeit, zu dem das kurzfristige Einmalzertifikat **70** durch den Berechtigungsnachweisserver **42** ausgegeben wird. Bei einem Ausführungsbeispiel ist die Dauer der Gültigkeitsperiode des kurzfristigen Einmalzertifikats **70** nicht explizit spezifiziert durch ein Dauerfeld **65** in dem nichtunterzeichneten Zertifikat **60**. Bei diesem Ausführungsbeispiel ist die Dauer der Gültigkeitsperiode des kurzfristigen Einmalzertifikats **70** durch eine Richtlinie festgelegt.

[0058] Das kurzfristige Einmalzertifikat **70** umfasst auch ein Signaturfeld **77**, das eine Signatur eines Berechtigungsnachweisservers **42** enthält. Die Signatur in dem Signaturfeld **77** wird hergestellt durch den Bezugnachweisserver **42** auf der Sequenz der Felder **71**, **72**, **73** und **76** und auch, falls notwendig, der Spezifikation des Kryptosystems, das verwendet wurde, um die Signatur zu erzeugen, und verwendet werden muss, um die Signatur zu verifizieren.

[0059] Bei einem Ausführungsbeispiel ist das kurzfristige Einmalzertifikat **70** mit einem X.509v3-Zertifikat implementiert.

[0060] Ein On-Line-Protokoll zum Ausgeben eines kurzfristigen Einmalzertifikats **70** an das Subjekt **34** von dem Berechtigungsnachweisserver **42** für das nicht-unterzeichnete Zertifikat **60** ist in Fig. 5 allgemein bei **200** dargestellt. Bei Schritt **202** sendet das Subjekt **34** eine Mitteilung an den Berechtigungsnachweisserver **42**, die das nichtunterzeichnete Zertifikat **60** enthält und anfordert, dass ein kurzfristiges Einmalzertifikat für das nichtunterzeichnete Zertifikat **60** ausgegeben wird.

[0061] Bei Schritt **204** berechnet der Berechtigungsnachweisserver **42** einen kryptographischen Hash-Wert des nichtunterzeichneten Zertifikats **60** durch die vereinbarte kollisionsresistente Hash-Funktion. Bei Schritt **204** verifiziert der Berechtigungsnachweisserver **42** dann, dass der berechnete kryptographische Hash-Wert in der Hash-Tabelle **44** vorliegt. Bei Schritt **206** erzeugt der Berechtigungsnachweisserver **42** das kurzfristige Einmalzertifikat **70** und sendet das kurzfristige Einmalzertifikat **70** an das Subjekt **34**.

[0062] Bei Schritt **204** führt der Berechtigungsnachweisserver **42** den Nachschlag in der Hash-Tabelle **44** mit einer effizienten und rechentechnisch unaufwendigen Operation durch. Die Signaturoperation, die durch den Berechtigungsnachweisserver **42** in Schritt **206** durchgeführt wird, um das kurzfristige Einmalzertifikat **70** zu erzeugen, ist jedoch eine rechentechnisch aufwendige Operation. Trotzdem wird der Schritt **206** mit der rechentechnisch aufwendigen Signatur-Operation nur durchgeführt, falls der Nachschlag in der Hash-Tabelle **44** erfolgreich ist. Die Auswirkung eines Dienstverweigerungsangriffs gegen den Berechtigungsnachweisserver **42** ist reduziert, indem der Schritt **206** nur durchgeführt wird, falls der Nachschlag in Schritt **204** erfolgreich ist.

[0063] Ein On-Line-Protokoll, das durch das Subjekt **34** verwendet wird, um dem Verifizierer **36** seine Identität nachzuweisen, ist allgemein bei **300** in Fig. 6 dargestellt. Bei Schritt **302** sendet das Subjekt **34** das ausgegebene kurzfristige Einmalzertifikat **70** an den Verifizierer **36**. Bei Schritt **304** verifiziert der Verifizierer **36**, dass das Ablaufdatum und die Ablaufzeit, die in dem kurzfristigen Ablauffeld **76** des kurzfristigen Einmalzertifikats **70** spezifiziert sind, nicht erreicht wurden.

[0064] Bei Schritt **306** verwendet der Verifizierer **36** einen öffentlichen Schlüssel des Berechtigungsnachweisservers **42** zum Verifizieren der Signatur in dem Signaturfeld **77** des kurzfristigen Einmalzertifikats **70**. Der Verifizierer **36** kennt den öffentlichen Schlüssel des Berechtigungsnachweisservers **42** entweder direkt oder durch die Zertifizierung durch eine höhere Zertifikatautorität.

[0065] Bei Schritt **308** weist das Subjekt **34** die Kenntnis des privaten Schlüssels **46** nach, der dem öffentlichen Schlüssel **72** zugeordnet ist, der in dem kurzfristigen Einmalzertifikat **70** enthalten ist. Schritt **308** wird auf eine Weise durchgeführt, die von dem Kryptosystem abhängt, für das das private/öffentliche Schlüssel-Paar durch das Subjekt **34** erzeugt wurde. Beispielsweise weist das Subjekt **34** bei einem digitalen Signaturkryptosystem Kenntnis des privaten Schlüssels **46** nach durch Verwenden des privaten Schlüssels **46** zum digitalen Unterzeichnen einer Menge, die von einer Zufallsmenge abgeleitet wird, die durch den Verifizierer **36** erzeugt wird. Der Verifizierer **36** verifiziert dann die digitale Signatur unter Verwendung des öffentlichen Schlüssels **72** in dem kurzfristigen Einmalzertifikat **70**.

[0066] Das Subjekt **34** kann das kurzfristige Einmalzertifikat **70** löschen, wenn das kurzfristige Einmalzertifikat abläuft, weil das Subjekt **34** ein neues kurzfristiges Einmalzertifikat erhalten kann durch Senden des nicht-unterzeichneten Zertifikats an den Berechtigungsnachweisserver **42**. Bei einem Ausführungsbeispiel speichert das Subjekt **34** das kurzfristige Einmalzertifikat in dem flüchtigen Speicher und speichert es nicht auf Platte.

[0067] Ein Off-Line-Protokoll zum Aufheben des nichtunterzeichneten Zertifikats **60** ist allgemein bei **400** in Fig. 7 dargestellt. Das Off-Line-Protokoll **400** wird durchgeführt, wenn der private Schlüssel **46** des Subjekts **34** verfälscht ist oder die Identifikations-Attribute in dem Langfristige-Identifikationsinformationen-Feld **63** nicht mehr für das Subjekt **34** gelten, weil in jedem Fall das Binden des öffentlichen Schlüssels **62** an die Identifikations-Attribute ungültig ist.

[0068] Bei Schritt **402** gewinnt die Registrierungsautorität **38** das nicht-unterzeichnete Zertifikat **60** von der Zertifikatdatenbank **40** wieder und berechnet einen kryptographischen Hash-Wert des nicht-unterzeichneten Zertifikats **60** unter Verwendung der vereinbarten kollisionsresistenten Hash-Funktion. Bei einem Ausführungsbeispiel markiert die Registrierungsautorität **38** das nicht-unterzeichnete Zertifikat **60** in der Zertifikatdatenbank **40** als ungültig für Prüfungszwecke. Bei einem alternativen Ausführungsbeispiel, wo die Beibehaltung des nicht-unterzeichneten Zertifikats **60** in der Zertifikatdatenbank **40** für Prüfungszwecke nicht erforderlich ist, löscht die Registrierungsautorität **38** das nichtunterzeichnete Zertifikat **60** von der Zertifikatdatenbank **40**.

[0069] Bei Schritt **404** sendet die Registrierungsautorität **38** eine Mitteilung an den Berechtigungsnachweisserver **42**, die den kryptographischen Hash-Wert

des nicht-unterzeichneten Zertifikats **60** enthält, der in Schritt **402** berechnet wird. Die Mitteilung, die in Schritt **404** gesendet wird, erfordert auch, dass der Berechtigungsnachweisserver **42** den entsprechenden kryptographischen Hash-Wert des nichtunterzeichneten Zertifikats **60** von der Hash-Tabelle **44** entfernt.

[0070] Bei Schritt **406** entfernt der Berechtigungsnachweisserver **42** den kryptographischen Hash-Wert des nicht-unterzeichneten Zertifikats **60** von der Hash-Tabelle **44**, was dem kryptographischen Hash-Wert entspricht, der in der Mitteilung von der Registrierungsautorität **38** in Schritt **404** gesendet wurde. Nachdem Schritt **406** abgeschlossen ist, gibt der Berechtigungsnachweisserver **42** keine kurzfristigen Einmalzertifikate **70** für das nicht-unterzeichnete Zertifikat **60** mehr aus. Sobald das Protokoll **40** ausgeführt wurde, kann folglich weder das Subjekt **34** noch ein Angreifer ein kurzfristiges Einmalzertifikat erhalten, indem er das nichtunterzeichnete Zertifikat **60** dem Berechtigungsnachweisserver **42** präsentiert.

[0071] Ein alternatives Ausführungsbeispiel einer leichten PKI gemäß der vorliegenden Erfindung ist allgemein bei **30'** in Fig. 8 dargestellt. Die Komponenten **32'**, **34'**, **36'**, **38'**, **40'** , **42'** , **44'** , **46'** , **48'** , **50'** , **52'** , **54'** und **56'** der PKI **30'** arbeiten im wesentlichen gleich und sind im allgemeinen wesentlich gleich gekoppelt wie die entsprechenden Komponenten **32**, **34**, **36**, **38**, **40**, **42**, **44**, **46**, **48**, **50**, **52**, **54** und **56** der PKI **30**, die oben beschrieben sind.

[0072] Die PKI **30'** umfasst jedoch ein Verzeichnis **90**. Bei einem Ausführungsbeispiel ist das Verzeichnis **90** ein leichtes Verzeichniszugriffsprotokoll- (LDAP-) Verzeichnis. Die PKI **30'** umfasst auch eine Netzwerkverbindung **92** zum Koppeln des Berechtigungsnachweisservers **42'** mit dem Verzeichnis **90**, um es dem Berechtigungsnachweisserver **42'** zu ermöglichen, auf das Verzeichnis **90** zuzugreifen. Der Berechtigungsnachweisserver **42'** erhält kurzfristige Autorisierungs-Informationen, die in dem Verzeichnis **90** gespeichert sind. Der Berechtigungsnachweisserver **42'** fügt die kurzfristigen Autorisierungs-Informationen, die von dem Verzeichnis **90** erhalten werden, den kurzfristigen Einmalzertifikaten hinzu, die durch den Berechtigungsnachweisserver **42'** ausgegeben werden, um kurzfristige Berechtigungsnachweiszertifikate zu erzeugen, die für die Autorisierung des Subjekts **34'** verwendet werden können.

[0073] Die kurzfristigen Autorisierungsinformationsdaten, die in dem Verzeichnis **90** enthalten sind, beziehen sich auf Attribute oder Autorisierungs-Informationen über das Subjekt **34'**. Beispielhafte kurzfristige Autorisierungs-Informationen umfassen die Kostenautorisierungsgrenze für eine Firmenanwendung, die Mitfinanzierungsmenge für eine Versicherungsanwendung, die Plattenspeicherquote für eine Informationstechnologie- (IT-) Anwendung, und Benutzer-ID plus Gruppen-ID für Unix-Zugriffsanwendungen.

[0074] Bei der PKI **30'** ist der Verifizierer **36'** ein Anwendungsprogramm, das auf einem Servercomputersystem läuft und das Subjekt **34'** ist ein Clientprogramm, das die Anwendung verwendet.

[0075] Nicht-unterzeichnete Zertifikate, die durch die Registrierungsautorität **38'** ausgegeben werden, sind im wesentlichen ähnlich wie die nicht-unterzeichneten Zertifikate, die durch die Registrierungsautorität **38** ausgegeben werden, wie z. B. das nicht-unterzeichnete Zertifikat **60** von Fig. 2.

[0076] Die PKI **30'** verwendet das Off-Line-Protokoll **100**, das in Fig. 3 dargestellt ist, zum Ausgeben des nichtunterzeichneten Zertifikats **60** von der Registrierungsautorität **38**. Außerdem verwendet die PKI **30'** das in Fig. 7 dargestellte Off-Line-Protokoll **400** für die Registrierungsautorität **38'** zum Aufheben des nicht-unterzeichneten Zertifikats **60**.

[0077] Ein Ausführungsbeispiel eines strukturierten kurzfristigen Einmalzertifikats, das durch den Berechtigungsnachweisserver **42** ausgegeben wird, ist in Fig. 9 allgemein bei **80** dargestellt. Das kurzfristige Einmalzertifikat **80** ist ein strukturiertes Zertifikat.

[0078] Das strukturierte kurzfristige Einmalzertifikat **80** umfasst ein Metadaten- (MD-) Feld **81**, einen öffentlichen Schlüssel (PK) **82**, ein Kurzfristiger-Ablauf-Feld **86** und ein Signaturfeld **87**, die im wesentlichen ähnlich sind wie das Metadatenfeld **71**, der öffentliche Schlüssel **72**, das Kurzfristiger-Ablauf-Feld **76** und das Signaturfeld **77** des nicht strukturierten kurzfristigen Einmalzertifikats **70** von Fig. 4. Das strukturierte kurzfristige Einmalzertifikat **80** umfasst jedoch Ordner **88a** – **88n**, die jeweils den Anwendungen **36'a** – **36'n** entsprechen. Für jeden Verifizierer/Anwendung **36'**, auf die das Subjekt/der Client **34'** zugreifen kann, wie es beispielsweise durch ein Benutzerprofil spezifiziert ist, gibt es einen kryptographischen Ordner **88**. Jeder kryptographische Ordner **88** enthält langfristige Identifikationsinformationen **83** und/oder kurzfristige Autorisierungsinformationen **89**, wie sie für den entsprechenden Verifizierer/die entsprechende Anwendung **36'** zum Durchführen von Autorisierungs-Entscheidungen über das Subjekt/den Client **34'** erforderlich sind. Bei einem Ausführungsbeispiel ist das strukturierte kurzfristige Einmalzertifikat **80** durch Hinzufügen einer Ordnererweiterung zu einem X.509v3-Zertifikat implementiert.

[0079] Ein On-Line-Protokoll zum Ausgeben eines strukturierten kurzfristigen Einmalzertifikats **80** an das Subjekt/den Client **34'** von dem Berechtigungsnachweisserver **42'** für das nicht-unterzeichnete Zer-

tifikat **60** ist in Fig. 10 allgemein bei **500** dargestellt. Bei Schritt **502** sendet das Subjekt/der Client **34'** eine Mitteilung an den Berechtigungsnachweisserver **42**, die das nicht-unterzeichnete Zertifikat **60** enthält und fordert an, dass ein kurzfristiges Einmalzertifikat für das nicht-unterzeichnete Zertifikat **60** ausgegeben wird.

[0080] Bei Schritt **504** berechnet der Berechtigungsnachweisserver **42'** einen kryptographischen Hash-Wert des nichtunterzeichneten Zertifikats **60** mit einer vereinbarten kollisionsresistenten Hash-Funktion. Bei Schritt **504** verifiziert der Berechtigungsnachweisserver **42'** dann, dass der berechnete kryptographische Hash-Wert in der Hash-Tabelle **44** vorliegt.

[0081] Bei Schritt **506** greift der Berechtigungsnachweisserver **42** über die Netzwerkverbindung **92** auf das Verzeichnis **90** zu und erhält kurzfristige Autorisierungs-Informationen für das strukturierte kurzfristige Einmalzertifikat **80**.

[0082] Bei Schritt **508** kombiniert der Berechtigungsnachweisserver **42'** die kurzfristigen Autorisierungs-Informationen, die von dem Verzeichnis **90** bei Schritt **506** erhalten werden, mit den Identifikationsattributen in dem Langfristige-Identifikationsinformationen-Feld **63** des nichtunterzeichneten Zertifikats **60**. Bei Schritt **508** erzeugt der Berechtigungsnachweisserver **42'** einen kryptographischen Ordner **88** für jeden Verifizierer/jede Anwendung **36'**, auf die durch das Subjekt/den Client **34'** zugegriffen werden kann, wobei jeder kryptographische Ordner **88** alle langfristigen Identifikationsinformationen und/oder kurzfristigen Autorisierungs-Informationen enthält, die durch den Verifizierer/die Anwendung **36'** erforderlich sind, um Autorisierungsentscheidungen über das Subjekt/den Client **34'** zu treffen. Bei Schritt **508** verwendet der Berechtigungsnachweisserver **42'** kryptographische Ordner **88** zum Erzeugen des strukturierten kurzfristigen Einmalzertifikats **80**.

[0083] Bei Schritt **510** sendet der Berechtigungsnachweisserver **42'** das strukturierte kurzfristige Einmalzertifikat **80** an das Subjekt/den Client **34'**, wobei alle Ordner des kurzfristigen Einmalzertifikats offen sind.

[0084] Ein On-Line-Protokoll zum Autorisieren des Subjekts/Client **34'** ist in Fig. 11 allgemein bei **600** dargestellt. Das On-Line-Protokoll **600** wird durch das Subjekt/den Client **34'** verwendet, um dem Verifizierer/der Anwendung **36'** seine Identität nachzuweisen. Das On-Line-Protokoll **600** wird auch durch den Verifizierer/die Anwendung **36'** verwendet, um Autorisierungsentscheidungen bezüglich des Subjekts/Client **34'** zu treffen, wie z. B. Erlauben/Verweigern von Zugriff oder Autorisieren von spezifischen Transaktionen.

[0085] Bei Schritt **602** schließt das Subjekt/der Client **34'** alle Ordner **88** in dem strukturierten kurzfristigen Einmalzertifikat **80**, außer dem Ordner, der die notwendigen Identifikations-/Autorisierungs-Informationen **83**/**89** enthält, die durch den Verifizierer/die Anwendung **36'** erforderlich sind, um Autorisierungsentscheidungen bezüglich des Subjekts/des Client **34'** zu treffen. Bei Schritt **604** sendet das Subjekt/der Client **34'** das strukturierte kurzfristige Einmalzertifikat **80** an den Verifizierer/die Anwendung **36'**.

[0086] Bei Schritt **606** verifiziert der Verifizierer/die Anwendung **36'**, dass das Ablaufdatum/-zeit, die in dem Ablauffeld **86** des strukturierten kurzfristigen Einmalzertifikats **80** spezifiziert ist, nicht abgelaufen ist.

[0087] Bei Schritt **608** verwendet der Verifizierer/die Anwendung **36'** einen öffentlichen Schlüssel des Berechtigungsnachweisservers **42'** zum Verifizieren der Signatur in dem Signaturfeld **87** des strukturierten kurzfristigen Einmalzertifikats **80**. Der Verifizierer/die Anwendung **36'** kennt den öffentlichen Schlüssel des Berechtigungsnachweisservers **42** entweder direkt oder durch Zertifizierung durch eine höhere Zertifikatautorität.

[0088] Bei Schritt **610** weist das Subjekt/der Client **34'** Kenntnis des privaten Schlüssels **46'** nach, der dem öffentlichen Schlüssel **82** des strukturierten kurzfristigen Einmalzertifikats **80** zugeordnet ist. Schritt **610** wird auf eine Weise durchgeführt, die von dem Kryptosystem abhängt, für das das Privater/Öffentlicher-Schlüssel-Paar durch das Subjekt/den Client **34'** erzeugt wurde. Beispielsweise weist das Subjekt/der Client **34'** in einem digitalen Signaturkryptosystem Kenntnis des privaten Schlüssels **46'** nach, durch Verwenden des privaten Schlüssels **46'** zum digitalen Unterzeichnen einer Menge, die von einer Zufallsmenge abgeleitet wird, die durch den Verifizierer/die Anwendung **36'** erzeugt wird. Der Verifizierer/die Anwendung **36'** verifiziert dann diese digitale Signatur unter Verwendung des öffentlichen Schlüssels **82** des strukturierten kurzfristigen Einmalzertifikats **80'**.

[0089] Bei Schritt **612** extrahiert der Verifizierer/die Anwendung **36'** die Identifikations-/Autorisierungs-Informationen **83**/**89**, die in dem offenen Ordner **88** des strukturierten kurzfristigen Einmalzertifikats **80** enthalten sind. Bei Schritt **612** verwendet der Verifizierer/die Anwendung **36'** dann die Identifizierungs-/Autorisierungs-Informationen **83**/**89** zum Treffen von Autorisierungsentscheidungen bezüglich des Subjekts/Clients **34'**.

[0090] Das On-Line-Protokoll **600** zum Autorisieren des Subjekts/Client **34'** verwendet das strukturierte kurzfristige Einmalzertifikat **80** mit einem Ordner für jede Anwendung, auf die durch das Subjekt/den Cli-

ent **34'** zugegriffen werden kann, wie es durch ein Benutzerprofil bestimmt ist. Dies stellt sicher, dass jede Anwendung nur Zugriff zu Autorisierungs-Informationen hat, die dieselbe erfordert. Trotzdem kann die Autorisierung, die durch die PKI **30'** durchgeführt wird, mit nicht strukturierten kurzfristigen Einmalzertifikaten implementiert werden, wo statt einem strukturierten kurzfristigen Einmalzertifikat **80** mehrere nicht strukturierte kurzfristige Einmalzertifikate verwendet werden.

[0091] Die PKI **30**/**30'** gemäß der vorliegenden Erfindung ist stark vereinfacht und wesentlich effizienter als herkömmliche PKIs. Beispielsweise müssen Anwendungen das kurzfristige Einmalzertifikat nur für Authentifizierung und/oder Autorisierung verwenden. Das nicht-unterzeichnete Zertifikat **60**, das das traditionelle langfristige Zertifikat ersetzt, kann für die Verwendung durch das Subjekt reserviert werden, wenn ein kurzfristiges Einmalzertifikat angefordert wird. Da das nicht-unterzeichnete Zertifikat **60** nicht durch Anwendungen verwendet wird, muss es nicht-unterzeichnet werden. Anstatt dem Unterzeichnen des nicht-unterzeichneten Zertifikats **60** hält der Berechtigungsnachweisserver die kryptographische Hash-Tabelle **44**, die kryptographische Hash-Werte der nicht-unterzeichneten Zertifikate enthält, die aktuell gültig sind. Auf diese Weise wird die Zertifikatsaufhebung einfach durch Entfernen des kryptographischen Hash-Werts des nicht-unterzeichneten Zertifikats von der Hash-Tabelle **44** durchgeführt. Daher ist anders als bei herkömmlichen PKIs keine Signatur erforderlich, kein Ablaufdatum erforderlich und es besteht kein Bedarf an CRLs für das nicht-unterzeichnete Zertifikat **60** der PKI **30**/**30'** gemäß der vorliegenden Erfindung.

[0092] Die PKI **30**/**30'** erfordert eine Zertifikatstatusprüfung, ähnlich wie die On-Line-Zertifikatstatusprüfung, die durch das OCSP erforderlich ist. Die Zertifikatstatusprüfung der PKI **30**/**30'** gemäß der vorliegenden Erfindung tritt jedoch auf, wenn das Subjekt das kurzfristige Einmalzertifikat anfordert, und nicht wenn das Subjekt auf die Anwendung zugreift, wie es z. B. durch das OCSP erforderlich ist.

[0093] Eine verteilte Zertifikatautorität **132** für die Verwendung bei der PKI **30**/**30'** gemäß der vorliegenden Erfindung ist in Fig. 12 dargestellt. Die verteilte Zertifikatautorität **132** umfasst eine Registrierungsautorität **138** mit einer Zertifikatdatenbank **140**, die mit einem verteilten Berechtigungsnachweisserver **142** kommuniziert.

[0094] Der verteilte Berechtigungsnachweisserver **142** umfasst Berechtigungsnachweisserver **142a** – **142n**. Jeder Berechtigungsnachweisserver **142** umfasst eine entsprechende Hash-Tabellen-Unterteilung **144**. Bei einem Ausführungsbeispiel ist die kryptographische Hash-Tabelle **144** in Hash-Tabellen-Unterteilungen **144a** – **149n** unterteilt, gemäß einem Wert von einigen der Bits des kryptographischen Hash-Werts. Bei einer PKI **30**/**30'**, die eine verteilte Zertifikatautorität **132** verwendet, die verteilte Berechtigungsnachweisserver **142a** – **142n** aufweist, sendet das Subjekt eine Anforderung für ein kurzfristiges Einmalzertifikat direkt an die korrekte Hash-Tabellen-Unterteilung **144**.

[0095] Die Zertifikatautorität **132** wird ferner optimiert durch direktes Koppeln jedes Berechtigungsnachweisservers **142** mit seiner eigenen Kopie des Verzeichnisses **190**.

[0096] Die PKI **30**/**30'** gemäß der vorliegenden Erfindung ist hoch skalierbar, weil viele Engpässe der herkömmlichen PKIs entfernt sind. Die nicht-unterzeichneten Zertifikate **60**, die durch die PKI **30**/**30'** verwendet werden, laufen nicht ab und müssen nicht regelmäßig erneuert werden. Außerdem werden CRLs nicht verwendet. Mit der PKI **30**/**30'** wurden keine wesentlichen Engpässe eingeführt.

[0097] Ein potentieller Engpass der PKI **30**/**30'** ist, dass der Berechtigungsnachweisserver **42**/**42'**/**142** kurzfristige Einmalzertifikate sehr häufig ausgibt, wie z. B. einmal am Tag, alle paar Stunden oder sogar alle paar Minuten. Diese Frequenz des Ausgebens kurzfristiger Einmalzertifikate von dem Berechtigungsnachweisserver gemäß der vorliegenden Erfindung ist jedoch kein wesentlicher Engpass, weil die Hash-Tabelle unterteilt werden kann, wie z. B. in Hash-Tabellen-Abschnitte **144a** – **144n** der verteilten Zertifikatautorität **132**, die in Fig. 12 dargestellt ist, und der Berechtigungsnachweisserver kann wie erforderlich reproduziert werden, wie z. B. die Berechtigungsnachweisserver **142a** – **142n** der verteilten Zertifikatautorität **132**.

[0098] Ein weiterer potentieller Engpass mit der PKI **30**/**30'** ist die Zertifikatdatenbank **40**/**40'** der Registrierungsautorität **38**/**38'**. Die Zertifikatdatenbank **40**/**40'** ist jedoch kein wesentlicher Engpass, weil auf die Zertifikatdatenbank nur zugegriffen wird, wenn nicht-unterzeichnete Zertifikate **60** ausgegeben oder aufgehoben werden. Die Zertifikatdatenbank **40**/**40'** kann unter Verwendung eines Relationale-Datenbank-Verwaltungssystems (DBMS) implementiert werden, das Millionen nicht-unterzeichneter Zertifikate handhaben kann.

[0099] Ein weiterer potentieller Engpass mit dem PKI **30**/**30'** ist das Verzeichnis **90**. Das Verzeichnis **90** ist kein wesentlicher Engpass, weil das Verzeichnis **90** reproduziert werden kann, um es möglich zu machen, Millionen von Benutzer zu handhaben. Außerdem ist der LDAP-Verkehr zu dem Verzeichnis **90** wesentlich reduziert, da Anwendungen nicht auf das Verzeichnis **90** zugreifen, um Autorisierungsentscheidungen zu treffen, da bei dem Ausführungsbei-

spiel, wo die PKI **30'** verwendet wird, um das Subjekt zu autorisieren, alle notwendigen Autorisierungs-Informationen in dem kurzfristigen Einmalzertifikat **80** enthalten sind. Daher kann die PKI gemäß der vorliegenden Erfindung Millionen von Benutzern skalieren.

Beispielhafte Anwendungen der PKI gemäß der vorliegenden Erfindung

[0100] Die PKI gemäß der vorliegenden Erfindung kann vorteilhafterweise bei einem großen Bereich von Anwendungen verwendet werden. Die folgenden zwei Beispiele liefern nur zwei der zahlreichen Anwendungen für die PKI gemäß der vorliegenden Erfindung.

Webserver-Zertifikate

[0101] Eine PKI gemäß der vorliegenden Erfindung für eine Webserver-Zertifikat-Anwendung ist allgemein bei **730** in Fig. 13 dargestellt. Die PKI **730** umfasst eine Zertifikatautorität **732** (mit Berechtigungsnachweisserver), einen Webserver/Subjekt **734** und einen Browser/Verifizierer **736**, die alle durch ein Internet **731** gekoppelt sind.

[0102] Die PKI **730** verwendet keine kurzfristigen Autorisierungs-Informationen in ihrem kurzfristigen Einmalzertifikat. Daher ist ein geeignetes kurzfristiges Einmalzertifikat für die PKI **30** das in Fig. 4 dargestellte kurzfristige Einmalzertifikat **70** ist, das ein nicht strukturiertes Zertifikat ist (d. h. keine Ordner). Außerdem enthält das kurzfristige Einmalzertifikat **70**, das in der PKI **730** verwendet wird, keine vertraulichen Informationen.

[0103] Ein Webserver-Zertifikatprotokoll für die PKI **730** ist allgemein bei **700** in Fig. 14 dargestellt. Bei Schritt **702** gibt die Zertifikatautorität **732** ein nicht-unterzeichnetes Zertifikat **60** für den öffentlichen Schlüssel des Webservers **734** aus. Das nicht-unterzeichnete Zertifikat ist nicht unterzeichnet, wird nur einmal wiedergewonnen und läuft nie ab.

[0104] Bei Schritt **704** fordert der Webserver **734** ein nicht strukturiertes kurzfristiges Einmalzertifikat **70** an. Das nichtunterzeichnete Zertifikat **60** wird als Teil der Webserver-Anforderung gesendet. Bei einem Ausführungsbeispiel spezifiziert das Metadatenfeld **61** die Dauer der Gültigkeitsperiode des kurzfristigen Einmalzertifikats **70**, das auszugeben ist.

[0105] Bei Schritt **706** verifiziert die Zertifikatautorität **732** das nicht-unterzeichnete Zertifikat **60**, das durch den Webserver **734** geliefert wird und gibt ein entsprechendes kurzfristiges Einmalzertifikat **70** aus. Bei Schritt **706** wird das kurzfristige Einmalzertifikat **70** von dem nichtunterzeichneten Zertifikat **60** abgeleitet durch Hinzufügen einer Ablaufzeit in dem Kurzfristiger-Ablauf-Feld **76**, wie z. B. 24 Stunden nach dem aktuellen Zeitpunkt und durch Hinzufügen der Signatur der Zertifikatautorität **732** in dem Signaturfeld **77**.

[0106] Bei Schritt **708** sendet der Webserver **734** das kurzfristige Einmalzertifikat **70** an den Browser **736**. Schritt **708** ist Teil eines Protokolls zum Herstellen einer SSL-Verbindung. Bei Schritt **710** wird zwischen dem Browser **736** und dem Webserver **734** ein Handshake durchgeführt. Bei Schritt **710** weist der Webserver **734** dem Browser **736** nach, dass der Webserver **734** den privaten Schlüssel kennt, der dem öffentlichen Schlüssel in dem kurzfristigen Einmalzertifikat **70** entspricht. Schritt **710** ist auch Teil des Protokolls zum Herstellen der SSL-Verbindung.

[0107] Bei Schritt **712** wird eine sichere Verbindung zwischen dem Browser **736** und dem Webserver **734** hergestellt. Bei Schritt **712** ist eine beispielhafte sichere Verbindung SSL, die Datenintegrität liefert, die Verbindungsüberfälle und andere Mann-in-der-Mitte-Angriffe verhindert. Die SSL liefert auch Entschlüsselung, um Vertraulichkeit sicherzustellen.

[0108] Bei herkömmlichen Webserver-Zertifikat-PKI-Anwendungen kann das Zertifikat des Webservers nicht aufgehoben werden oder der Browser muss auf die Zertifikatautorität zugreifen, um die aktuellste CRL zu erhalten, um den Zertifikat-Status über OCSP zu prüfen. Dass der Browser einer herkömmlichen Webserver-Zertifikat-PKI auf die Zertifikatautorität zugreift, ist äußerst unerwünscht, weil dieser Zugriff auf die Zertifikatautorität eine Verzögerung einführt, die durch den Benutzer als zusätzliche Verzögerung beim Zugreifen auf den Webserver wahrgenommen wird. Außerdem verhindert dieser Browser-Zugriff der Zertifikatautorität möglicherweise den Zugriff auf den Webserver, falls die Zertifikatautorität ausgeschaltet ist. Darüber hinaus erfordert CRL- oder OCSP-Verarbeiten einen zusätzlichen Code in dem Browser, der eventuell nicht in den Browser passt, falls der Browser auf einer kleinen Netzwerkanwendung läuft.

[0109] Im Gegensatz zu der herkömmlichen PKI kann die Zertifikatautorität **732** bei der PKI **730** gemäß der vorliegenden Erfindung das nicht-unterzeichnete Zertifikat **60** des Webservers aufheben. Nachdem die Zertifikatautorität **732** das nichtunterzeichnete Zertifikat **60** aufgehoben hat, ist der Webserver **734** nicht mehr in der Lage, kurzfristige Einmalzertifikate zu erhalten, und die Browser **736** sind nicht in der Lage, SSL-Verbindungen mit dem Webserver **734** herzustellen. Darüber hinaus verwendet der Browser **736** keine CRLs oder OCSP, daher ist der Browser-Zugriff der Zertifikatautorität **732** zum Erhalten der aktuellsten CRL oder zum Prüfen des Zertifikat-Status über die OCSP mit der PKI **730** nicht erforderlich.

Firmen-PKI

[0110] Eine Firmen-PKI gemäß der vorliegenden Erfindung ist allgemein bei **930** in Fig. 15 dargestellt. Die Unternehmens-PKI **930** umfasst eine Zertifikatautorität **932** (mit Berechtigungsnachweisserver), der über eine Netzwerkverbindung **950** mit einem Client **934** gekoppelt ist. Die Zertifikatautorität **932** ist über eine Netzwerkverbindung **992** mit einem LDAP-Verzeichnis **990** gekoppelt. Der Client **934** hat Zugriff auf einen privaten Schlüssel **946** eines Benutzers, der in einer Smartcard **948** gespeichert ist. Der Client **934** ist über Netzwerkverbindungen **952a**, **952b** bzw. **952c** mit Anwendungen **936a**, **936b** und **936c** gekoppelt.

[0111] Die Netzwerkverbindungen der Unternehmens-PKI **930** werden als sicher angesehen oder werden durch Host-zu-Host-IPSEC geschützt. Das kurzfristige Einmalzertifikat des Client **934** ist ein strukturiertes Zertifikat, wie das strukturierte kurzfristige Einmalzertifikat **80**, das in Fig. 9 dargestellt ist. Das strukturierte kurzfristige Einmalzertifikat **80** in der Unternehmens-PKI **930** enthält kurzfristige Autorisierungs-Informationen, die möglicherweise vertraulich sind.

[0112] Ein Autorisierungs-Protokoll für die Unternehmens-PKI **930** ist allgemein bei **900** in Fig. 16 dargestellt. Bei Schritt **902** gibt die Zertifikatautorität **932** ein nichtunterzeichnetes Zertifikat **60** für den öffentlichen Schlüssel des Benutzers aus. Schritt **902** muss nur einmal durchgeführt werden. Bei Schritt **904** legt der Client **934** das nicht-unterzeichnete Zertifikat **60** der Zertifikatautorität **932** vor. Schritt **904** wird beim der Netzwerkanmeldung durchgeführt.

[0113] Bei Schritt **906** ermöglicht ein Handshake zwischen der Zertifikatautorität **932** und dem Client **934** dem Client **934**, einer Zertifikatautorität **932** zu zeigen, dass der Client **934** Zugriff zu dem privaten Schlüssel **946** des Benutzers hat, der in der Smartcard **948** gespeichert ist. Schritt **906** wird bei der Netzwerkanmeldung durchgeführt. Bei Schritt **908** erhält die Zertifikatautorität **932** kurzfristige Autorisierungs-Informationen von dem LDAP-Verzeichnis **990**. Bei einem Ausführungsbeispiel ist das LDAP-Verzeichnis **990** mit der Zertifikatautorität **932** integriert. Schritt **908** wird bei der Netzwerkanmeldung durchgeführt.

[0114] Bei Schritt **910** gibt die Zertifikatautorität **932** ein strukturiertes kurzfristiges Einmalzertifikat **80** aus. Bei Schritt **910** sendet die Zertifikatautorität **932** das ausgegebene strukturierte kurzfristige Einmalzertifikat **80** an den Client **934**. Bei einer beispielhaften Anwendung der Unternehmens-PKI **930** umfasst das strukturierte kurzfristige Einmalzertifikat **80** drei Ordner, einen für jede Anwendung **936a**, **936b** und **936c**. Alle Ordner des strukturierten kurzfristigen Einmalzertifikats **80** sind offen. Ein Teil der Informationen in den Ordnern des strukturierten kurzfristigen Einmalzertifikats **80** ist möglicherweise vertraulich. Netzwerkverbindungen **952** werden jedoch als sicher angesehen oder durch Host-zu-Host-IPSEC geschützt. Schritt **910** wird bei der Netzwerkanmeldung durchgeführt.

[0115] Bei Schritt **912** legt der Client **934** der angeforderten Anwendung **936** das kurzfristige Einmalzertifikat **80** vor. Falls beispielsweise die angeforderte Anwendung **936b** ist, bleibt der Ordner **88b**, der der Anwendung **936b** entspricht, offen. Bei diesem Beispiel sind die Ordner **88a** und **88c** des kurzfristigen Einmalzertifikats **80**, das den Anwendungen **936a** und **936c** entspricht, geschlossen.

[0116] Bei Schritt **914** wird ein Handshake zwischen der angeforderten Anwendung **936b** und dem Client **934** durchgeführt. Bei Schritt **914** zeigt der Client **934** der Anwendung **936b**, dass der Client **934** Zugriff auf den privaten Schlüssel **946** des Benutzers hat, der in der Smartcard **948** gespeichert ist.

[0117] Die Unternehmens-PKI **930** gemäß der vorliegenden Erfindung ist im Vergleich zu herkömmlichen Unternehmens-PKIs rationalisiert. Die Unternehmens-PKI **930** muss keine CRLs oder OCSP verwenden. Alle Informationen, die benötigt werden, um Autorisierungsentscheidungen zu treffen, sind in dem strukturierten kurzfristigen Einmalzertifikat **80** enthalten. Daher benötigen die Anwendungen **936** keinen Zugriff auf das LDAP-Verzeichnis **990** zum Treffen von Autorisierungsentscheidungen über den Client **934**.

[0118] Die Unternehmens-PKI **930** kann Millionen von Benutzern handhaben. Die PKI **930** ist geeignet zum Liefern von Authentifizierungs- und Autorisierungsdiensten für alle Angestellten und Geschäftspartner einer Firma jeder Größe.

[0119] Fig. 17 stellt ein Ausführungsbeispiel eines Computersystems **250** und ein externes computerlesbares Medium **252** dar, das gemäß der vorliegenden Erfindung verwendet werden kann, um eine oder mehrere der Hauptsoftware-Programmkomponenten einer leichten PKI gemäß der vorliegenden Erfindung zu implementieren, wie z. B. PKI **30**, PKI **30'**, PKI **730**, PKI **830** und PKI **930**. Ausführungsbeispiele des externen computerlesbaren Mediums **252** umfassen, sind aber nicht beschränkt auf: eine CD-ROM, eine Diskette und eine Plattenkassette. Jede der Hauptsoftware-Programmkomponenten einer leichten PKI gemäß der vorliegenden Erfindung kann in einer Vielzahl von kompilierten und interpretierten Computersprache implementiert sein. Das externe computerlesbare Medium **252** speichert Quellcode, Objektcode, ausführbaren Code, Shell-Skripte und/oder Dynamische-Verbindung-Bibliotheken für

eine der Hauptsoftware-Programmkomponenten einer leichten PKI gemäß der vorliegenden Erfindung. Ein Eingabegerät **254** liest das externe computerlesbare Medium **252** und liefert diese Daten an das Computersystem **250**. Ausführungsbeispiele des Eingabegeräts **254** umfassen, sind aber nicht beschränkt auf: einen CD-ROM-Leser, ein Disketten-Laufwerk und eine Datenkassettenlesevorrichtung.

[0120] Das Computersystem **250** umfasst eine zentrale Verarbeitungseinheit **256** zum Ausführen einer der Hauptsoftware-Programmkomponenten einer leichten PKI gemäß der vorliegenden Erfindung. Das Computersystem **250** umfasst auch einen lokalen Plattenspeicher **262** zum lokalen Speichern einer der Hauptsoftware-Programmkomponenten einer leichten PKI gemäß der vorliegenden Erfindung vor, während und nach der Ausführung. Jede der Hauptsoftware-Programmkomponenten einer leichten PKI gemäß der vorliegenden Erfindung verwendet auch den Speicher **260** in dem Computersystem während der Ausführung. Auf die Ausführung einer der Hauptsoftware-Programmkomponenten einer leichten PKI gemäß der vorliegenden Erfindung hin werden Ausgangsdaten erzeugt und zu dem Ausgabegerät **258** gerichtet. Ausführungsbeispiele des Ausgabegeräts **258** umfassen, sind aber nicht beschränkt auf: eine Computeranzeigevorrichtung, einen Drucker und/oder eine Plattenspeichervorrichtung.

[0121] Obwohl hierin zu Darstellungszwecken des bevorzugten Ausführungsbeispiels spezifische Ausführungsbeispiele dargestellt und beschrieben wurden, ist für Durchschnittsfachleute auf diesem Gebiet klar, dass eine große Vielzahl von Implementierungen für die spezifischen gezeigten und beschriebenen Ausführungsbeispiele eingesetzt werden kann, ohne von dem Schutzbereich der vorliegenden Erfindung abzuweichen. Fachleute auf dem Gebiet der Chemie, Mechanik, Elektromechanik, Elektrizität und Computer werden ohne weiteres erkennen, dass die vorliegende Erfindung in einer großen Vielzahl von Ausführungsbeispielen implementiert werden kann. Diese Anwendung soll alle Adaptionen oder Variationen der hierin erörterten bevorzugten Ausführungsbeispiele abdecken. Daher ist klar, dass diese Erfindung nur durch die Ansprüche begrenzt ist.

Patentansprüche

1. Eine Öffentlicher-Schlüssel-Infrastruktur (**30**), die auch durch PKI identifiziert ist, die ein Subjekt (**34**), einen Verifizierer (**36**) und eine Registrierungsautorität (**38**) umfasst, wobei die PKI gekennzeichnet ist durch

die Registrierungsautorität, die eine Off-Line-Registrierungsautorität (**38**) ist, zum Ausgeben eines ersten nicht-unterzeichneten Zertifikats (**60**) off-line an das Subjekt, das einen öffentlichen Schlüssel (**62**) des Subjekts an langfristige Identifikationsinformationen (**63**) bindet, die sich auf das Subjekt beziehen, wobei die Registrierungsautorität eine Zertifikatdatenbank (**40**) von nicht-unterzeichneten Zertifikaten beibehält, in der dieselbe das erste nichtunterzeichnete Zertifikat speichert;

einen On-Line-Berechtigungsnachweis-Server (**42**) zum Ausgeben eines kurzfristigen Einmalzertifikats (**70**) on-line an das Subjekt, wobei das kurzfristige Einmalzertifikat den öffentlichen Schlüssel des Subjekts von dem ersten nicht-unterzeichneten Zertifikat an die langfristigen Identifikationsinformationen bindet, die sich auf das Subjekt des ersten nicht-unterzeichneten Zertifikats beziehen, wobei der Berechtigungsnachweis-Server eine Tabelle (**44**) beibehält, die Einträge enthält, die gültigen nicht-unterzeichneten Zertifikaten entsprechen, die in der Zertifikatdatenbank gespeichert sind; und

wobei das Subjekt das kurzfristige Einmalzertifikat dem Verifizierer für eine Authentifizierung präsentiert und zeigt, dass das Subjekt Kenntnis eines privaten Schlüssels (**46**) hat, der dem öffentlichen Schlüssel in dem kurzfristigen Einmalzertifikat entspricht.

2. Die PKI gemäß Anspruch 1, bei der das kurzfristige Einmalzertifikat ein Ablaufdatum/Zeit umfasst.

3. Die PKI gemäß Anspruch 2, bei der eine Gültigkeitsperiode, von dem Zeitpunkt, zu dem der Berechtigungsnachweisserver das kurzfristige Einmalzertifikat erteilt, bis zu dem Ablaufdatum/Zeit ausreichend kurz ist, so dass das kurzfristige Zertifikat keiner Aufhebung unterzogen werden muss.

4. Die PKI gemäß Anspruch 1 oder 2, bei der das kurzfristige Einmalzertifikat keiner Aufhebung unterzogen wird.

5. Die PKI gemäß Anspruch 1, bei der die Tabelle, die durch den Berechtigungsnachweisserver beibehalten wird, eine Hash-Tabelle ist, die kryptographische Hash-Werte von gültigen nicht-unterzeichneten Zertifikaten enthält, die in der Zertifikatdatenbank gespeichert sind, und einen kryptographischen Hash-Wert des ersten nicht-unterzeichneten Zertifikats umfasst, wobei das Subjekt das ausgegebene erste nichtunterzeichnete Zertifikat dem Berechtigungsnachweisserver präsentiert, um das kurzfristige Einmalzertifikat zu erhalten.

6. Die PKI gemäß Anspruch 1, bei der die Registrierungsautorität und der Berechtigungsnachweisserver in einer Zertifikatautorität enthalten sind, und wobei die Zertifikatautorität eine verteilte Zertifikatautorität ist, die zumindest zwei verteilte Berechtigungsnachweisserver umfasst.

7. Die PKI gemäß Anspruch 6, bei der die zumindest zwei verteilten Berechtigungsnachweisserver zumindest zwei entsprechende Hashtabellenunter-

teilungen umfassen, die kryptographische Hash-Werte von gültigen nichtunterzeichneten Zertifikaten enthalten, die den nichtunterzeichneten Zertifikaten entsprechen, die in der Zertifikatdatenbank gespeichert sind, wobei eine der Hashtabellenunterteilungen einen kryptographischen Hash-Wert des ersten nicht-unterzeichneten Zertifikats enthält, wobei das Subjekt das ausgegebene erste nicht-unterzeichnete Zertifikat einem der zumindest zwei verteilten Berechtigungsnachweisserver präsentiert, um das kurzfristige Einmalzertifikat zu erhalten.

8. Die PKI gemäß Anspruch 1, bei der das kurzfristige Einmalzertifikat ein nicht strukturiertes kurzfristiges Zertifikat ist.

9. Die PKI gemäß Anspruch 1, die ferner folgendes Merkmal umfasst:
ein Verzeichnis zum Speichern kurzfristiger Berechtigungsinformationen, die sich auf das Subjekt beziehen;
wobei das kurzfristige Einmalzertifikat auch die öffentlichen Schlüssel des Subjekts von dem ersten nicht-unterzeichneten Zertifikat an die kurzfristigen Berechtigungsinformationen bindet, die sich auf das Subjekt von dem Verzeichnis beziehen; und
wobei das Subjekt das kurzfristige Einmalzertifikat dem Verifizierer für eine Berechtigung präsentiert und zeigt, dass das Subjekt Kenntnis eines privaten Schlüssels hat, der dem öffentlichen Schlüssel in dem kurzfristigen Einmalzertifikat entspricht.

10. Die PKI gemäß Anspruch 1, die ferner folgende Merkmale umfasst:
einen zweiten Verifizierer; und
wobei das kurzfristige Zertifikat ein strukturiertes kurzfristiges Zertifikat ist, das folgende Merkmale umfasst:
einen ersten Ordner, der dem ersten genannten Verifizierer entspricht und langfristige Informationen und kurzfristige Informationen enthält, wie sie durch den ersten genannten Verifizierer gefordert werden;
einen zweiten Ordner, der dem zweiten Verifizierer entspricht und langfristige Informationen und kurzfristige Informationen enthält, wie sie durch den zweiten Verifizierer gefordert werden;
wobei der erste Ordner geöffnet ist und der zweite Ordner geschlossen ist, wenn das Subjekt das kurzfristige Einmalzertifikat dem ersten genannten Verifizierer für eine Berechtigung präsentiert, wobei das Schließen des zweiten Ordners seinen Inhalt für den ersten genannten Verifizierer unlesbar macht; und
wobei der erste Ordner geschlossen wird und der zweite Ordner geöffnet wird, wenn das Subjekt das kurzfristige Einmalzertifikat dem zweiten Verifizierer für eine Berechtigung präsentiert, wobei das Schließen des ersten Ordners seinen Inhalt für den zweiten Verifizierer unlesbar macht.

11. Die PKI gemäß Anspruch 10, bei der der erste Ordner und der zweite Ordner als Erweiterungsfelder eines X.509v3-Zertifikats implementiert sind.

12. Die PKI gemäß Anspruch 1, bei der die Registrierungsautorität und der Berechtigungsnachweisserver in einer Zertifikatsautorität enthalten sind, und bei der die Zertifikatsautorität das erste nicht-unterzeichnete Zertifikat aufhebt, wenn die Bindung des öffentlichen Schlüssels des Subjekts an die langfristigen Identifikationsinformationen, die sich auf das Subjekt beziehen, ungültig wird.

13. Die PKI gemäß Anspruch 1, bei der die Zertifikatsautorität ein Aufhebungsprotokoll durchführt, um das erste nicht-unterzeichnete Zertifikat aufzuheben, wobei das Aufhebungsprotokoll Folgendes umfasst:
die Registrierungsautorität empfängt das erste nicht-unterzeichnete Zertifikat von der Zertifikatdatenbank und berechnet einen kryptographischen Hash-Wert des ersten nicht-unterzeichneten Zertifikats;
Senden einer Mitteilung von der Registrierungsautorität an den Berechtigungsnachweisserver, der den kryptographischen Hash-Wert des ersten nichtunterzeichneten Zertifikats enthält, und Anfordern, dass der Berechtigungsnachweisserver den entsprechenden kryptographischen Hash-Wert des ersten nicht-unterzeichneten Zertifikats aus seiner Hash-Tabelle entfernt; und
der Berechtigungsnachweisserver entfernt den kryptographischen Hash-Wert des ersten nichtunterzeichneten Zertifikats aus seiner Hash-Tabelle.

14. Ein Verfahren zum Authentifizieren eines Subjekts (**34**), das das Ausgeben eines kurzfristigen Einmalzertifikats an das Subjekt und das Präsentieren des kurzfristigen Einmalzertifikats an einen Verifizierer (**36**) umfasst, wobei das Verfahren ferner gekennzeichnet ist durch:
Ausgeben eines ersten nicht-unterzeichneten Zertifikats (**60**) off-line an das Subjekt, das einen öffentlichen Schlüssel (**62**) des Subjekts an langfristige Identifikationsinformationen (**63**) bindet, die sich auf das Subjekt beziehen;
Beibehalten einer Zertifikatdatenbank (**40**) von nicht-unterzeichneten Zertifikaten off-line, was das Speichern des ersten nicht-unterzeichneten Zertifikats in der Zertifikatdatenbank umfasst;
Ausgeben des kurzfristigen Einmalzertifikats (**70**) on-line an das Subjekt, wobei das kurzfristige Einmalzertifikat den öffentlichen Schlüssel des Subjekts von dem ersten nicht-unterzeichneten Zertifikat an die langfristigen Identifikationsinformationen bindet, die sich auf das Subjekt von dem ersten nichtunterzeichneten Zertifikat beziehen;
Beibehalten einer Tabelle (**44**) on-line, die Einträge enthält, die gültigen nicht-unterzeichneten Zertifikaten entsprechen, die in der Zertifikatdatenbank gespeichert sind; und
Präsentieren des kurzfristigen Einmalzertifikats

durch das Subjekt an den Verifizierer (**36**) für eine Authentifizierung und Zeigen, dass das Subjekt Kenntnis eines privaten Schlüssels (**46**) hat, der dem öffentlichen Schlüssel in dem kurzfristigen Einmalzertifikat entspricht.

15. Das Verfahren gemäß Anspruch 14, bei dem das kurzfristige Einmalzertifikat ein Ablaufdatum/Zeit umfasst.

16. Das Verfahren gemäß Anspruch 15, bei dem eine Gültigkeitsperiode von dem Zeitpunkt, zu dem das kurzfristige Einmalzertifikat erteilt wird, zu dem Ablaufdatum/Zeit ausreichend kurz ist, so dass das kurzfristige Zertifikat keiner Aufhebung unterzogen werden muss.

17. Das Verfahren gemäß Anspruch 14 oder 15, bei dem das kurzfristige Einmalzertifikat keiner Aufhebung unterzogen wird.

18. Das Verfahren gemäß Anspruch 14, bei dem die Tabelle durch einen Berechtigungsnachweisserver beibehalten wird, und eine Hash-Tabelle ist, die kryptographische Hash-Werte von gültigen nicht-unterzeichneten Zertifikaten enthält, die in der Zertifikatdatenbank gespeichert sind, und einen kryptographischen Hash-Wert des ersten nicht-unterzeichneten Zertifikats enthält, wobei das Verfahren ferner folgenden Schritt umfasst:
Präsentieren des ausgegebenen ersten nichtunterzeichneten Zertifikats durch das Subjekt an den Berechtigungsnachweisserver, um das kurzfristige Einmalzertifikat zu erhalten.

19. Das Verfahren gemäß Anspruch 14, bei dem das kurzfristige Einmalzertifikat ein nicht strukturiertes kurzfristiges Zertifikat ist.

20. Das Verfahren gemäß Anspruch 14, das ferner folgenden Schritt umfasst:
Speichern von kurzfristigen Berechtigungsinformationen, die sich auf das Subjekt beziehen, in einem Verzeichnis, wobei das kurzfristige Einmalzertifikat auch den öffentlichen Schlüssel des Subjekts von dem ersten nicht-unterzeichneten Zertifikat an die kurzfristigen Berechtigungsinformationen bindet, die sich auf das Subjekt von dem Verzeichnis beziehen; und
Präsentieren des kurzfristigen Einmalzertifikats durch das Subjekt an den Verifizierer für eine Berechtigung und Zeigen, dass das Subjekt Kenntnis eines privaten Schlüssels hat, der dem öffentlichen Schlüssel in dem kurzfristigen Einmalzertifikat entspricht.

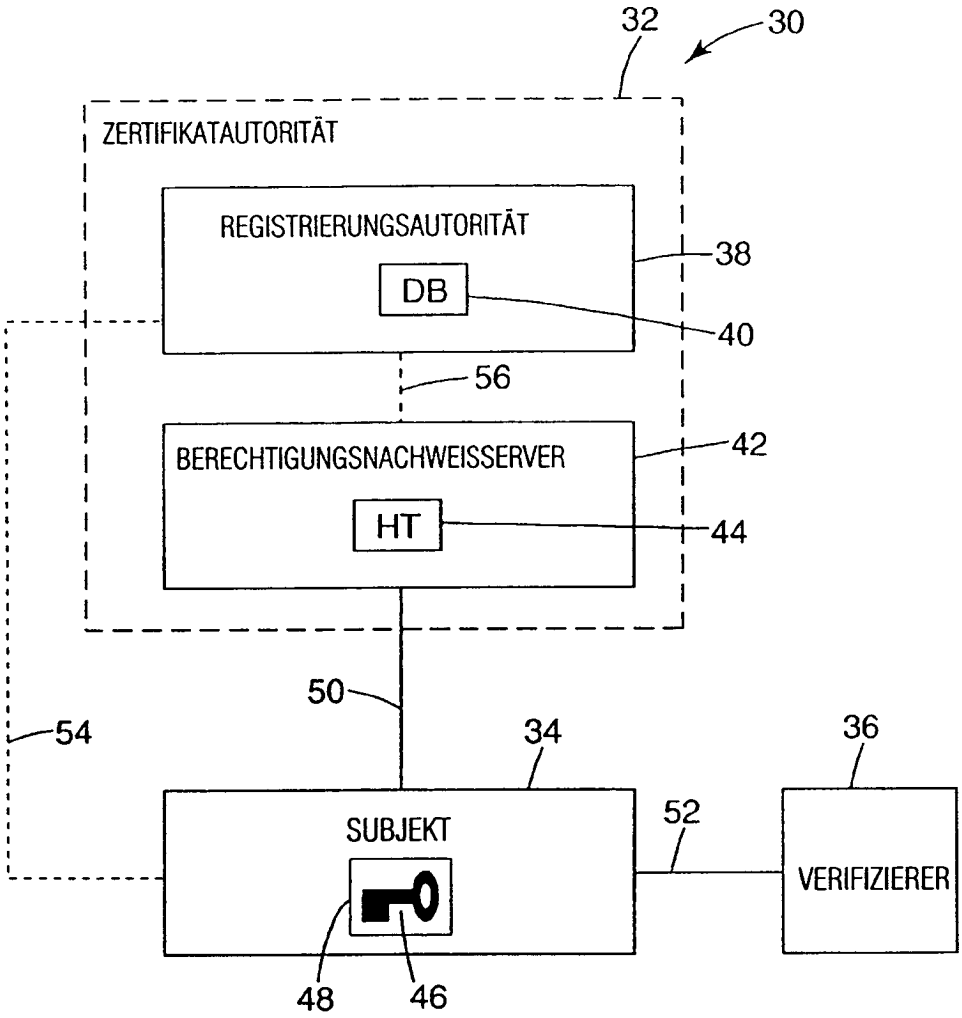
21. Das Verfahren gemäß Anspruch 14, bei dem das kurzfristige Zertifikat ein strukturiertes kurzfristiges Zertifikat ist, das einen ersten Ordner umfasst, der dem ersten genannten Verifizierer entspricht und langfristige Informationen und kurzfristige Informationen enthält, wie es durch den ersten genannten Verifizierer gefordert wird, und einen zweiten Ordner umfasst, der einem zweiten Verifizierer entspricht und langfristige Informationen und kurzfristige Informationen enthält, wie es durch den zweiten Verifizierer gefordert wird, wobei das Verfahren ferner folgende Schritte umfasst:
Schließen des zweiten Ordners und Offenlassen des ersten Ordners vor dem Präsentierschritt, falls das kurzfristige Einmalzertifikat durch das Subjekt dem ersten genannten Verifizierer für eine Berechtigung präsentiert wird, wobei das Schließen des zweiten Ordners seinen Inhalt für den ersten genannten Verifizierer unlesbar macht; und
Schließen des ersten Ordners und Offenlassen des zweiten Ordners vor dem Präsentierschritt, falls das kurzfristige Einmalzertifikat durch das Subjekt dem zweiten Verifizierer für eine Berechtigung präsentiert wird, wobei das Schließen des ersten Ordners seinen Inhalt für den zweiten Verifizierer unlesbar macht.

22. Das Verfahren gemäß Anspruch 14, das ferner folgenden Schritt umfasst:
Aufheben des ersten nicht-unterzeichneten Zertifikats, wenn das Binden des öffentlichen Schlüssels des Subjekts an die langfristigen Identifikationsinformationen, die sich auf das Subjekt beziehen, ungültig wird.

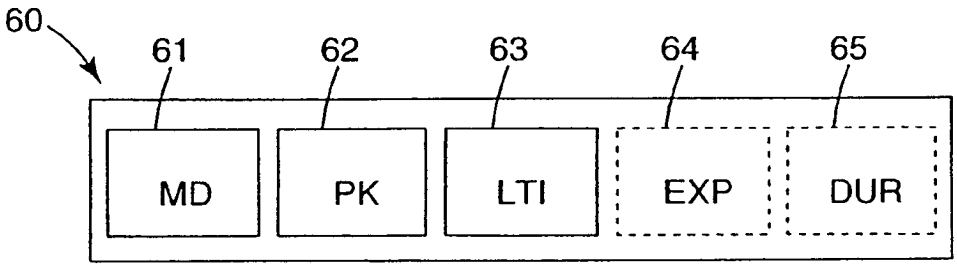
23. Das Verfahren gemäß Anspruch 22, das ferner folgenden Schritt umfasst:
Durchführen eines Aufhebungsprotokolls zum Aufheben des ersten nicht-unterzeichneten Zertifikats, wobei das Aufhebungsprotokoll folgende Schritte umfasst:
Wiedergewinnen des ersten nicht-unterzeichneten Zertifikats von der Zertifikatdatenbank und Berechnen eines kryptographischen Hash-Werts des ersten nichtunterzeichneten Zertifikats;
Senden einer Mitteilung, die den kryptographischen Hash-Wert des ersten nicht-unterzeichneten Zertifikats umfasst, und Anfordern, dass der entsprechende kryptographische Hash-Wert des ersten nichtunterzeichneten Zertifikats von der Hash-Tabelle desselben entfernt wird; und
Entfernen des kryptographischen Hash-Werts des ersten nicht-unterzeichneten Zertifikats von der Hash-Tabelle desselben.

Es folgen 14 Blatt Zeichnungen

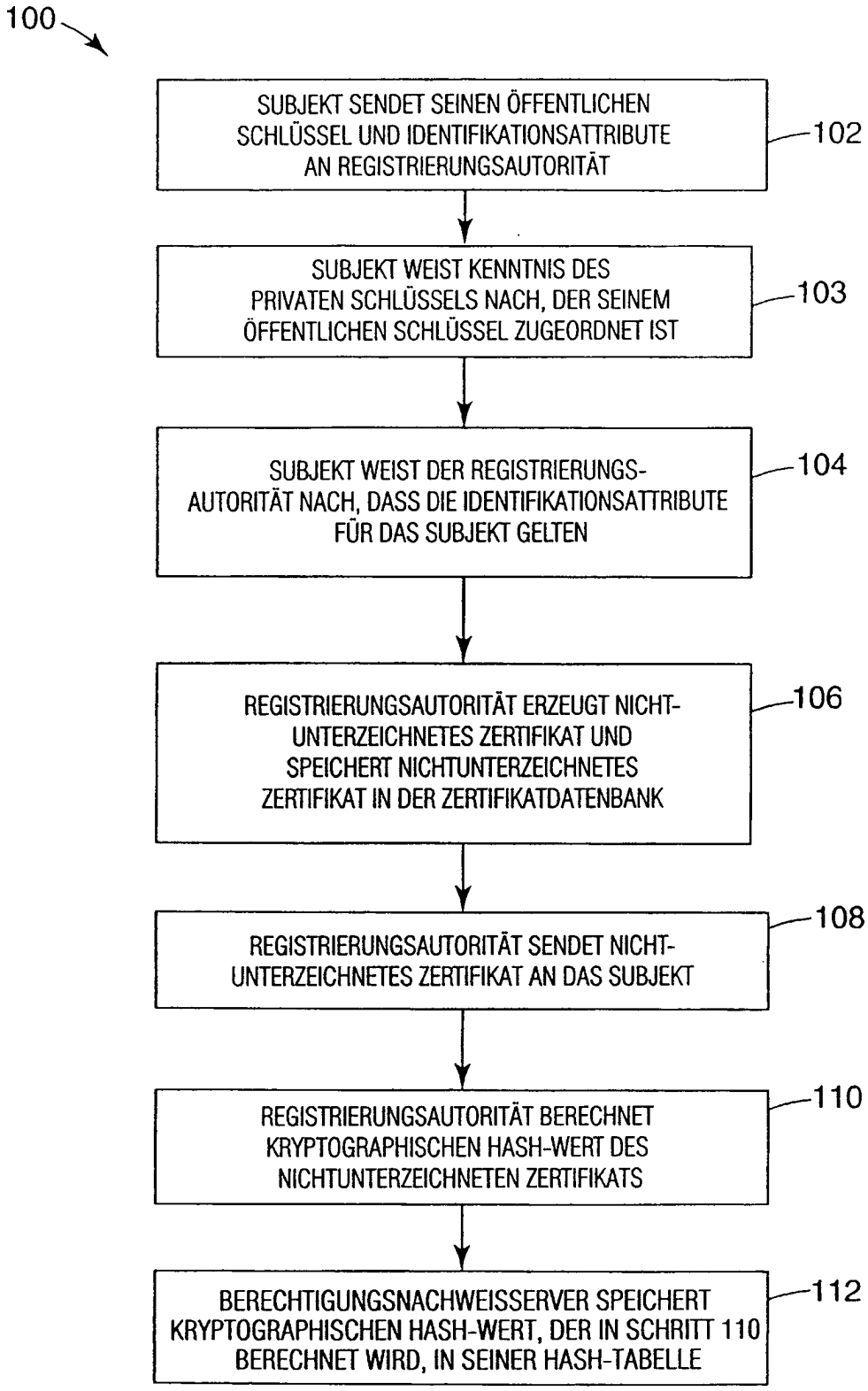
Anhängende Zeichnungen



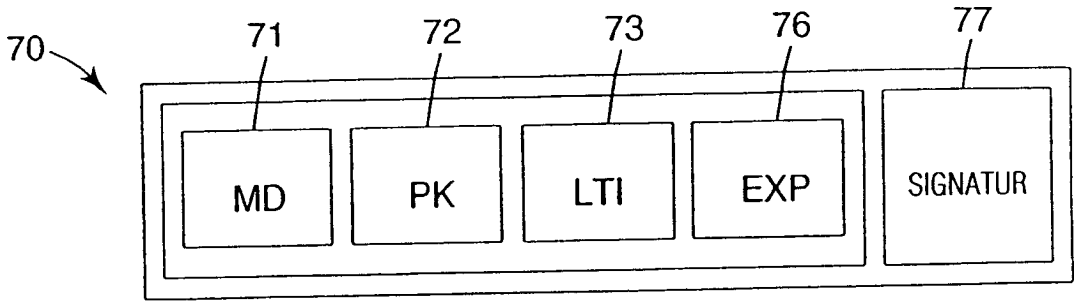
FIGUR 1



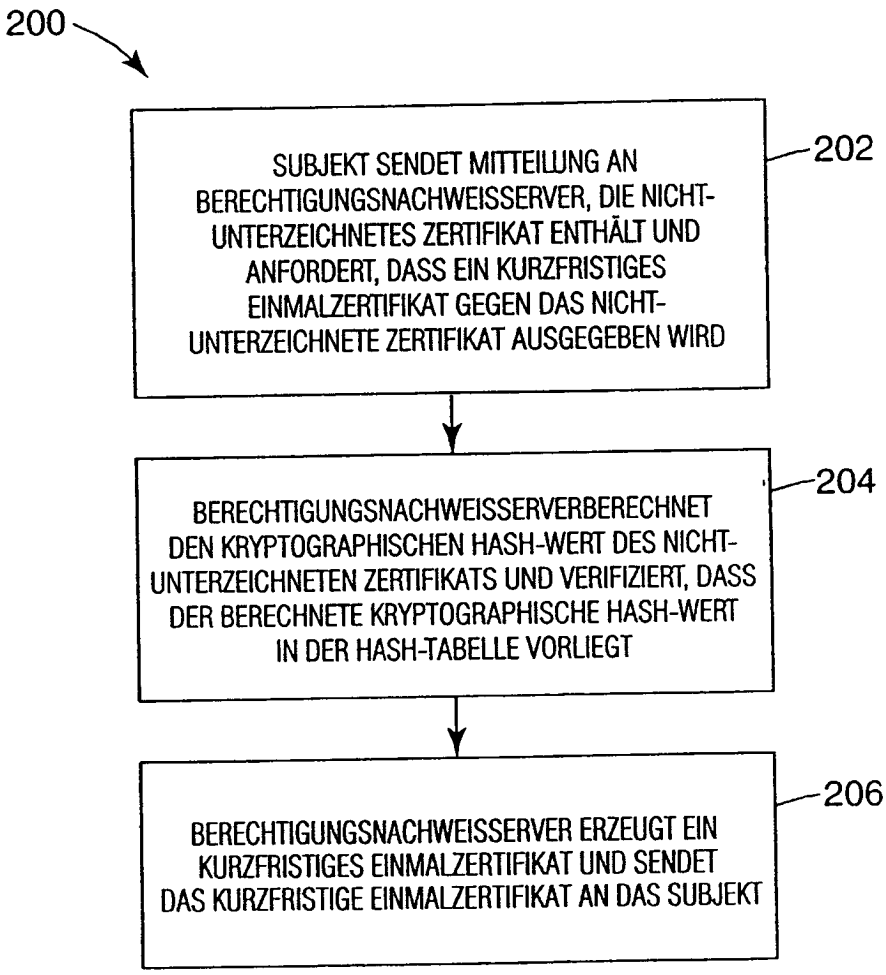
FIGUR 2


100
SUBJEKT SENDET SEINEN ÖFFENTLICHEN SCHLÜSSEL UND IDENTIFIKATIONSATTRIBUTE AN REGISTRIERUNGSAUTORITÄT
102
SUBJEKT WEIST KENNTNIS DES PRIVATEN SCHLÜSSELS NACH, DER SEINEM ÖFFENTLICHEN SCHLÜSSEL ZUGEORDNET IST
103
SUBJEKT WEIST DER REGISTRIERUNGS-AUTORITÄT NACH, DASS DIE IDENTIFIKATIONSATTRIBUTE FÜR DAS SUBJEKT GELTEN
104
REGISTRIERUNGSAUTORITÄT ERZEUGT NICHT-UNTERZEICHNETES ZERTIFIKAT UND SPEICHERT NICHTUNTERZEICHNETES ZERTIFIKAT IN DER ZERTIFIKATDATENBANK
106
REGISTRIERUNGSAUTORITÄT SENDET NICHT-UNTERZEICHNETES ZERTIFIKAT AN DAS SUBJEKT
108
REGISTRIERUNGSAUTORITÄT BERECHNET KRYPTOGRAPHISCHEN HASH-WERT DES NICHTUNTERZEICHNETEN ZERTIFIKATS
110
BERECHTIGUNGSNACHWEISSERVER SPEICHERT KRYPTOGRAPHISCHEN HASH-WERT, DER IN SCHRITT 110 BERECHNET WIRD, IN SEINER HASH-TABELLE
112

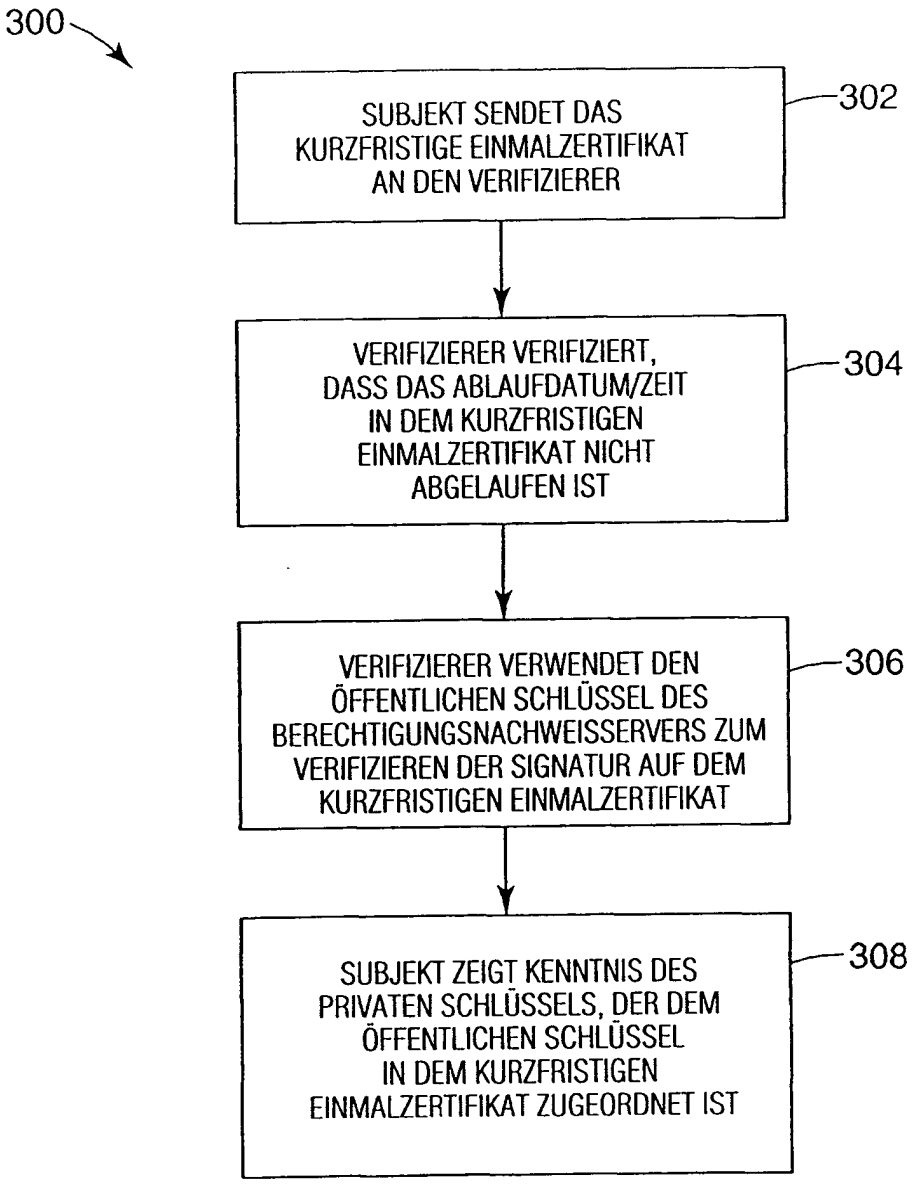
FIGUR 3



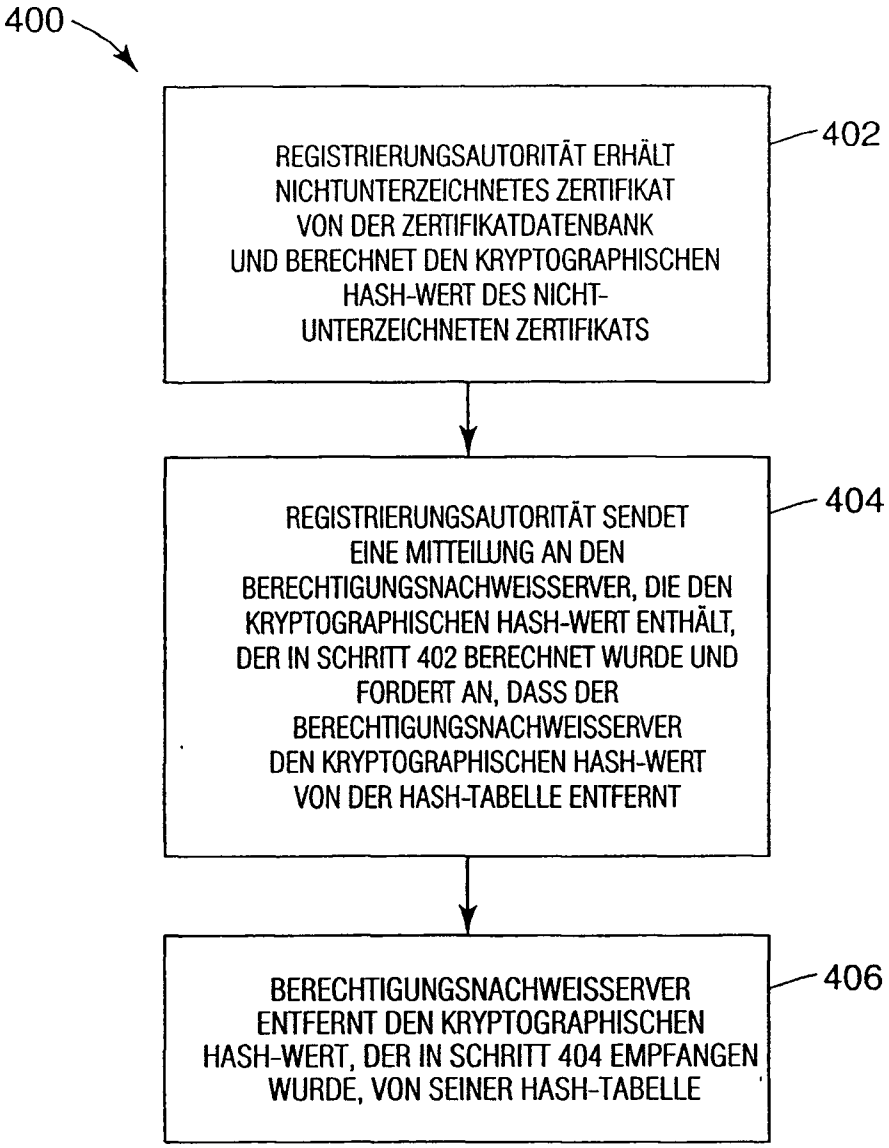
FIGUR 4



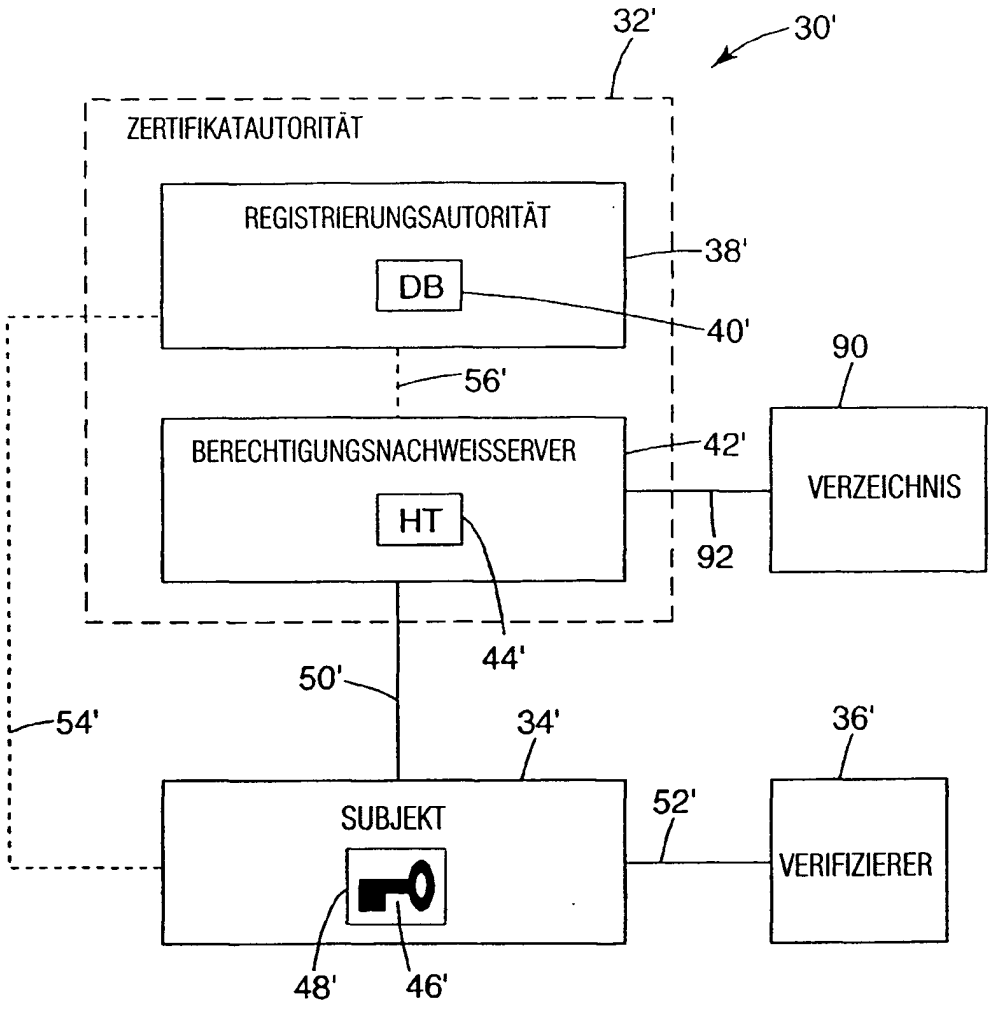
FIGUR 5


300
SUBJEKT SENDET DAS KURZFRISTIGE EINMALZERTIFIKAT AN DEN VERIFIZIERER
302
VERIFIZIERER VERIFIZIERT, DASS DAS ABLAUFDATUM/ZEIT IN DEM KURZFRISTIGEN EINMALZERTIFIKAT NICHT ABGELAUFEN IST
304
VERIFIZIERER VERWENDET DEN ÖFFENTLICHEN SCHLÜSSEL DES BERECHTIGUNGSNACHWEISSERVERS ZUM VERIFIZIEREN DER SIGNATUR AUF DEM KURZFRISTIGEN EINMALZERTIFIKAT
306
SUBJEKT ZEIGT KENNTNIS DES PRIVATEN SCHLÜSSELS, DER DEM ÖFFENTLICHEN SCHLÜSSEL IN DEM KURZFRISTIGEN EINMALZERTIFIKAT ZUGEORDNET IST
308

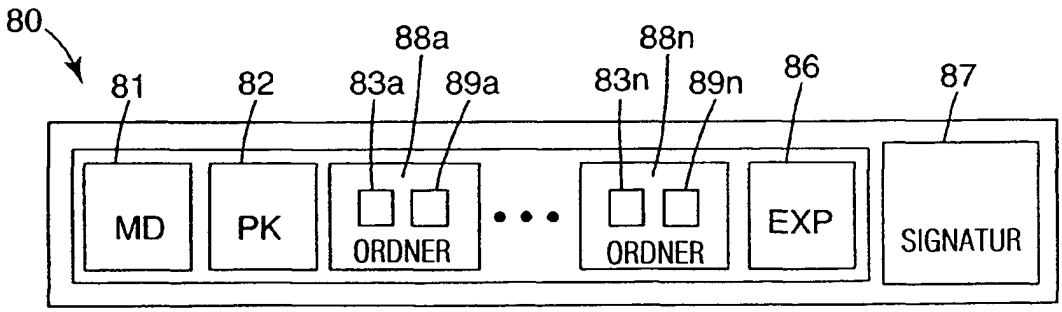
FIGUR 6


400
REGISTRIERUNGSAUTORITÄT ERHÄLT NICHTUNTERZEICHNETES ZERTIFIKAT VON DER ZERTIFIKATDATENBANK UND BERECHNET DEN KRYPTOGRAPHISCHEN HASH-WERT DES NICHT-UNTERZEICHNETEN ZERTIFIKATS
402
REGISTRIERUNGSAUTORITÄT SENDET EINE MITTEILUNG AN DEN BERECHTIGUNGSNACHWEISSERVER, DIE DEN KRYPTOGRAPHISCHEN HASH-WERT ENTHÄLT, DER IN SCHRITT 402 BERECHNET WURDE UND FORDERT AN, DASS DER BERECHTIGUNGSNACHWEISSERVER DEN KRYPTOGRAPHISCHEN HASH-WERT VON DER HASH-TABELLE ENTFERNT
404
BERECHTIGUNGSNACHWEISSERVER ENTFERNT DEN KRYPTOGRAPHISCHEN HASH-WERT, DER IN SCHRITT 404 EMPFANGEN WURDE, VON SEINER HASH-TABELLE
406

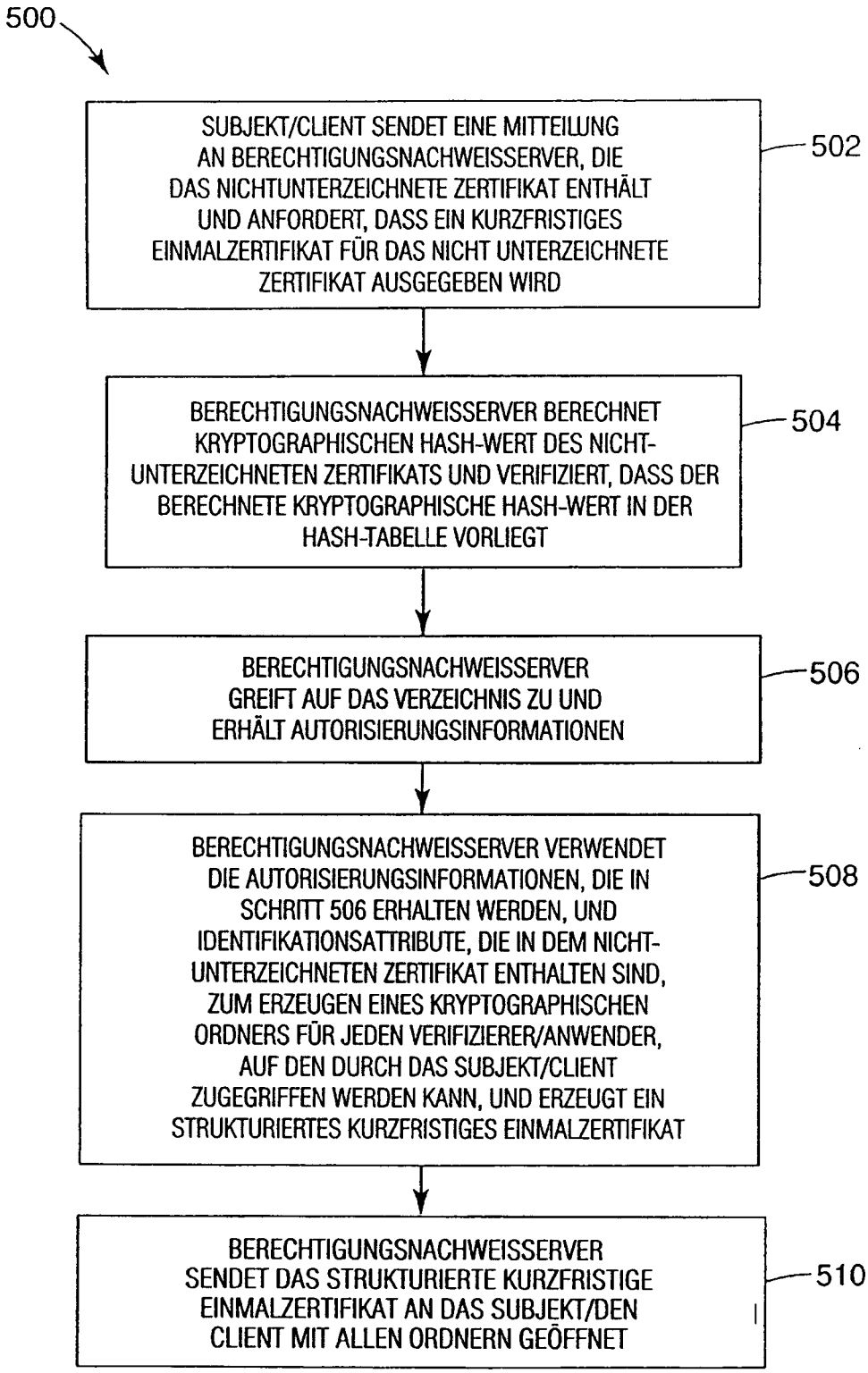
FIGUR 7



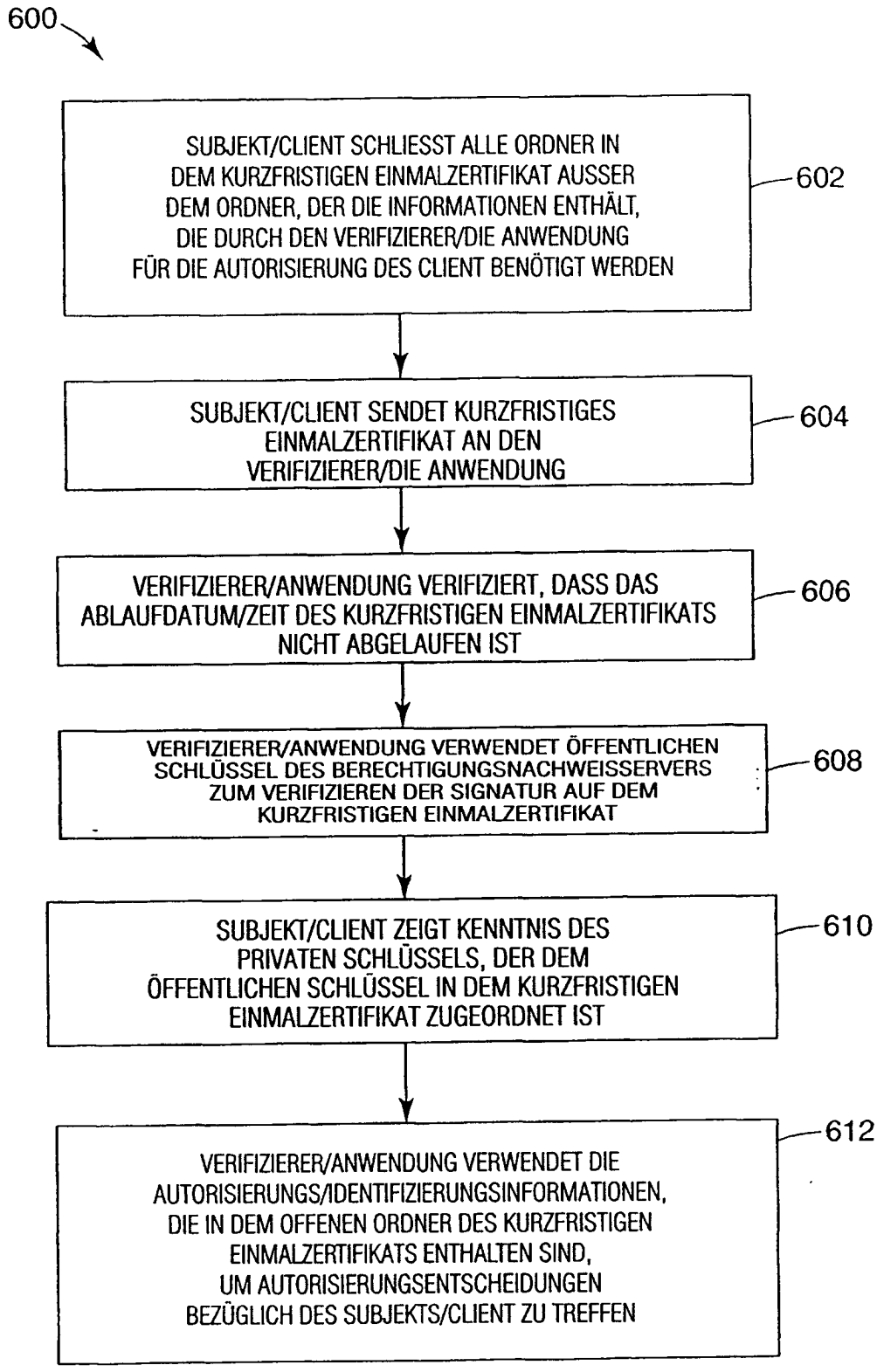
FIGUR 8



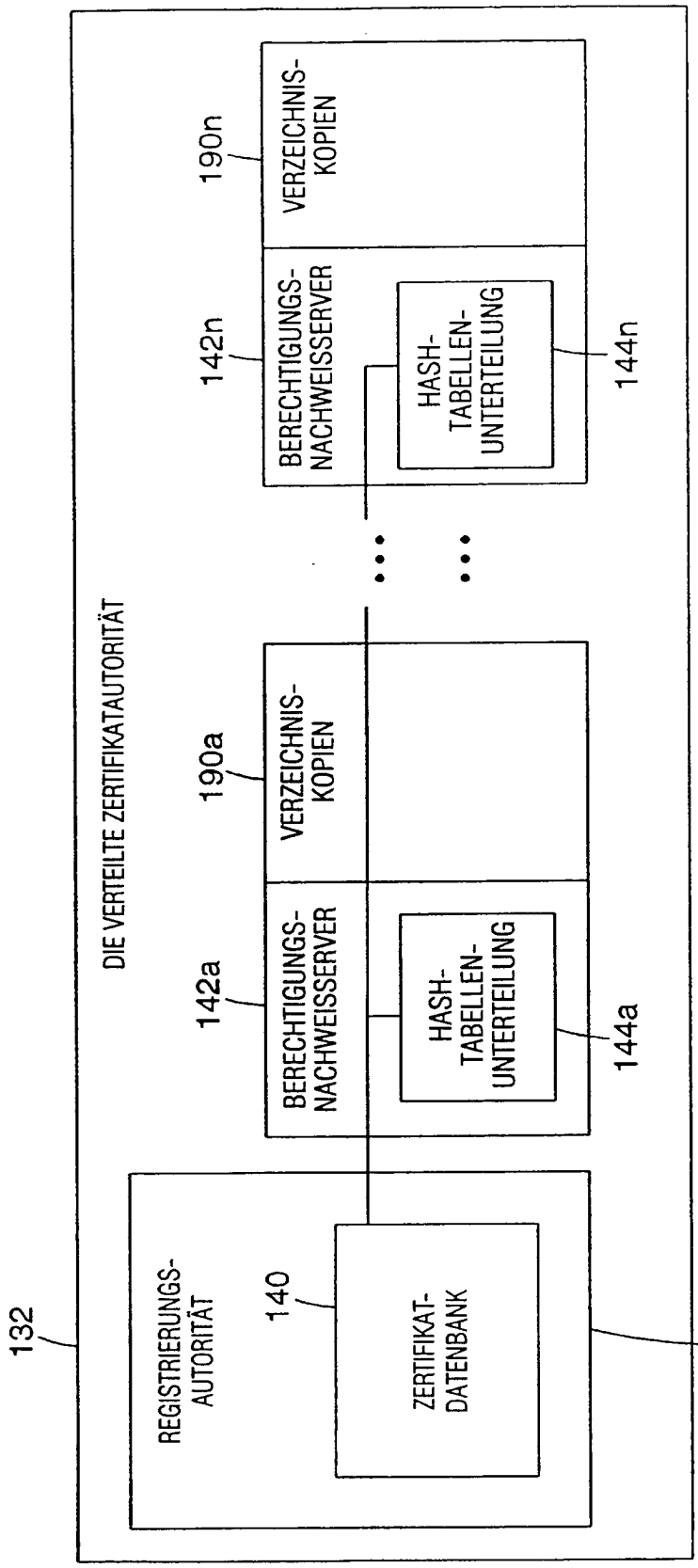
FIGUR 9


500
SUBJEKT/CLIENT SENDET EINE MITTEILUNG AN BERECHTIGUNGSNACHWEISSERVER, DIE DAS NICHTUNTERZEICHNETE ZERTIFIKAT ENTHÄLT UND ANFORDERT, DASS EIN KURZFRISTIGES EINMALZERTIFIKAT FÜR DAS NICHT UNTERZEICHNETE ZERTIFIKAT AUSGEGEBEN WIRD
502
BERECHTIGUNGSNACHWEISSERVER BERECHNET KRYPTOGRAPHISCHEN HASH-WERT DES NICHT-UNTERZEICHNETEN ZERTIFIKATS UND VERIFIZIERT, DASS DER BERECHNETE KRYPTOGRAPHISCHE HASH-WERT IN DER HASH-TABELLE VORLIEGT
504
BERECHTIGUNGSNACHWEISSERVER GREIFT AUF DAS VERZEICHNIS ZU UND ERHÄLT AUTORISIERUNGSINFORMATIONEN
506
BERECHTIGUNGSNACHWEISSERVER VERWENDET DIE AUTORISIERUNGSINFORMATIONEN, DIE IN SCHRITT 506 ERHALTEN WERDEN, UND IDENTIFIKATIONSATTRIBUTE, DIE IN DEM NICHT-UNTERZEICHNETEN ZERTIFIKAT ENTHALTEN SIND, ZUM ERZEUGEN EINES KRYPTOGRAPHISCHEN ORDNERS FÜR JEDEN VERIFIZIERER/ANWENDER, AUF DEN DURCH DAS SUBJEKT/CLIENT ZUGEGRIFFEN WERDEN KANN, UND ERZEUGT EIN STRUKTURIERTES KURZFRISTIGES EINMALZERTIFIKAT
508
BERECHTIGUNGSNACHWEISSERVER SENDET DAS STRUKTURIERTE KURZFRISTIGE EINMALZERTIFIKAT AN DAS SUBJEKT/DEN CLIENT MIT ALLEN ORDNERN GEÖFFNET
510

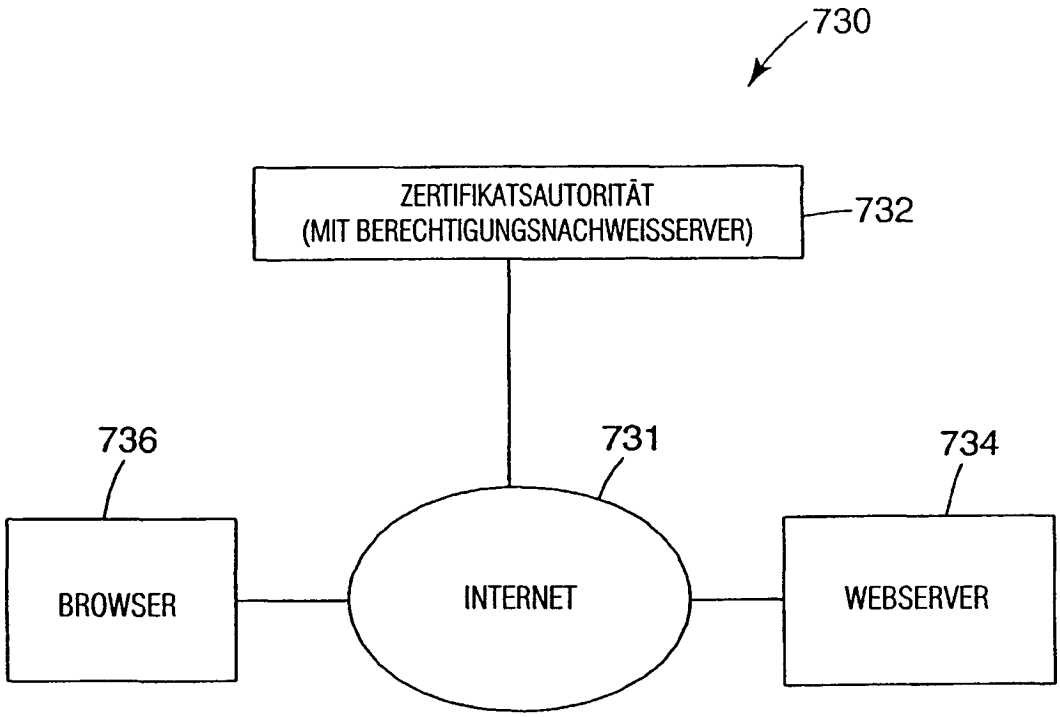
FIGUR 10


600
SUBJEKT/CLIENT SCHLIESST ALLE ORDNER IN DEM KURZFRISTIGEN EINMALZERTIFIKAT AUSSER DEM ORDNER, DER DIE INFORMATIONEN ENTHÄLT, DIE DURCH DEN VERIFIZIERER/DIE ANWENDUNG FÜR DIE AUTORISIERUNG DES CLIENT BENÖTIGT WERDEN
602
SUBJEKT/CLIENT SENDET KURZFRISTIGES EINMALZERTIFIKAT AN DEN VERIFIZIERER/DIE ANWENDUNG
604
VERIFIZIERER/ANWENDUNG VERIFIZIERT, DASS DAS ABLAUFDATUM/ZEIT DES KURZFRISTIGEN EINMALZERTIFIKATS NICHT ABGELAUFEN IST
606
VERIFIZIERER/ANWENDUNG VERWENDET ÖFFENTLICHEN SCHLÜSSEL DES BERECHTIGUNGSNACHWEISSERVERS ZUM VERIFIZIEREN DER SIGNATUR AUF DEM KURZFRISTIGEN EINMALZERTIFIKAT
608
SUBJEKT/CLIENT ZEIGT KENNTNIS DES PRIVATEN SCHLÜSSELS, DER DEM ÖFFENTLICHEN SCHLÜSSEL IN DEM KURZFRISTIGEN EINMALZERTIFIKAT ZUGEORDNET IST
610
VERIFIZIERER/ANWENDUNG VERWENDET DIE AUTORISIERUNGS/IDENTIFIZIERUNGSINFORMATIONEN, DIE IN DEM OFFENEN ORDNER DES KURZFRISTIGEN EINMALZERTIFIKATS ENTHALTEN SIND, UM AUTORISIERUNGSENTSCHEIDUNGEN BEZÜGLICH DES SUBJEKTS/CLIENT ZU TREFFEN
612

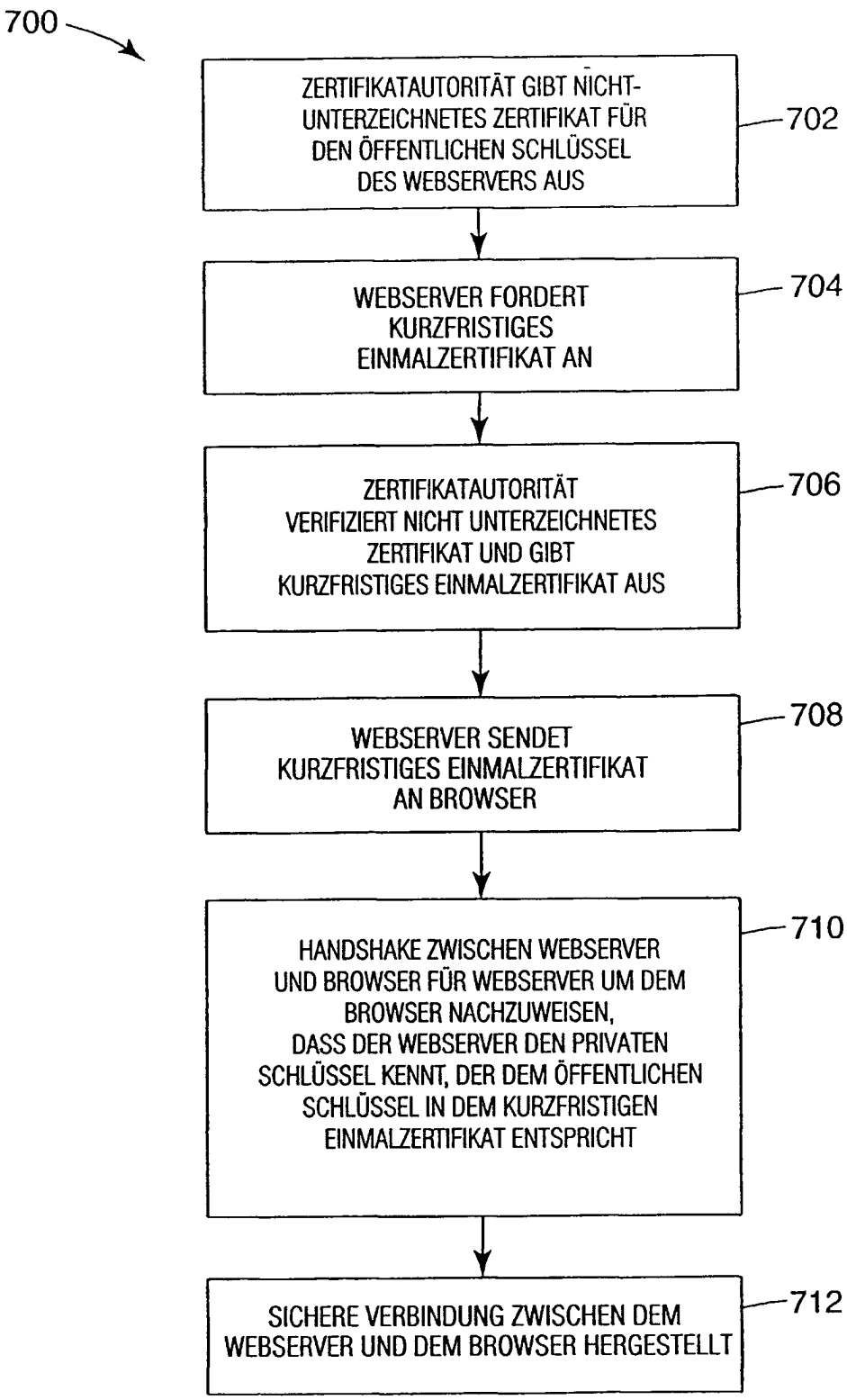
FIGUR 11


DIE VERTEILTE ZERTIFIKATAUTORITÄT
132
REGISTRIERUNGS-AUTORITÄT
140
ZERTIFIKAT-DATENBANK
138
BERECHTIGUNGS-NACHWEISSERVER
142a
HASH-TABELLEN-UNTERTEILUNG
144a
VERZEICHNIS-KOPIEN
190a
BERECHTIGUNGS-NACHWEISSERVER
142n
HASH-TABELLEN-UNTERTEILUNG
144n
VERZEICHNIS-KOPIEN
190n

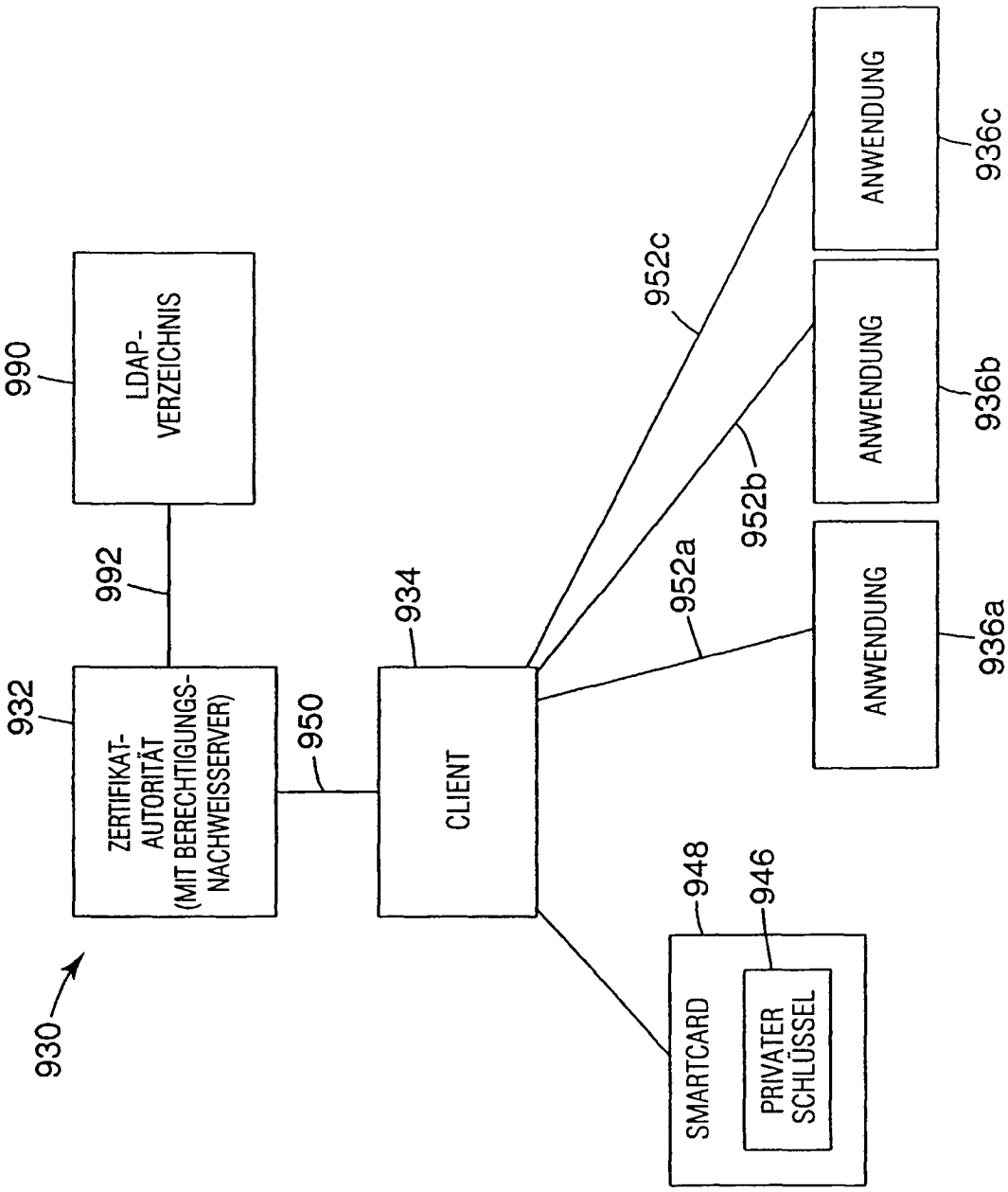
FIGUR 12


730
ZERTIFIKATSAUTORITÄT
(MIT BERECHTIGUNGSNACHWEISSERVER)
732
736
731
734
BROWSER
INTERNET
WEBSERVER

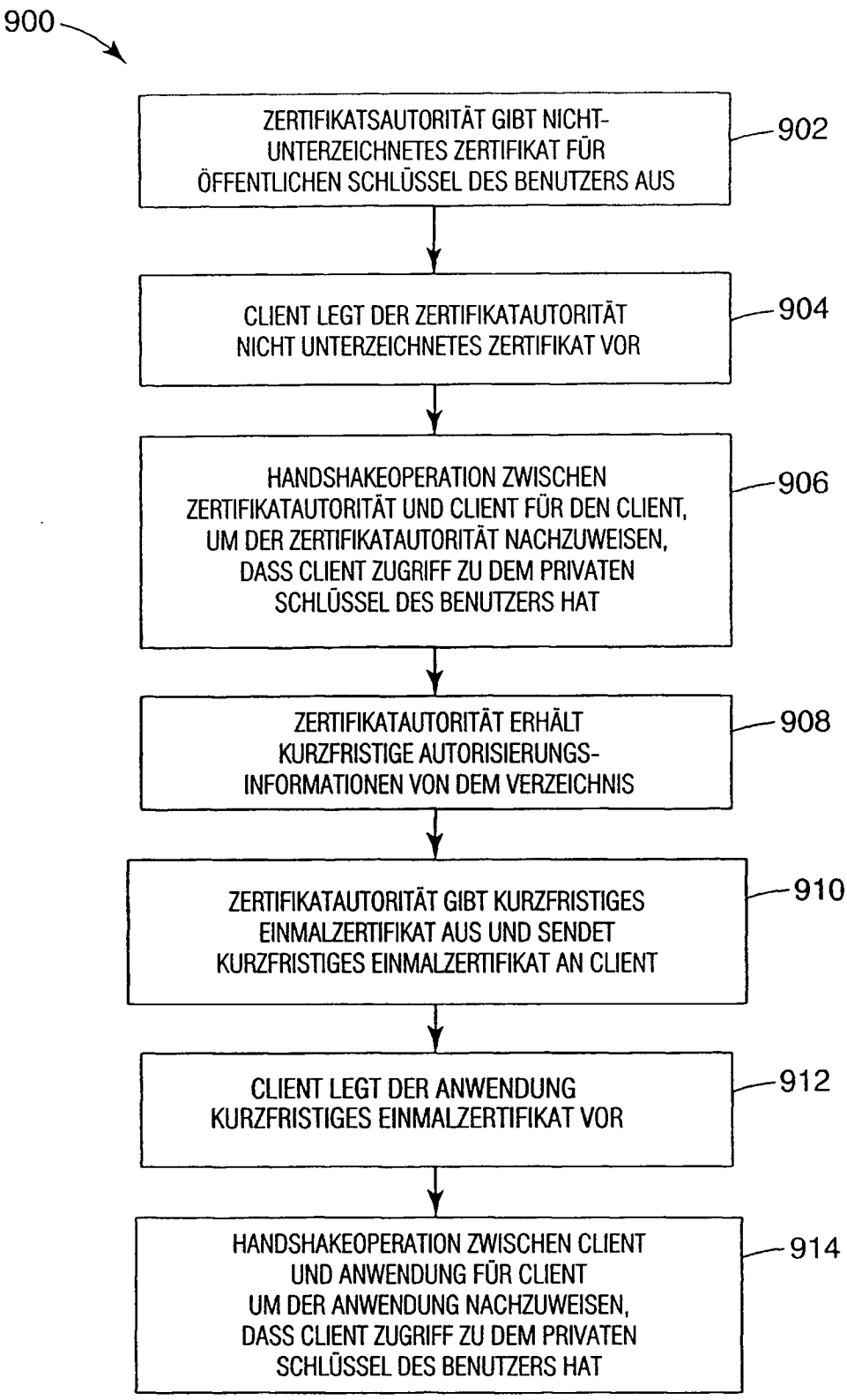
FIGUR 13


700
ZERTIFIKATAUTORITÄT GIBT NICHT-UNTERZEICHNETES ZERTIFIKAT FÜR DEN ÖFFENTLICHEN SCHLÜSSEL DES WEBSERVERS AUS
702
WEBSERVER FORDERT KURZFRISTIGES EINMALZERTIFIKAT AN
704
ZERTIFIKATAUTORITÄT VERIFIZIERT NICHT UNTERZEICHNETES ZERTIFIKAT UND GIBT KURZFRISTIGES EINMALZERTIFIKAT AUS
706
WEBSERVER SENDET KURZFRISTIGES EINMALZERTIFIKAT AN BROWSER
708
HANDSHAKE ZWISCHEN WEBSERVER UND BROWSER FÜR WEBSERVER UM DEM BROWSER NACHZUWEISEN, DASS DER WEBSERVER DEN PRIVATEN SCHLÜSSEL KENNT, DER DEM ÖFFENTLICHEN SCHLÜSSEL IN DEM KURZFRISTIGEN EINMALZERTIFIKAT ENTSPRICHT
710
SICHERE VERBINDUNG ZWISCHEN DEM WEBSERVER UND DEM BROWSER HERGESTELLT
712

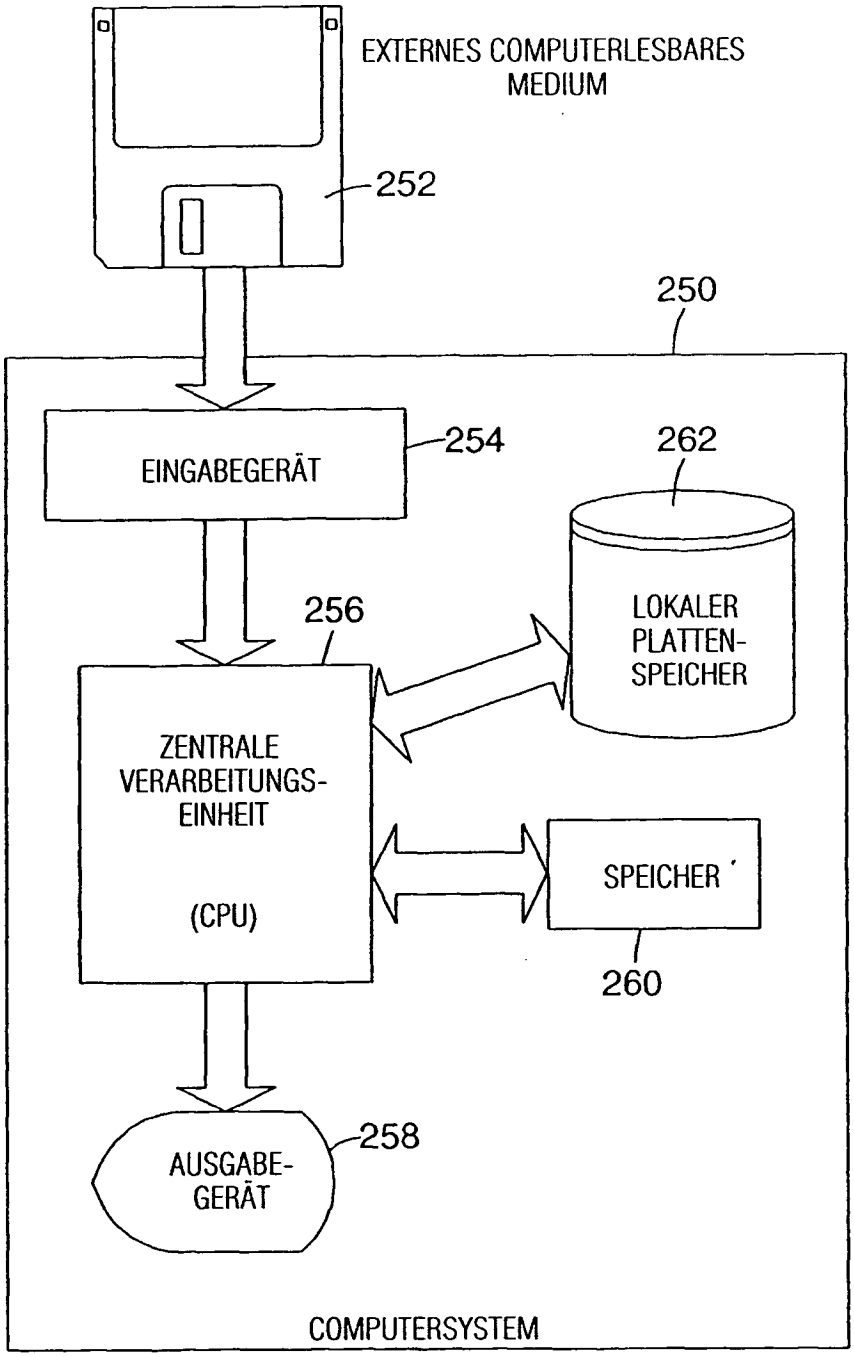
FIGUR 14


930
932
ZERTIFIKAT-AUTORITÄT (MIT BERECHTIGUNGS-NACHWEISSERVER)
950
CLIENT
934
990
LDAP-VERZEICHNIS
992
952a
952b
952c
ANWENDUNG
936a
ANWENDUNG
936b
ANWENDUNG
936c
SMARTCARD
948
PRIVATER SCHLÜSSEL
946

FIGUR 15


900
ZERTIFIKATSAUTORITÄT GIBT NICHT-UNTERZEICHNETES ZERTIFIKAT FÜR ÖFFENTLICHEN SCHLÜSSEL DES BENUTZERS AUS
902
CLIENT LEGT DER ZERTIFIKATAUTORITÄT NICHT UNTERZEICHNETES ZERTIFIKAT VOR
904
HANDSHAKEOPERATION ZWISCHEN ZERTIFIKATAUTORITÄT UND CLIENT FÜR DEN CLIENT, UM DER ZERTIFIKATAUTORITÄT NACHZUWEISEN, DASS CLIENT ZUGRIFF ZU DEM PRIVATEN SCHLÜSSEL DES BENUTZERS HAT
906
ZERTIFIKATAUTORITÄT ERHÄLT KURZFRISTIGE AUTORISIERUNGS-INFORMATIONEN VON DEM VERZEICHNIS
908
ZERTIFIKATAUTORITÄT GIBT KURZFRISTIGES EINMALZERTIFIKAT AUS UND SENDET KURZFRISTIGES EINMALZERTIFIKAT AN CLIENT
910
CLIENT LEGT DER ANWENDUNG KURZFRISTIGES EINMALZERTIFIKAT VOR
912
HANDSHAKEOPERATION ZWISCHEN CLIENT UND ANWENDUNG FÜR CLIENT UM DER ANWENDUNG NACHZUWEISEN, DASS CLIENT ZUGRIFF ZU DEM PRIVATEN SCHLÜSSEL DES BENUTZERS HAT
914

FIGUR 16


EXTERNES COMPUTERLESBARES MEDIUM
252
250
EINGABEGERÄT
254
262
LOKALER PLATTEN-SPEICHER
256
ZENTRALE VERARBEITUNGS-EINHEIT
(CPU)
SPEICHER
260
AUSGABE-GERÄT
258
COMPUTERSYSTEM

FIGUR 17