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

(10) **DE 601 07 634 T2** 2005.12.08

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 185 027 B1**
(21) Deutsches Aktenzeichen: **601 07 634.6**
(96) Europäisches Aktenzeichen: **01 120 564.8**
(96) Europäischer Anmeldetag: **29.08.2001**
(97) Erstveröffentlichung durch das EPA: **06.03.2002**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **08.12.2004**
(47) Veröffentlichungstag im Patentblatt: **08.12.2005**

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

(30) Unionspriorität:
2000261065 30.08.2000 JP

(84) Benannte Vertragsstaaten:
DE, FR, GB, IT

(73) Patentinhaber:
Hitachi Ltd., Tokio/Tokyo, JP

(74) Vertreter:
Strehl, Schübel-Hopf & Partner, 80538 München

(72) Erfinder:
Fujishiro, Takahiro, Tokyo 100-8220, JP; Tezuka, Satoru, Tokyo 100-8220, JP; Kumagai, Yoko, Tokyo 100-8220, JP; Morio, Tomoharu, Tokyo 100-8220, JP; Miyazaki, Yutaka, Tokyo 100-8220, JP

(54) Bezeichnung: **Verfahren und Vorrichtung zur Authentifizierung der Gültigkeit eines Zertifikats**

Beschreibung

HINTERGRUND DER ERFINDUNG

[0001] Die vorliegende Erfindung betrifft Techniken in einer PKI (Public Key Infrastructure, Infrastruktur für einen öffentlichen Schlüssel), die gut dafür geeignet sind, die Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel festzustellen, das dazu dient, eine Signatur für einen elektronischen Vorgang zu prüfen, der an einem bestimmten Terminal erhalten wird und das von einer Zertifizierungsstelle ausgegeben wurde, das nicht die Stelle ist, der das betreffende Terminal vertraut.

[0002] In verschiedenen Organisationen und Parteien auf privater und öffentlicher Basis wurden PKIs (Public Key Infrastructures, siehe oben) eingeführt und zur Anwendung gebracht, um Vorgänge elektronisch ausführen zu können, die bisher auf Papier erfolgt sind.

[0003] Die Fig. 12 zeigt die Beziehungen zwischen einer Anzahl von Zertifikationsstellen bei den derzeit bestehenden PKIs.

[0004] Wie gezeigt bilden die Zertifikationsstellen, die Zertifikate für öffentliche Schlüssel ausgeben und verwalten, eine Gruppe mit Baumstruktur, an deren Spitze die Quellen-Zertifikationsstelle CA1 steht. Die Gruppe wird "Sicherheitsdomain" genannt. Die Quellen-Zertifikationsstelle CA1 gibt Zertifikate für öffentliche Schlüssel an die direkt unter ihr liegenden Zertifikationsstellen $CA2_1$ bis $CA2_n$ aus. Jede der Zertifikationsstellen $CA2_1$ bis $CA2_n$ gibt Zertifikate für öffentliche Schlüssel an die direkt unter ihnen liegenden Zertifikationsstellen $CA3_1$ bis $CA3_n$ aus. Auf diese Weise gibt jede an einer oberhalb im Baum liegenden Stelle Zertifikate für öffentliche Schlüssel an die direkt unter ihr liegenden Stellen aus. Die Zertifikationsstellen CAS_1 bis CAS_{nm} ganz unten am Baum (im folgenden "Terminal-Zertifikationsstellen" genannt) geben Zertifikate für öffentliche Schlüssel an Nutzerterminals EE_1 bis EE_x aus, an denen elektronische Vorgänge ausgeführt werden (im folgenden "Endeinheiten" genannt).

[0005] Die Gültigkeit eines geheimen Schlüssels (Signaturschlüssels), den die einzelnen Endeinheiten EE_1 bis EE_x für die Signatur eines elektronischen Dokuments verwenden, wird mit dem Zertifikat für den öffentlichen Schlüssel bescheinigt, das von der einen der Terminal-Zertifikationsstellen CAS_1 bis CAS_{nm} ausgegeben wurde, die für die betreffende Endeinheit zuständig ist. Die Gültigkeit des geheimen Schlüssels, den die einzelnen Terminal-Zertifikationsstellen CAS_1 bis CAS_{nm} für die Signatur des Zertifikats für den ausgegebenen öffentlichen Schlüssel verwenden, wird von dem Zertifikat für den öffentlichen Schlüssel bescheinigt, das von der einen der Zertifikationsstellen $CA(S-1)_1$ bis $CA(S-1)_{n(m-1)}$ ausgegeben wird, die für die betreffende Terminal-Zertifikationsstelle zuständig ist. Der geheime Schlüssel, der für die Signatur von jeder den Endeinheiten EE_1 bis EE_x verwendet wird, wird schließlich von dem Zertifikat für den öffentlichen Schlüssel bescheinigt, das von der Quellen-Zertifikationsstelle CA1 ausgegeben wird. Die Zertifikationsstelle, die schließlich die Gültigkeit der Schlüssel bescheinigt, die für die Signaturen von den Endeinheiten EE_1 bis EE_x verwendet werden, der mit anderen Worten die Endeinheiten EE_1 bis EE_x vertrauen und die sich im Baum ganz oben befindet, wird "Vertrauensanker" genannt.

[0006] Wie in der Fig. 12 gezeigt, bringt die Endeinheit EE_1 an einem elektronischen Dokument wie einer geschriebenen Anmeldung, die zu der Endeinheit EE_x übertragen werden soll, unter Verwendung ihres eigenen geheimen Schlüssels eine Signatur an. Außerdem hängt die Endeinheit EE_1 an das signierte elektronische Dokument ein Zertifikat für einen öffentlichen Schlüssel an, das zu dem genannten geheimen Schlüssel paßt und das von der Terminal-Zertifikationsstelle CAS_1 für diese Endeinheit EE_1 ausgegeben wurde, und sendet dann das Dokument und das Zertifikat zu der Endeinheit EE_x.

[0007] Die Endeinheit EE_x kann die Signatur des von der Endeinheit EE_1 erhaltenen elektronischen Dokuments anhand des Zertifikats für den öffentlichen Schlüssel prüfen, das an das elektronische Dokument angehängt wurde. Da jedoch das Zertifikat für den öffentlichen Schlüssel nicht von der Terminal-Zertifikationsstelle CAS_{nm} für die Endeinheit EE_x ausgegeben wurde, kann die Endeinheit EE_x dem betreffenden Zertifikat für den öffentlichen Schlüssel nicht unmittelbar vertrauen. Die Endeinheit EE_x muß sicherstellen, daß die Gültigkeit des betreffenden Zertifikats für den öffentlichen Schlüssel von der Quellen-Zertifikationsstelle CA1 bescheinigt wird, die der Vertrauensanker für die Endeinheit EE_x ist. Ein Gültigkeits-Authentifizierungsprozeß für das Zertifikat für den öffentlichen Schlüssel wird mit den folgenden Schritten ausgeführt:

(1) Suche nach dem Pfad vom Vertrauensanker zu der Zertifikationsstelle, die das Zertifikat für den öffentlichen Schlüssel ursprünglich ausgegeben hat:

Mit einem Vertrauensanker (hier der Quellen-Zertifikationsstelle CA1) als Start-Zertifikationsstelle wird der Prozeß des Untersuchens der Ausgabe-Zielorte für die Zertifikate für öffentliche Schlüssel, die von der Start-Zertifikationsstelle ausgegeben wurden, und der weiteren Untersuchung, ob sich unter den untersuchten Ausgabe-Zielorten nachgeordnete Zertifikationsstellen befinden, die Ausgabe-Zielorte von Zertifikaten für öffentliche Schlüssel sind, die von den nachgeordneten Zertifikationsstellen ausgegeben wurden, solange fortgesetzt, bis sich unter den unter-

suchten Ausgabeorten diejenige Zertifikationsstelle befindet, die das betreffende Zertifikat für einen öffentlichen Schlüssel ursprünglich ausgegeben hat (hier die Terminal-Zertifikationsstelle CAS_1 für die Endeinheit EE_1). Es wird damit nach dem Pfad vom Vertrauensanker zu der Zertifikationsstelle gesucht, die das betreffende Zertifikat für den öffentlichen Schlüssel ursprünglich ausgegeben hat.

(2) Verifikation des festgestellten Pfades:

Es werden die von den einzelnen Zertifikationsstellen auf dem im Schritt (1) festgestellten Pfad an die jeweils direkt unterhalb auf dem Pfad angeordneten Zertifikationsstellen ausgegebenen Zertifikate für öffentliche Schlüssel aufgenommen. Der Prozeß des Verifizierens der Signatur des betreffenden Zertifikats für einen öffentlichen Schlüssel, dessen Gültigkeit zu bescheinigen ist (hier das Zertifikat für öffentliche Schlüssel, das von der Terminal-Zertifikationsstelle CAS_1 an die Endeinheit EE_1 ausgegeben wurde), wird im Lichte des von der direkt oberhalb der Zertifikationsstelle (hier der Terminal-Zertifikationsstelle CAS_1), die das betreffende Zertifikat für einen öffentlichen Schlüssel ausgegeben hat, angeordneten Zertifikationsstelle (hier der Zertifikationsstelle $CA(S-1)_1$) ausgegebenen Zertifikats für den öffentlichen Schlüssel, und das folgende Überprüfen, wenn die Verifikation positiv ist, der Signatur des Zertifikats für den öffentlichen Schlüssel, der von der direkt oberhalb angeordneten Zertifikationsstelle ausgegeben wurde, im Lichte des Zertifikats für einen öffentlichen Schlüssel, der von der direkt unterhalb angeordneten Zertifikationsstelle ausgegeben wurde, fortgesetzt, bis die oberhalb angeordnete Zertifikationsstelle den Vertrauensanker erreicht. Wenn die Verifikation der Signatur sich bis zum Vertrauensanker als gut herausstellt, wird die Gültigkeit des Zertifikats für den öffentlichen Schlüssel, die zu prüfen ist, bescheinigt.

[0008] Die Endeinheit EE_x kann die Gültigkeit des von der Endeinheit EE_1 erhaltenen elektronischen Dokuments dadurch bescheinigen, daß die Signatur des elektronischen Dokuments unter Verwendung des an dem elektronischen Dokument angebrachten Zertifikats für den öffentlichen Schlüssel verifiziert wird, und daß die Gültigkeit des Zertifikats für den öffentlichen Schlüssel, das zum Überprüfen der Signatur des elektronischen Dokuments verwendet wird, gemäß den Schritten (1) und (2) bescheinigt wird.

[0009] B. Schneier: 'Applied Cryptography, Protocols, Algorithms, and Source Code in C', John Wiley & Sons, New York, USA, ISBN: 0-471-11709-9, Seiten 574 bis 577 beschreibt ein Verfahren zur Überprüfung der Gültigkeit eines Zertifikats mit den Schritten, die im Oberbegriff des Patentanspruchs 1 genannt sind.

[0010] Bei der obigen Vorgehensweise wird vorausgesetzt, daß der Prozeß zur Überprüfung der Gültigkeit des Zertifikats für den öffentlichen Schlüssel in der Endeinheit ausgeführt wird. Der Aufwand für den Prozeß zur Überprüfung der Gültigkeit eines Zertifikats ist jedoch groß, so daß die Endeinheiten eine hohe Verarbeitungskapazität aufweisen müssen, um den Prozeß ausführen zu können. Von der IETF wurde daher vorgeschlagen, daß ein Server zum Überprüfen der Gültigkeit eines Zertifikats vorgesehen wird, der mit der Endeinheit über ein Netzwerk verbunden ist und der anstelle der Endeinheit die Gültigkeit des Zertifikats für den öffentlichen Schlüssel überprüft.

ZUSAMMENFASSUNG DER ERFINDUNG

[0011] Der bekannte Server zum Überprüfen der Gültigkeit eines Zertifikats überprüft die Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel durch Ausführen der oben angegebenen Schritte (1) und (2) jedesmal dann, wenn er eine Anforderung dazu von einer Endeinheit erhält. Die Zeitspanne zum Ausführen der Schritte (1) und (2) von der Anforderung der Endeinheit zur Überprüfung der Gültigkeit des Zertifikats für den öffentlichen Schlüssel bis zum Erhalten des Ergebnisses der Überprüfung ist daher verlängert.

[0012] Bei dem Beispiel der Fig. 12 gibt es nur eine Sicherheitsdomain. Es existiert jedoch parallel eine Vielzahl von Sicherheitsdomains, da verschiedene Organisationen und Parteien auf privater und öffentlicher Basis PKIs eingeführt und zur Verwendung freigegeben haben. Unter den verschiedenen Sicherheitsdomains kann der Prozeß zum Überprüfen der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel wie in den Schritten (1) und (2) durch eine Kreuz-Zertifizierung derart erfolgen, daß die Quellen-Zertifikationsstellen der einzelnen Sicherheitsdomains die Zertifikate für öffentliche Schlüssel gegenseitig austauschen, oder daß eine Brücken-Zertifikationsstelle geschaffen wird, die eine solche Kreuz-Zertifikation zwischen den Quellen-Zertifikationsstellen für die einzelnen Sicherheitsdomains ausführt. Wenn der Prozeß zum Überprüfen der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel bei einer Vielzahl von Sicherheitsdomains auf diese Weise ausgeführt wird, steigt jedoch die Anzahl von Zertifikationsstellen an, und die Beziehungen zwischen den Zertifikationsstellen werden komplizierter als die Baumstruktur der Fig. 12, so daß die Belastung beim Ausführen der Schritte (1) und (2) ansteigt. Die Zeitspanne von der Anforderung der Endeinheit zum Überprüfen der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel bis zum Erhalt des Ergebnisses der Überprüfung steigt damit ebenfalls weiter an und führt zu einer Verschlechterung des Services.

[0013] Die vorliegende Erfindung erfolgte ange-

sichts der obigen Umstände, ihre Aufgabe ist es, die Zeitspanne von einer Anforderung zum Überprüfen der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel bis zur Feststellung der Gültigkeit zu verkürzen.

[0014] Zur Lösung der Aufgabe wird erfindungsgemäß in einem Server zum Überprüfen der Gültigkeit eines Zertifikats, der mit einer Anzahl von Terminals (Endeinheiten) und Zertifikationsstellen über ein Netzwerk verbunden ist, in Verbindung mit einer Anforderung von einem bestimmten Terminal zur Überprüfung der Gültigkeit eines von einer Zertifikationsstelle ausgegebenen Zertifikats für einen öffentlichen Schlüssel, die keine Zertifikationsstelle ist, der vom Terminal vertraut wird, der im folgenden angegebene Prozeß ausgeführt.

[0015] Unabhängig von der Anforderung eines Terminals zur Überprüfung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel werden möglicherweise periodisch die folgenden Schritte ausgeführt:
Ein Pfadsuchschritt, bei dem ein Verfahren ausgeführt wird, in dem mit einer beliebigen Zertifizierungsstelle als Startzertifizierungsstelle der Ausgabe-Zielort für ein von der Startzertifizierungsstelle ausgegebenes Zertifikat für einen öffentlichen Schlüssel festgestellt wird und, wenn eine Zertifizierungsstelle der Ausgabe-Zielort ist, der Ausgabe-Zielort des von der Ausgabe-Zielort-Zertifizierungsstelle ausgegebenen Zertifikats für einen öffentlichen Schlüssel festgestellt wird, wobei das Verfahren fortgesetzt wird, bis alle Ausgabe-Zielorte der Zertifikate für öffentliche Schlüssel Terminals sind, wodurch die Pfade gefunden werden, die sich von der Startzertifizierungsstelle bis zu den Terminal-Zertifizierungsstellen erstrecken, die Zertifikate für öffentliche Schlüssel an Terminals ausgegeben haben; ein Pfadverifizierungsschritt, bei dem für jeden bei der Pfadsuche gefundenen Pfad ein Verfahren ausgeführt wird, in dem die Startzertifizierungsstelle ganz oben angeordnet wird und die Signatur des Zertifikats für den öffentlichen Schlüssel, das von der Terminal-Zertifizierungsstelle auf dem zugehörigen Pfad ausgegeben wurde, verifiziert wird im Hinblick auf das Zertifikat für den öffentlichen Schlüssel, das von der direkt darüber angeordneten Zertifizierungsstelle ausgegeben wurde, und bei positiv ausgegangener Verifizierung die Signatur des Zertifikats für den öffentlichen Schlüssel, das von der direkt darüber liegenden Zertifizierungsstelle ausgegeben wurde, verifiziert wird im Hinblick auf das Zertifikat für den öffentlichen Schlüssel, das von der wiederum darüber liegenden Zertifizierungsstelle ausgegeben wurde, wobei das Verfahren fortgesetzt wird, bis die direkt darüber liegende Zertifizierungsstelle die Startzertifizierungsstelle wird, wodurch die Pfade verifiziert werden; und
ein Pfadregistrierungsschritt, bei dem solche Pfade, für die die Pfadverifizierung positiv ausgegangen ist, in einer Datenbank registriert werden.

[0016] Wenn dann ein bestimmtes Terminal eine Anforderung zur Überprüfung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel, das von einer anderen Terminal-Zertifizierungsstelle als einer Zertifizierungsstelle ausgegeben wurde, der das Terminal vertraut, wird die Gültigkeit des Zertifikats für den öffentlichen Schlüssel dadurch überprüft, daß festgestellt wird, ob der Pfad zwischen der Zertifizierungsstelle, der das Terminal vertraut, und der Startzertifizierungsstelle sowie der Pfad zwischen der anderen Terminal-Zertifizierungsstelle und der Startzertifizierungsstelle in der Datenbank registriert sind.

[0017] Erfindungsgemäß braucht, wenn von einem bestimmten Terminal eine Anforderung zur Überprüfung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel erhalten wird, der Anforderung nicht durch die Suche nach dem Pfad vom Vertrauensanker des bestimmten Terminals zu der das Zertifikat ursprünglich ausgebenden Stelle und die Überprüfung des festgestellten Pfades in den obigen Schritten (1) und (2) gefolgt werden. Es ist demgemäß möglich, die Zeitspanne vom Erhalt der Anforderung auf die Überprüfung eines Zertifikats für einen öffentlichen Schlüssel bis zur Feststellung der Gültigkeit davon zu verkürzen.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0018] Fig. 1 ist eine Darstellung des schematischen Aufbaus eines PKI-Systems, bei dem eine Ausführungsform der vorliegenden Erfindung angewendet wird;

[0019] Fig. 2 ist eine Darstellung der Beziehungen zwischen den einzelnen Zertifikationsstellen CA in dem PKI-System der Fig. 1;

[0020] Fig. 3 eine Blockdarstellung des schematischen Aufbaus einer Endeinheit EE in der Fig. 1;

[0021] Fig. 4 eine Blockdarstellung des schematischen Aufbaus der Zertifikationsstelle CA in der Fig. 1;

[0022] Fig. 5 eine Blockdarstellung des schematischen Aufbaus eines Zertifikationsprüfzentrums VC in der Fig. 1;

[0023] Fig. 6 eine Blockdarstellung eines Beispiels für den Hardwareaufbau der Endeinheiten EE, der Zertifikationsstellen CA und der Zertifikationsprüfzentren VC in den Fig. 3, Fig. 4 und Fig. 5;

[0024] Fig. 7 ein Flußdiagramm zur Erläuterung der Suche nach Pfaden, deren Überprüfung und Verwaltung, wie sie im Zertifikationsprüfzentrum VC der

Fig. 5 ausgeführt wird;

[0025] Fig. 8 ein Flußdiagramm zur Erläuterung der Suche nach Pfaden, deren Überprüfung und Verwaltung, wie sie im Zertifikationsprüfzentrum VC der Fig. 5 ausgeführt wird;

[0026] Fig. 9 eine Darstellung der Pfade, die sich von einer Brücken-Zertifikationsstelle CA_{bridge} zu Terminal-Zertifikationsstellen CA erstrecken und die von der Pfadsucheinheit **32** des Zertifikationsprüfzentrums VC im Falle der Zertifikationsstellen und der Beziehungen der Fig. 2 festgestellt werden;

[0027] Fig. 10 ein Flußdiagramm zur Erläuterung der Überprüfung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel durch das Zertifikationsprüfzentrum VC der Fig. 5;

[0028] Fig. 11 ein Flußdiagramm zur Erläuterung der Überprüfung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel durch das Zertifikationsprüfzentrum VC der Fig. 5; und

[0029] Fig. 12 eine Darstellung der Beziehungen zwischen einer Anzahl von Zertifikationsstellen bei einer bekannten PKI.

GENAUE BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

[0030] Es werden nun Ausführungsformen der vorliegenden Erfindung beschrieben.

[0031] Die Fig. 1 ist eine Darstellung des schematischen Aufbaus eines PKI-Systems, bei dem eine Ausführungsform der vorliegenden Erfindung angewendet wird.

[0032] Wie in der Fig. 1 gezeigt, ist das PKI-System bei dieser Ausführungsform so aufgebaut, daß eine Anzahl von Endeinheiten EE, die Nutzerterminals für elektronische Vorgänge sind oder Anforderungsannahmeserver für die Annahme von Anforderungen von Nutzerterminals, um elektronische Vorgänge für die Nutzerterminals auszuführen, eine Anzahl von Zertifikationsstellen CA für die Ausstellung und Verwaltung von Zertifikaten für öffentliche Schlüssel und ein Zertifikatprüfzentrum VC zum Überprüfen der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel gemäß einer Anforderung von der Endeinheit EE über ein Netzwerk NET verbunden sind, das zum Beispiel aus LANs, WANs und das diese verbindende Internet aufgebaut wird.

[0033] Die Fig. 2 ist eine Darstellung eines Beispiels für die Beziehungen zwischen den einzelnen Zertifikationsstellen CA in dem PKI-System der Fig. 1.

[0034] Wie gezeigt wird bei dem PKI-System dieser Ausführungsform davon ausgegangen, daß eine Anzahl von Sicherheitsdomains $SD(SD_1 – SD_3)$ auf privater und staatlicher Basis nebeneinander existieren. Einige der Sicherheitsdomains SD (in der Fig. 2 SD_2 und SD_3) sollen miteinander so in Beziehung stehen, daß ihre Quellen-Zertifikationsstellen CA (in der Fig. 2 CA_{21} und CA_{31}) eine Kreuz-Zertifizierung durch zum Beispiel die gegenseitige Ausstellung von Zertifikaten für öffentliche Schlüssel ausführen. Außerdem sollen die Quellen-Zertifikationsstellen CA der einzelnen Sicherheitsdomains SD (in der Fig. 2 CA_{11}, CA_{21} und CA_{31}) zwischen sich und einer Brücken-Zertifikationsstelle CA_{bridge} dadurch eine Kreuz-Zertifikation ausführen, daß zum Beispiel sowohl an die als auch von der Brücken-Zertifikationsstelle CA_{bridge} Zertifikate für öffentliche Schlüssel ausgegeben werden. Auf diese Weise kann von einer Zertifikationsstelle CA, die zu einer bestimmten Sicherheitsdomain SD gehört, und einer Zertifikationsstelle CA, die zu einer anderen Sicherheitsdomain SD gehört, ein Pfad ausgebildet werden, so daß die Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel, das von einer Zertifikationsstelle CA ausgegeben wird, von der anderen Zertifikationsstelle CA geprüft werden kann.

[0035] Es werden nun die Endeinheit EE, die Zertifikationsstelle CA und das Zertifikationsprüfzentrum VC erläutert, die das obige PKI-System bilden.

[0036] Zuerst wird die Endeinheit EE erläutert.

[0037] Die Fig. 3 ist eine Blockdarstellung des schematischen Aufbaus der Endeinheit EE.

[0038] Wie gezeigt umfaßt die Endeinheit EE eine Verarbeitungseinheit **10a**, eine Speichereinheit **10b**, eine Kommunikationseinheit **16**, die zur Kommunikation mit einer anderen Einrichtung über das Netzwerk NET dient, und eine Ein/Ausgabeeinheit **17**, die elektronische Dokumente eingibt und ausgibt, die von Nutzern erstellt wurden, oder elektronische Dokumente, die von anderen Endeinheiten EE oder anderen Nutzerterminals erhalten werden, und die Anweisungen von den Nutzern entgegennimmt.

[0039] Die Verarbeitungseinheit **10a** umfaßt eine Signaturerzeugungseinheit **14**, eine Signaturprüfeinheit **15** und eine Steuereinheit **18**, die die verschiedenen Einheiten der Endeinheit EE steuert.

[0040] Die Speichereinheit **10b** umfaßt eine Halteeinheit **11** für elektronische Dokumente, die die elektronischen Dokumente festhält, die von den Nutzern erstellt wurden (oder von Nutzerterminals erhalten werden, wenn die Endeinheit EE der Annahmeserver ist), eine Schlüsselhalteeinheit **12**, die geheime Schlüssel (Signaturschlüssel) enthält sowie die Zertifikate für öffentliche Schlüssel, die zu den jeweiligen geheimen Schlüsseln gehören, und eine Verifikati-

onssubjekt-Halteeinheit **13**, die die signierten elektronischen Dokumente und Zertifikate für öffentliche Schlüssel enthält, die von anderen Endeinheiten EE erhalten werden.

[0041] Bei diesem Aufbau wird, wenn die Steuereinheit **18** über die Ein/Ausgabeeinheit **17** eine Anweisung erhält, daß ein in der Halteeinheit **11** für elektronische Dokumente enthaltenes elektronisches Dokument zu einer anderen Endeinheit EE zu senden ist, das betreffende elektronische Dokument aus der Halteeinheit **11** ausgelesen und dieses Dokument der Signaturerzeugungseinheit **14** übergeben. Die Signaturerzeugungseinheit **14** erzeugt eine Signatur für das betreffende elektronische Dokument unter Verwendung eines geheimen Schlüssels aus der Schlüsselhalteeinheit **12**. Danach erzeugt die Steuereinheit **18** ein signiertes elektronisches Dokument dadurch, daß die von der Signaturerzeugungseinheit **14** erzeugte Signatur an das aus der Halteeinheit **11** ausgelesene elektronische Dokument angehängt wird. An das erzeugte signierte elektronische Dokument wird außerdem ein Zertifikat für einen öffentlichen Schlüssel aus der Schlüsselhalteeinheit **12** angehängt, woraufhin es dann mittels der Kommunikationseinheit **16** zu der Adresse der Endeinheit EE übertragen wird, die der vom Nutzer angegebene Übertragungs-Zielort ist.

[0042] Wenn die Steuereinheit **18** ein signiertes elektronisches Dokument und ein Zertifikat für einen öffentlichen Schlüssel über die Kommunikationseinheit **16** von einer anderen Endeinheit EE aufnimmt, veranlaßt sie, daß die Verifikationssubjekt-Halteeinheit **13** das Dokument festhält, und teilt gleichzeitig die Halteoperation der Signaturprüfeinheit **15** mit. Die Signaturprüfeinheit **15** prüft die Signatur des signierten elektronischen Dokuments in der Verifikationssubjekt-Halteeinheit **13** unter Verwendung des zusammen mit dem elektronischen Dokument erhaltenen Zertifikats für den öffentlichen Schlüssel. Nur wenn die Überprüfung positiv verläuft, wird das signierte elektronische Dokument als legal erachtet und gegebenenfalls von der Ein/Ausgabeeinheit **17** ausgegeben.

[0043] Wenn jedoch bei positiv verlaufener Signaturverifikation das für diese Signatur verwendete Zertifikat für den öffentlichen Schlüssel von einer anderen Terminal-Zertifikationsstelle CA als der Terminal-Zertifikationsstelle CA der Endeinheit EE (die das Zertifikat für den öffentlichen Schlüssel an die eigene Endeinheit EE ausgegeben hat) ausgegeben wurde, sendet die Signaturprüfeinheit **15** eine Anforderung zum Überprüfen der Gültigkeit des Zertifikats für den öffentlichen Schlüssel für die Signaturprüfung zu dem Zertifikatprüfzentrum VC. Die Authentisierungsanforderung enthält, falls erforderlich, Angaben zur Vertrauenswürdigkeit (Verfahrensweise) über das Niveau der Zertifikation und/oder eine Absicherung für die Zertifikationsstelle. Nur wenn die Gültigkeit des betreffenden Zertifikats vom Zertifikatprüfzentrum VC bestätigt wird, wird das signierte elektronische Dokument als legal behandelt und gegebenenfalls von der Ein/Ausgabeeinheit **17** ausgegeben. Die Vertrauenswürdigkeit wird durch den Geschäftsumfang oder dergleichen des elektronischen Vorgangs angezeigt, der von dem signierten elektronischen Dokument ausgeführt wird. Die Vertrauenswürdigkeit kann auch zum Beispiel durch die Vertraulichkeit eines Dokuments oder durch die Vertrauenswürdigkeit der signierenden Person oder des signierten elektronischen Dokuments (soweit die Meldung der signierenden Person selbst erforderlich ist oder die Verarbeitung über ein Netzwerk akzeptabel ist) angezeigt werden.

[0044] Es wird nun die Zertifikationsstelle CA erläutert.

[0045] Die Fig. 4 ist eine Blockdarstellung des schematischen Aufbaus der Zertifikationsstelle CA.

[0046] Wie gezeigt umfaßt die Zertifikationsstelle CA eine Verarbeitungseinheit **20a**, eine Speichereinheit **20b**, eine Kommunikationseinheit **26**, die zur Kommunikation mit einer anderen Einrichtung über das Netzwerk NET dient, und eine Ein/Ausgabeeinheit **27**, die Zertifikate für öffentliche Schlüssel etc. eingibt und ausgibt und die Anweisungen von den Nutzern entgegennimmt.

[0047] Die Verarbeitungseinheit **20a** umfaßt eine Ausstellungseinheit **21**, die Zertifikate für öffentliche Schlüssel ausstellt, eine Verwaltungseinheit **22**, die die von Ausstellungseinheit **21** ausgegebenen Zertifikate für öffentliche Schlüssel verwaltet, und eine Steuereinheit **28**, die die verschiedenen Einheiten der Zertifikationsstelle CA steuert.

[0048] Die Speichereinheit **20b** umfaßt eine Datenbank **23** für Zertifikate für öffentliche Schlüssel, die die von der Ausstellungseinheit **21** ausgegebenen Zertifikate für öffentliche Schlüssel festhält, eine Halteeinheit **24** für die Ausstellungszielort-Verwaltungsliste, die die Ausstellungszielort-Verwaltungsliste festhält, die die Ausstellungs-Zielorte für die in der Datenbank **23** enthaltenen Zertifikate für öffentliche Schlüssel beschreibt, und eine Halteeinheit **25** für eine Zertifikations-Widerrufsliste.

[0049] Wenn bei diesem Aufbau die Steuereinheit **28** eine Anforderung für die Ausstellung eines Zertifikats für einen öffentlichen Schlüssel über die Ein/Ausgabeeinheit **27** oder die Kommunikationseinheit **26** erhält, zeigt sie die Annahme der Anforderung der Ausstellungseinheit **21** an. Die Ausstellungseinheit **21** erzeugt dann einen geheimen Schlüssel (Signaturschlüssel), den die Anforderungsstelle für die Ausstellung zur Erzeugung einer Signatur verwendet, und das Zertifikat für den öffentlichen Schlüssel,

der zu dem geheimen Schlüssel gehört. Bei dieser Gelegenheit signiert die Ausstellungseinheit **21** das Zertifikat über den öffentlichen Schlüssel unter Verwendung des geheimen Schlüssels ihrer Zertifikationsstelle CA. Falls erforderlich, gibt die Ausstellungseinheit **21** in dem Zertifikat für den öffentlichen Schlüssel die Gültigkeitsdauer für dieses Zertifikat, die Namen von Zertifikationsstellen, denen nicht zu vertrauen ist (Namenseinschränkungen), die maximale Pfadlänge für die Feststellung der Gültigkeit des betreffenden Zertifikats (die maximal erlaubte Zahl von Zertifikationsstellen auf einem Pfad) und die Vertrauenswürdigkeit einer Signatur auf der Basis der Verbindung des geheimen Schlüssels mit dem betreffenden Zertifikat für den öffentlichen Schlüssel an, die durch den Geschäftsumfang und dergleichen des elektronischen Vorgangs ausgedrückt wird. Danach werden das erzeugte Zertifikat für den öffentlichen Schlüssel und der geheime Schlüssel per Post oder mittels Kommunikation über die Ein/Ausgabeeinheit **27** oder die Kommunikationseinheit **26** an die Anforderungsstelle für die Ausstellung abgegeben. Das betreffende Zertifikat für den öffentlichen Schlüssel wird in der Datenbank **23** für Zertifikate über öffentliche Schlüssel gespeichert, und die Informationen über den Zielort der Ausstellung (d.h. die Anforderungsstelle für die Ausstellung) wird in die Anforderungs-Zielort-Verwaltungsliste in der Halteeinheit **24** für diese Liste eingeschrieben.

[0050] Wenn die Steuereinheit **28** eine Anforderung für das Zurückziehen eines Zertifikats für einen öffentlichen Schlüssel über die Ein/Ausgabeeinheit **27** oder die Kommunikationseinheit **26** erhalten hat, teilt sie diese Annahme der Anforderung der Verwaltungseinheit **22** mit. Die Verwaltungseinheit **22** löscht dann das zurückzuziehende Zertifikat für einen öffentlichen Schlüssel aus der Datenbank **23** für solche Zertifikate und löscht gleichzeitig die Informationen über den Ausstellungs-Zielort für dieses Zertifikat aus der Ausstellungs-Zielort-Verwaltungsliste in der Halteeinheit **24** für diese Liste. Es ist jedoch nicht wichtig, daß das zurückzuziehende Zertifikat für einen öffentlichen Schlüssel aus der Datenbank **23** für solche Zertifikate gelöscht wird. Die Verwaltungseinheit **22** erzeugt periodisch eine Zertifikat-Widerrufliste (abgekürzt "CRL" oder auch "ARL"), in der die Informationen über die zurückgezogenen Zertifikate über öffentliche Schlüssel enthalten sind, die in der CRL-Halteeinheit **25** gespeichert werden. Die Verwaltungseinheit **22** gibt vorzugsweise das Datum und die Stunde der Erzeugung einer neuen CRL in der gegenwärtigen CRL an.

[0051] Wenn die Steuereinheit **28** eine Anfrage bezüglich der Informationen über den Widerruf eines Zertifikats für einen öffentlichen Schlüssel durch die Kommunikationseinheit **26** von einer anderen Einrichtung erhält, durchsucht sie die Zertifikat-Widerrufsliste in der CRL-Halteeinheit **25**, um festzustellen, ob das betreffende Zertifikat für einen öffentlichen Schlüssel zurückgezogen wurde. Die Steuereinheit **28** gibt das Ergebnis der Prüfung als Antwort an die anfragende Einrichtung über die Kommunikationseinheit **26** zurück (das für eine solche Anfrage und die Antwort verwendete Kommunikationsprotokoll ist OCSP, die Abkürzung für "Online Certification Status Protocol").

[0052] Die Verwaltungseinheit **22** führt auch den Prozeß zum Überprüfen der Gültigkeitsdauer für die einzelnen Zertifikate für öffentliche Schlüssel in der Datenbank **23** für solche Zertifikate aus, um diejenigen Zertifikate für öffentliche Schlüssel aus der Datenbank **23** zu löschen, deren Gültigkeitsdauer abgelaufen ist, und um die Informationen für den Ausstellungs-Zielort der betreffenden Zertifikate für öffentliche Schlüssel aus der Ausstellungs-Zielort-Verwaltungsliste in der Halteeinheit **24** für diese Liste zu löschen.

[0053] Es wird nun das Zertifikatprüfzentrum VC erläutert.

[0054] Die **Fig. 5** ist eine Blockdarstellung des schematischen Aufbaus des Zertifikatprüfzentrums VC.

[0055] Wie gezeigt umfaßt das Zertifikationsprüfzentrum VC eine Verarbeitungseinheit **30a**, eine Speichereinheit **30b**, eine Kommunikationseinheit **36**, die zur Kommunikation mit einer anderen Einrichtung über das Netzwerk NET dient, und eine Ein/Ausgabeeinheit **37**, die Zertifikate für öffentliche Schlüssel etc. annimmt und ausgibt und die Anweisungen von den Nutzern entgegennimmt.

[0056] Die Verarbeitungseinheit **30a** umfaßt eine Pfadsucheinheit **32**, eine Pfadprüfeinheit **33**, eine Gültigkeitsdauer/Widerrufstatus-Prüfeinheit **34**, eine Gültigkeitsprüfeinheit **35** und eine Steuereinheit **38**, die die verschiedenen Einheiten des Zertifikationsprüfzentrums VC steuert. Die Speichereinheit **30b** umfaßt eine Pfad-Datenbank **31** und eine Datenbank **39** für einen Zertifikat-Widerrufslisten-(CRL)-Erzeugungs-Zeitplan.

[0057] Die Pfadsucheinheit **31** sucht periodisch nach Pfaden, die sich von der Brücken-Zertifikationsstelle CA_{bridge} zu den einzelnen Terminal-Zertifikationsstellen CA erstrecken, die an die Endeinheiten EE Zertifikate für öffentliche Schlüssel ausgestellt haben.

[0058] Jedesmal, wenn von der Pfadsucheinheit **31** nach einem Pfad gesucht wurde, prüft die Pfadprüfeinheit **32** den von der Pfadsucheinheit **31** festgestellten Pfad. Die Pfadprüfeinheit **32** speichert dann den Pfad, dessen Prüfung positiv verlaufen ist, in der Pfad-Datenbank **31**. Der Pfad wird dabei zusammen mit dem Namen der Terminal-Zertifikationsstelle CA gespeichert, die der oberhalb angeordneten Brü-

cken-Zertifikationsstelle CA_{bridge} nachgeordnet ist und deren Zertifikate für öffentliche Schlüssel von den Zertifikationsstellen CA auf dem Pfad erhalten wurden und von diesen Zertifikationsstellen CA an die Zertifikationsstellen CA ausgestellt wurden, die ihnen direkt nachgeordnet sind (an die Endeinheiten EE, wenn die ursprünglich ausstellenden Zertifikationsstellen CA die Terminal-Zertifikationsstellen CA sind).

[0059] Die Gültigkeitsdauer/Widerrufsstatus-Prüfeinheit **34** prüft die Gültigkeitsdauer und den Widerrufsstatus der Zertifikate für öffentliche Schlüssel für die in der Pfad-Datenbank **31** gespeicherten Pfade. Diese Zertifikate für öffentliche Schlüssel sind die, die von den Zertifikationsstellen CA auf dem Pfad an die Zertifikationsstellen CA ausgegeben wurden, die sich direkt nach den ursprünglich ausgebenden Zertifikationsstellen CA auf dem Pfad befinden (die Endeinheiten EE, wenn die ursprünglich ausstellenden Zertifikationsstellen CA die Terminal-Zertifikationsstellen CA sind). Die Einheit **34** aktualisiert die Pfad-Datenbank **33** entsprechend dem Ergebnis der Prüfung.

[0060] Die Gültigkeitsdauer/Widerrufsstatus-Prüfeinheit **34** speichert auch den Zeitplan zur Erzeugung der nächsten CRL, der in den CRLs (Zertifikat-Widerrufslisten) enthalten ist, die von den CRL-Halteeinheiten **25** der jeweiligen Zertifikationsstellen CA erhalten wurden, in der CRL-Erzeugungs-Zeitplan-Datenbank **39** zusammen mit den betreffenden Zertifikationsstellen CA.

[0061] Bei einer Anforderung von einer Endeinheit EE prüft die Gültigkeitsprüfeinheit **35** die Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel, das von einer der Terminal-Zertifikationsstellen CA ausgestellt wurde, die nicht die Terminal-Zertifikationsstelle CA ist, die zu der betreffenden Endeinheit EE gehört.

[0062] Die Endeinheit EE, die Zertifikationsstelle CA und das Zertifikationsprüfzentrum VC der Fig. 3 bis Fig. 5 können zum Beispiel derart realisiert werden, daß eine CPU **61** die in einem Speicher **62** gespeicherten Programme in einem allgemeinen elektronischen Computer wie in der Fig. 6 gezeigt abarbeitet. Der elektronische Computer umfaßt die CPU **61**, den Speicher **62**, eine externe Speichereinrichtung **63** wie eine Festplatte, eine Leseeinrichtung **64**, die Informationen aus einem tragbaren Speichermedium **69** wie einer CD-ROM ausliest, eine Kommunikationseinrichtung **65**, die dazu dient, über das Netzwerk mit einer anderen Einrichtung in Verbindung zu treten, eine Eingabeeinrichtung **66** wie eine Tastatur oder eine Maus, eine Ausgabeeinrichtung **67** wie einen Monitor oder einen Drucker, und ein Interface **68** zum Austauschen von Daten unter den Elementen des Computers. Die Kommunikationseinheiten **16**, **26** und **36** werden so realisiert, daß die CPU **61** von der Kommunikationseinrichtung **65** Gebrauch macht; die Ein/Ausgabeeinheiten **17**, **27** und **37** so, daß die CPU **61** von der Eingabeeinrichtung **66**, der Ausgabeeinrichtung **67** und der Leseeinrichtung **64** Gebrauch macht; und die Speichereinheiten **10b**, **20b** und **30b** so, daß die CPU **61** vom Speicher **62** und der externen Speichereinrichtung **63** Gebrauch macht. Die Verarbeitungseinheiten **10a**, **20a** und **30a** werden als Prozesse auf der CPU **61** realisiert.

[0063] Die vorgegebenen Programme zum Realisierung der Endeinheiten EE, der Zertifikationsstellen CA und des Zertifikationsprüfzentrums VC auf dem elektronischen Computer können jeweils mittels der Leseeinrichtung **64** aus dem Speichermedium **69** ausgelesen werden oder von einem anderen Server mittels der Kommunikationseinheit **65** über das Netzwerk heruntergeladen werden, um nach der einmaligen Speicherung in der externen Speichereinrichtung **63** oder auch ohne Speicherung in der externen Speichereinrichtung **63** in den Speicher **62** geladen zu werden, woraufhin sie auf der CPU **61** laufen können.

[0064] Es wird nun die Arbeitsweise des Zertifikationsprüfzentrums VC mit dem obigen Aufbau beschrieben.

[0065] Die Operation des Zertifikationsprüfzentrums VC dieser Ausführungsform ist in die Operation zur Suche nach und das Prüfen und das Verwalten von Pfaden und die Operation des Überprüfens der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel unterteilt.

[0066] Es wird nun die Operation zur Suche nach und das Prüfen und das Verwalten von Pfaden beschrieben.

[0067] Die Fig. 7 und Fig. 8 sind Flußdiagramme zur Erläuterung der Operation zur Suche nach und das Prüfen und das Verwalten von Pfaden, die im Zertifikationsprüfzentrum VC dieser Ausführungsform ausgeführt wird.

[0068] Wie in der Fig. 7 gezeigt, fordert, wenn eine vorgegebene Zeitspanne (zum Beispiel ein Tag) verstrichen ist, die Steuereinheit **38** die Pfadsucheinheit **32** auf, nach Pfaden zu suchen (Schritt S1001). Die Pfadsucheinheit **32** sich dann nach Pfaden, die sich von der Brücken-Zertifikationsstelle CA_{bridge} zu den einzelnen Terminal-Zertifikationsstellen CA erstrecken (Schritt S1002).

[0069] Konkret greift die Pfadsucheinheit **32** auf die Halteeinheit **24** für die Ausstellungs-Zielort-Verwaltungsliste der Brücken-Zertifikationsstelle CA_{bridge} zu, um Informationen über die Ausstellungs-Zielorte der Zertifikate für öffentliche Schlüssel zu erhalten, die von der Brücken-Zertifikationsstelle CA_{bridge} ausgestellt wurden. Wenn die erhaltenen Ausstel-

lungs-Zielorte die Zertifikationsstellen CA sind, greift die Pfadsucheinheit **32** auf die Halteeinheit **24** für die Ausstellungs-Zielort-Verwaltungsliste der Zertifikationsstellen CA jedes der Ausstellungs-Zielorte zu, um die Ausstellungs-Zielorte für die Zertifikate für öffentliche Schlüssel zu untersuchen, die von den einzelnen Zertifikationsstellen CA ausgestellt wurden. Dieser Prozeß wird fortgesetzt, bis die Ausstellungs-Zielorte für die Zertifikate für öffentliche Schlüssel die Endeinheiten EE werden, um dadurch nach den Pfaden zu suchen, die sich von der Brücken-Zertifikationsstelle CA_{bridge} zu den einzelnen Terminal-Zertifikationsstellen CA erstrecken. Damit der Prozeß nicht aufgrund von Schleifen in den Pfaden unbegrenzt iteriert wird, wird, wenn die von der Halteeinheit **24** für die Ausstellungs-Zielort-Verwaltungsliste erhaltenen Ausstellungs-Zielorte einer bestimmten Zertifikationsstelle CA eine Zertifikationsstelle CA enthalten, die sich oberhalb des vorher ausgebildeten Teilpfades befindet, der Prozeß nicht ausgeführt, in dem die bestimmte Zertifikationsstelle CA der Ausstellungs-Zielort ist.

[0070] Der Pfadsuchprozeß im Schritt S1002 wird anhand des beispielhaften Falles näher beschrieben, daß die einzelnen Zertifikationsstellen CA die in der Fig. 2 gezeigten Beziehungen aufweisen.

[0071] Zuerst greift die Pfadsucheinheit **32** auf die Halteeinheit **24** für die Ausstellungs-Zielort-Verwaltungsliste der Brücken-Zertifikationsstelle CA_{bridge} zu, um Informationen über die Zertifikationsstellen CA_{11}, CA_{21} und CA_{31} zu erhalten, das heißt Informationen über die Ausstellungs-Zielorte der Zertifikate für öffentliche Schlüssel, die von der Brücken-Zertifikationsstelle CA_{bridge} ausgestellt wurden.

[0072] Daraufhin führt die Pfadsucheinheit **32** den folgenden Prozeß aus, in dem von jedem der Ausstellungs-Zielorte (den Zertifikationsstellen CA_{11}, CA_{21} und CA_{31}) Kenntnis genommen wird, die von der Brücken-Zertifikationsstelle CA_{bridge} erhalten wurden.

[0073] Wenn der dabei notierte Ausstellungs-Zielort die Zertifikationsstelle CA ist (im folgenden "notierte Zertifikationsstelle CA" genannt), bildet die Pfadsucheinheit **32** einen Teilpfad von der Brücken-Zertifikationsstelle CA_{bridge} bis zur notierten Zertifikationsstelle CA aus. Daraufhin greift die Pfadsucheinheit **32** auf die Halteeinheit **24** für die Ausstellungs-Zielort-Verwaltungsliste der notierten Zertifikationsstelle CA zu, um Informationen über die Ausstellungs-Zielorte der von dieser Zertifikationsstelle CA ausgestellten Zertifikate für öffentliche Schlüssel zu erhalten. Es wird dabei angenommen, daß der notierte Ausstellungs-Zielort die Zertifikationsstelle CA_{11} ist, so daß der Teilpfad von der Brücken-Zertifikationsstelle CA_{bridge} zur Zertifikationsstelle CA_{11} verläuft und als Informationen über die Ausstellungs-Zielorte der Zertifikationsstelle CA_{11} Informationen über die Zertifikationsstellen CA_{bridge}, CA_{12} und CA_{13} erhalten werden.

[0074] Die Pfadsucheinheit **32** prüft dann, ob sich unter den von der Zertifikationsstelle CA_{11} erhaltenen Ausstellungs-Zielorten (CA_{bridge}, CA_{11} und CA_{13}) eine Zertifikationsstelle CA (im folgenden "Schleifen-Zertifikationsstelle CA") auf dem Teilpfad befindet. Wenn es einen solchen Ausstellungs-Zielort (eine Zertifikationsstelle CA) gibt, wird sie von den zu behandelnden Subjekten ausgeschlossen. Entsprechend wird hier die Zertifikationsstelle CA_{bridge} von den zu behandelnden Subjekten ausgeschlossen. Dann prüft die Pfadsucheinheit **32**, ob sich unter von der Zertifikationsstelle CA_{11} erhaltenen Ausstellungs-Zielorten eine Endeinheit EE befindet. Wenn es eine solche Endeinheit EE gibt, wird die Zertifikationsstelle CA_{11} zu der Terminal-Zertifikationsstelle CA. Hier ist die Endeinheit EE jedoch nicht in den von der Zertifikationsstelle CA_{11} erhaltenen Ausstellungs-Zielorten enthalten. Die Pfadsucheinheit **32** notiert daher entweder die Ausstellungs-Zielorte außer der Schleifen-Zertifikationsstelle CA, die von der Zertifikationsstelle CA_{11} erhalten wurden (das heißt die Zertifikationsstellen CA_{12} und CA_{13}), um den Teilpfad bis zu der Terminal-Zertifikationsstelle CA zu erweitern, die sich zwischen der Brücken-Zertifikationsstelle CA_{bridge} und der Zertifikationsstelle CA_{11} befindet.

[0075] Wenn der notierte Ausstellungs-Zielort eine Zertifikationsstelle CA ist, bildet die Pfadsucheinheit **32** einen Teilpfad aus, der diese notierte Zertifikationsstelle CA in Abwärtsrichtung mit dem vorher erhaltenen Teilpfad verbindet. Die Pfadsucheinheit **32** greift dann auf die Halteeinheit **24** für die Ausstellungs-Zielort-Verwaltungsliste der notierten Zertifikationsstelle CA zu, um Informationen über die Ausstellungs-Zielorte der von der betreffenden notierten Zertifikationsstelle CA ausgestellten Zertifikate für öffentliche Schlüssel zu erhalten. Es wird hier angenommen, daß der notierte Ausstellungs-Zielort (die Zertifikationsstelle CA) die Zertifikationsstelle CA_{12} ist, so daß der Teilpfad nun von der Brücken-Zertifikationsstelle CA_{bridge} über die Zertifikationsstelle CA_{11} zur Zertifikationsstelle CA_{12} verläuft und als Informationen über die Ausstellungs-Zielorte der Zertifikationsstelle CA_{12} die Endeinheiten EE_1 und EE_2 erhalten werden.

[0076] Dann prüft die Pfadsucheinheit **32**, ob sich unter den von der Zertifikationsstelle CA_{12} erhaltenen Ausstellungs-Zielorten (EE_1 und EE_2) eine Schleifen-Zertifikationsstelle CA befindet. Wenn es einen solchen Ausstellungs-Zielort (eine Schleifen-Zertifikationsstelle CA) gibt, wird sie von den zu behandelnden Subjekten ausgeschlossen. Da es hier keine Schleifen-Zertifikationsstelle CA gibt, geht die Pfadsucheinheit **32** zum nächsten Prozeß weiter und prüft, ob sich unter von der Terminal-Zertifikationsstelle CA_{12} erhaltenen Ausstellungs-Zielorten eine Endeinheit EE befindet. Hier sind nun alle erhaltenen

Ausstellungs-Zielorte Endeinheiten EE, so daß die Zertifikationsstelle CA_{12} zur Terminal-Zertifikationsstelle CA wird. Die Pfadsucheinheit **32** legt somit den Teilpfad, auf dem sich die Zertifikationsstelle CA_{12} ganz unten befindet, als den Pfad fest, der sich von der Brücken-Zertifikationsstelle CA_{bridge} zur Terminal-Zertifikationsstellen CA_{12} erstreckt ($CA_{bridge} – CA_{11} – CA_{12}$).

[0077] Die Pfadsucheinheit **32** prüft dann, ob es unter den Informationen über die Ausstellungs-Zielorte, die von der Zertifikationsstelle CA_{12} ganz unten am festgestellten Pfad erhalten werden, einen Ausstellungs-Zielort (eine Zertifikationsstelle CA, die keine Schleifen-Zertifikationsstelle CA ist) gibt, der bis jetzt nicht notiert wurde. Wenn es einen solchen Ausstellungs-Zielort gibt, führt die Einheit **32** den obigen Prozeß mit diesem Ausstellungs-Zielort als notierter Zertifikationsstelle CA weiter. Wenn es keinen solchen Ausstellungs-Zielort gibt, prüft die Einheit **32**, ob es unter den Informationen über die von der direkt oberhalb befindlichen Zertifikationsstelle CA_{11} erhaltenen Informationen über Ausstellungs-Zielorte einen Ausstellungs-Zielort (eine Zertifikationsstelle CA, die keine Schleifen-Zertifikationsstelle CA ist) gibt, der bis jetzt nicht notiert wurde. Wenn es einen solchen Ausstellungs-Zielort gibt, führt die Einheit **32** den obigen Prozeß mit diesem Ausstellungs-Zielort als notierter Zertifikationsstelle CA weiter. Unter den Informationen für Ausstellungs-Zielorte, die von der Zertifikationsstelle CA_{11} erhalten wurden, ist die Zertifikationsstelle CA_{13} noch nicht notiert, so daß die Einheit **32** den obigen Prozeß mit der Zertifikationsstelle CA_{13} als notierter Zertifikationsstelle CA ausführt und damit den Pfad festlegt, der sich von Brücken-Zertifikationsstelle CA_{bridge} zur Terminal-Zertifikationsstelle CA_{13} erstreckt ($CA_{bridge} – CA_{11} – CA_{13}$).

[0078] Auf diese Weise führt die Pfadsucheinheit **32** den obigen Prozeß für jede der Zertifikationsstellen CA auf dem erfaßten Pfad aus, bis jeder Ausstellungs-Zielort (jede Zertifikationsstelle CA außer den Schleifen-Zertifikationsstellen CA), der bis jetzt nicht notiert war, unter den Informationen für Ausstellungs-Zielorte, die von den betreffenden Zertifikationsstellen CA erhalten wurden, nicht existent werden. Die Einheit **32** legt so den Pfad fest, der sich von der Brücken-Zertifikationsstelle CA_{bridge} bis zur Terminal-Zertifikationsstelle CA erstreckt. Wenn die einzelnen Zertifikationsstelle CA die in der Fig. 2 gezeigten Beziehungen aufweisen, sind die Pfade von der Brücken-Zertifikationsstelle CA_{bridge} zur Terminal-Zertifikationsstelle CA, die von der Pfadsucheinheit **32** erfaßt werden, die in der Fig. 9 gezeigten Pfade.

[0079] Wenn die von der Brücken-Zertifikationsstelle CA_{bridge} zur Terminal-Zertifikationsstelle CA führenden Pfade von der Pfadsucheinheit **32** erfaßt wurden, fordert die Steuereinheit **38** des Zertifikationsprüfzentrums VC die Pfadprüfeinheit **33** auf, die Pfade zu überprüfen. Die Pfadprüfeinheit **33** prüft dann die von der Pfadsucheinheit **32** erfaßten Pfade (Schritt S1003).

[0080] Konkret führt die Pfadprüfeinheit **33** für jeden der von der Pfadsucheinheit **32** erfaßten Pfade den folgenden Prozeß aus.

[0081] Zuerst greift die Pfadprüfeinheit **33** auf die Datenbanken **23** für Zertifikate für öffentliche Schlüssel der einzelnen Zertifikationsstellen CA auf jedem Pfad zu, um die Zertifikate für öffentliche Schlüssel zu erhalten, die diese Zertifikationsstellen CA an die Zertifikationsstellen CA direkt unterhalb auf dem betreffenden Pfad ausgegeben haben (bzw. an die Endeinheiten EE, wenn die Zugriffs-Zielort-Zertifikationsstelle CA die Terminal-Zertifikationsstelle CA ist).

[0082] Daraufhin prüft die Pfadprüfeinheit **33** die Signatur des von der Terminal-Zertifikationsstelle CA am untersten Zweig des Pfades ausgegebenen Zertifikats für einen öffentlichen Schlüssel anhand des von der Zertifikationsstelle CA direkt oberhalb ausgegebenen Zertifikats für den öffentlichen Schlüssel. Wenn die Prüfung positiv verläuft, prüft die Einheit **33** die Signatur des von der betreffenden Zertifikationsstelle CA direkt oberhalb ausgegebenen Zertifikats für den öffentlichen Schlüssel anhand des von der direkt oberhalb davon ausgegebenen Zertifikats für den öffentlichen Schlüssel. Der Prozeß wird fortgeführt, bis die oben befindliche Zertifikationsstelle CA zu der Brücken-Zertifikationsstelle CA_{bridge} wird, wodurch der Pfad vorläufig geprüft ist.

[0083] Zum Beispiel wird bei der vorläufigen Prüfung des Pfades, der sich in der Fig. 2 von der Brücken-Zertifikationsstelle CA_{bridge} zu der Terminal-Zertifikationsstelle CA_{13} erstreckt ($CA_{bridge} – CA_{11} – CA_{13}$), zuerst die Signatur des von der Terminal-Zertifikationsstelle CA_{13} ausgegebenen Zertifikat für den öffentlichen Schlüssel anhand des Zertifikats geprüft, den die Quellen-Zertifikationsstelle CA_{11}, die die Zertifikationsstelle CA direkt oberhalb der Terminal-Zertifikationsstelle CA_{13} ist, an diese Terminal-Zertifikationsstelle CA_{13} ausgegeben hat. Daraufhin wird, wenn die Prüfung positiv verlaufen ist, die Signatur des von der Quellen-Zertifikationsstelle CA_{11} ausgegebenen Zertifikats für den öffentlichen Schlüssel anhand des Zertifikats geprüft, den die Brücken-Zertifikationsstelle CA_{bridge}, die die Zertifikationsstelle CA direkt oberhalb der Quellen-Zertifikationsstelle CA_{11} ist, an diese Quellen-Zertifikationsstelle CA_{11} ausgegeben hat. Wenn die Prüfung positiv verläuft, ist die vorläufige Prüfung des Pfades von der Brücken-Zertifikationsstelle CA_{bridge} zu der Terminal-Zertifikationsstelle CA_{13} positiv abgeschlossen.

[0084] Wenn die vorläufige Prüfung positiv verlaufen ist, prüft die Pfadprüfeinheit **33**, ob für die Zertifikate öffentlicher Schlüssel, die von den einzelnen

Zertifikationsstellen CA auf dem betreffenden Pfad erhalten wurden, eine Einschränkung vorliegt, wie der Name von anderen Zertifikationsstellen, denen nicht vertraut wird (Namenseinschränkung) oder die maximale Pfadlänge, die für die Authentisierung der Gültigkeit von Zertifikaten für öffentliche Schlüssel erlaubt ist (die maximal mögliche Anzahl von Zertifikationsstellen auf dem Pfad). Wenn eine solche Einschränkung vorliegt, prüft die Einheit **33**, ob diese bei dem betreffenden Pfad eingehalten wird, und entscheidet, daß die Überprüfung des betreffenden Pfades positiv verlaufen ist, wenn die Einschränkung eingehalten wurde.

[0085] Zum Beispiel ergibt, wenn die vorläufige Prüfung des Pfades von der Brücken-Zertifikationsstelle CA_{bridge} zu der Terminal-Zertifikationsstelle CA_{26} ($CA_{bridge} – CA_{31} – CA_{21} – CA_{22} – CA_{25} – CA_{26}$) in der Fig. 2 positiv verlaufen ist, die endgültige Prüfung des Pfades kein positives Ergebnis, wenn die Zertifikationsstelle CA_{31} der Name für eine Zertifikationsstelle ist, der in dem von der Zertifikationsstelle CA_{26} erhaltenen Zertifikat für einen öffentlichen Schlüssel nicht vertraut wird. Die Überprüfung des Pfades ergibt auch dann kein positives Ergebnis, wenn eine Anzahl von Zertifikationsstellen = 5 als Pfadlänge in dem von der Zertifikationsstelle CA_{26} erhaltenen Zertifikat für einen öffentlichen Schlüssel angegeben ist.

[0086] Wenn die von der Pfadsucheinheit **32** gefundenen Pfade wie oben angegeben von der Pfadprüfeinheit **33** geprüft wurden, löscht die Steuereinheit **38** zuerst den in der Pfad-Datenbank **31** gespeicherten Inhalt und speichert dann in der Pfad-Datenbank **31** in Verbindung mit den Terminal-Zertifikationsstellen CA ganz unten an den entsprechenden Pfaden und mit den von den Zertifikationsstellen CA auf diesem Pfad erhaltenen Zertifikaten für öffentliche Schlüssel in der Pfad-Datenbank **31** diejenigen Pfade ein, deren Überprüfung durch der Pfadprüfeinheit **33** positiv verlaufen ist (Schritt S1004).

[0087] Die Gültigkeitsdauer/Widerrufsstatus-Prüfeinheit **34** prüft, ob sich unter den in der Pfad-Datenbank **31** gespeicherten Zertifikaten für den öffentlichen Schlüssel ein Zertifikat befindet, dessen Gültigkeitsdauer abgelaufen ist (Schritt S1005). Bei Vorhandensein eines solchen Zertifikats wird auf die Datenbank **23** für Zertifikate für öffentliche Schlüssel der das betreffende Zertifikat für einen öffentlichen Schlüssel ursprünglich ausgebenden Zertifikationsstelle CA zugegriffen, um nach dem Zertifikat für den öffentlichen Schlüssel zu suchen, das neu an den Ausstellungs-Zielort des betreffenden Zertifikats für einen öffentlichen Schlüssel ausgegeben wurde (Schritt S1006).

[0088] Wenn sich in der Datenbank **23** für Zertifikate für öffentliche Schlüssel der ursprünglich ausgebenden Zertifikationsstelle CA kein solches neues Zertifikat befindet, werden die Informationen über den in Verbindung mit dem Zertifikat mit abgelaufener Gültigkeitsdauer gespeicherten Pfad aus der Pfad-Datenbank **31** gelöscht (Schritt S1007). Wenn ein neues Zertifikat für den öffentlichen Schlüssel in der Datenbank **23** für Zertifikate für öffentliche Schlüssel der ursprünglich ausgebenden Zertifikationsstelle CA vorhanden ist, wird dieses ausgelesen. Die Überprüfung des in der Pfad-Datenbank **31** in Verbindung mit dem Zertifikat für einen öffentlichen Schlüssel mit abgelaufener Gültigkeitsdauer gespeicherten Pfades erfolgt zum gleichen Zweck wie im Schritt S1003 unter Verwendung des Zertifikats für den öffentlichen Schlüssel, das neu erhalten wurde, anstelle des Zertifikats, dessen Gültigkeitsdauer abgelaufen ist (Schritt S1008).

[0089] Die Pfad-Überprüfung im Schritt S1008 kann ersetzt werden durch eine Maßnahme, bei der die Signatur des Zertifikat für den öffentlichen Schlüssel, das neu erhalten wurde, im Lichte des Zertifikats für den öffentlichen Schlüssel geprüft wird, das von der Zertifikationsstelle CA auf dem betreffenden Pfad direkt oberhalb der dieses Zertifikat für einen öffentlichen Schlüssel ursprünglich ausgebenden Zertifikationsstelle CA ausgegeben wurde, wobei die Überprüfung des betreffenden Pfades als positiv verlaufen angesehen wird, wenn die Überprüfung der Signatur positiv verlaufen ist.

[0090] Wie in der Fig. 8 gezeigt, wird, wenn die Überprüfung des Pfades positiv verlaufen ist ("Ja" im Schritt S1009), das in der Pfad-Datenbank **31** in Verbindung mit dem betreffenden Pfad gespeicherte Zertifikat für einen öffentlichen Schlüssel mit abgelaufener Gültigkeitsdauer durch das neu erhaltene Zertifikat für den öffentlichen Schlüssel ersetzt (Schritt S1010). Wenn die Überprüfung des Pfades nicht positiv verlaufen ist ("Nein" im Schritt S1009), wird der in Verbindung mit dem Zertifikat für den öffentlichen Schlüssel mit abgelaufener Gültigkeitsdauer in der Pfad-Datenbank **31** gespeicherte Pfad gelöscht (Schritt S1011).

[0091] Die Gültigkeitsdauer/Widerrufsstatus-Prüfeinheit **34** überprüft dann die Datenbank **39** für die Erzeugung eines Zeitplans für die Zertifikations-Widerrufsliste (CRL), um nach Zertifikationsstellen CA zu suchen, die mit einem CRL-Zeitplan in Verbindung stehen, der bereits abgelaufen ist (Schritt S1012). Bei Vorhandensein einer solchen Zertifikationsstelle CA ("Ja" im Schritt S1013) wird auf die CRL-Halteeinheit **25** der betreffenden Zertifikationsstelle CA zugegriffen, um die von dieser Zertifikationsstelle CA ausgegebene neueste CRL zu erhalten (Schritt S1014). Außerdem wird in der Datenbank **39** für den Zeitplan zur CRL-Erzeugung der in Verbindung mit der betreffenden Zertifikationsstelle CA gespeicherte CRL-Erzeugungszeitplan akualisiert, um dem zu entsprechen, der in der neuen CRL enthalten ist (Schritt S1015).

[0092] Dann prüft die Gültigkeitsdauer/Widerrufsstatus-Prüfeinheit **34**, ob das in der neuen CRL enthaltene Zertifikat für einen öffentlichen Schlüssel in der Pfad-Datenbank **31** gespeichert ist (Schritt S1016). Wenn das Zertifikat gespeichert ist, werden Informationen über einen Pfad, der mit diesem Zertifikat in Verbindung stehen, aus der Pfad-Datenbank **31** gelöscht (Schritt S1017).

[0093] Es wird nun die Operation des Überprüfens der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel erläutert.

[0094] Die Fig. 10 und Fig. 11 sind Flußdiagramme für die bei der vorliegenden Ausführungsform im Zertifikat-Prüfzentrum VC ausgeführten Operation des Überprüfens der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel.

[0095] Wenn die Steuereinheit **38** von der Kommunikationseinheit **36** eine Anforderung zur Überprüfung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel erhält, die den Namen einer Terminal-Zertifikationsstelle CA für eine bestimmte Endeinheit EE enthält und von einer Terminal-Zertifikationsstelle CA, die nicht diese Terminal-Zertifikationsstelle CA ist, für die Endeinheit EE ausgegeben wurde (Schritt S2001), teilt sie den Erhalt der Anforderung der Prüfeinheit **35** mit. Wenn der Name der Terminal-Zertifikationsstelle CA nicht in der Anforderung zur Überprüfung der Gültigkeit des Zertifikat für den öffentlichen Schlüssel enthalten ist, wird als Terminal-Zertifikationsstelle CA für die Endeinheit EE eine im Zertifikat-Prüfzentrum VC voreingestellte Standard-Zertifikationsstelle CA verwendet. Wenn die Terminal-Zertifikationsstelle CA, die das Zertifikat für einen öffentlichen Schlüssel ausgegeben hat, dessen Gültigkeit zu prüfen ist, nicht die obige Terminal-Zertifikationsstelle CA ist, wird dies der Prüfeinheit **35** auch mitgeteilt.

[0096] Die Prüfeinheit **35** prüft dann, ob in Verbindung mit der Terminal-Zertifikationsstelle CA, die das Zertifikat für einen öffentlichen Schlüssel ausgegeben hat, das in der Anforderung angegeben ist, und ob in Verbindung mit der Terminal-Zertifikationsstelle CA für die anfordernde Endeinheit EE jeweils in der Pfad-Datenbank **31** ein Pfad gespeichert ist (Schritt S2002).

[0097] Wenn sich herausstellt, daß weder in Verbindung mit der Terminal-Zertifikationsstelle CA, die das betreffende Zertifikat für einen öffentlichen Schlüssel ausgegeben hat, noch in Verbindung mit der Terminal-Zertifikationsstelle CA für die anfordernde Endeinheit EE ein Pfad in der Pfad-Datenbank **31** gespeichert ist, teilt die Prüfeinheit **35** der anfordernden Endeinheit EE über die Kommunikationseinheit **36** mit, daß das betreffende Zertifikat für einen öffentlichen Schlüssel nicht gültig ist (Schritt S2003).

[0098] Wenn jedoch sowohl in Verbindung mit der Terminal-Zertifikationsstelle CA, die das betreffende Zertifikat für einen öffentlichen Schlüssel ausgegeben hat, als auch in Verbindung mit der Terminal-Zertifikationsstelle CA für die anfordernde Endeinheit EE ein Pfad in der Pfad-Datenbank **31** gespeichert ist, prüft die Prüfeinheit **35**, ob in Verbindung mit einem der zwei Pfade in der Pfad-Datenbank **31** eine Einschränkung vorliegt, wie der Name von anderen Zertifikationsstellen, denen nicht vertraut wird (Namenseinschränkung) oder die maximale Pfadlänge, die für die Authentisierung der Gültigkeit von Zertifikaten für öffentliche Schlüssel erlaubt ist (die maximal mögliche Anzahl von Zertifikationsstellen auf dem Pfad) (Schritt S2004).

[0099] Wenn keine solche Einschränkung vorliegt, geht die Prüfeinheit **35** zum Schritt S2006 weiter. Wenn eine solche Einschränkung vorliegt, geht die Prüfeinheit **35** zum Schritt S2005 weiter und prüft, ob die Einschränkung bei den beiden Pfaden eingehalten wird, ob mit anderen Worten in den Zertifikaten für öffentliche Schlüssel beschrieben ist, daß einer Zertifikationsstelle CA auf den beiden Pfaden nicht zu vertrauen ist und ob die Anzahl von Zertifikationsstelle CA auf jedem der zwei Pfade kleiner ist als die maximale Pfadlänge.

[0100] Beim Vorhandensein einer solchen Beschreibung stellt die Prüfeinheit **35** fest, daß auf den beiden Pfaden die Einschränkung nicht eingehalten wird, und teilt der anfordernden Endeinheit EE über die Kommunikationseinheit **36** mit, daß das Zertifikat für den öffentlichen Schlüssel nicht gültig ist (Schritt S2003). Ohne eine solche Beschreibung stellt die Prüfeinheit **35** fest, daß bei den beiden Pfaden die Einschränkung eingehalten wird, und geht zum Schritt S2006 weiter.

[0101] Im Schritt S2006 prüft die Prüfeinheit **35**, ob in der von der betreffenden Endeinheit EE erhalten Authentifizierungsanforderung die Vertrauenswürdigkeit enthalten ist, die durch den Geschäftsumfang und dergleichen des elektronischen Vorgang an der Endeinheit EE und dergleichen angezeigt wird. Wenn die Vertrauenswürdigkeit für den elektronischen Vorgang enthalten ist, prüft die Einheit **35** weiter, ob die in der Pfad-Datenbank **31** in Verbindung mit einem der beiden Pfade gespeicherten Zertifikate für öffentliche Schlüssel eine Angabe über die Vertrauenswürdigkeit enthalten, die die angegebene Vertrauenswürdigkeit für den elektronischen Vorgang nicht erfüllt (Schritt S2007).

[0102] Beim Vorhandensein einer solchen Angabe stellt die Prüfeinheit **35** fest, daß die beiden Pfade nicht zur Authentisierung der Gültigkeit des Zertifikats für den öffentlichen Schlüssel für den elektronischen Vorgang an der anfordernden Endeinheit EE verwendet werden können, und teilt der anfordern-

den Endeinheit EE über die Kommunikationseinheit **36** mit, daß das Zertifikat für den öffentlichen Schlüssel nicht gültig ist (Schritt S2003).

[0103] Wenn in der von der betreffenden Endeinheit EE erhaltenen Authentisierungsanforderung die Vertrauenswürdigkeit für den elektronischen Vorgang an der Endeinheit EE nicht enthalten ist oder wenn eine Vertrauenswürdigkeit für den elektronischen Vorgang enthalten ist, die in den in der Pfad-Datenbank **31** in Verbindung mit einem der beiden Pfade gespeicherten Zertifikaten für die öffentlichen Schlüssel beschriebene Vertrauenswürdigkeit gleich oder größer ist als die für den elektronischen Vorgang, stellt die Prüfeinheit **35** fest, daß das Zertifikat für den öffentlichen Schlüssel gültig ist, und teilt dies der anfordernden Endeinheit EE über die Kommunikationseinheit **36** mit (Schritt S2008).

[0104] Es wurde oben eine Ausführungsform der vorliegenden Erfindung beschrieben.

[0105] Bei dieser Ausführungsform wird unabhängig von einer Anforderung einer Endeinheit EE zur Authentisierung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel periodisch nach Pfaden von der Brücken-Zertifikationsstelle CA_{bridge} zu der jeweiligen Terminal-Zertifikationsstelle CA gesucht und solche Pfade überprüft. Wenn von einer bestimmten Endeinheit EE eine Anforderung zur Authentisierung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel erhalten wird, wird durch Prüfen der vorliegenden Pfade festgestellt, ob es einen Pfad durch die Brücken-Zertifikationsstelle CA_{bridge} zwischen der Terminal-Zertifikationsstelle CA für die betreffende Endeinheit EE und der das den Gegenstand der Anforderung bildende Zertifikat für einen öffentlichen Schlüssel ausgebende Zertifikationsstelle CA gibt und das betreffende Zertifikat gültig ist. Es ist damit möglich, die Zeitspanne von der Entgegennahme der Anforderung zur Authentifizierung der Gültigkeit des Zertifikats für einen öffentlichen Schlüssel bis zur Authentifizierung der Gültigkeit zu verringern.

[0106] Wenn bei der vorliegenden Ausführungsform die Anforderung zur Authentifizierung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel von einer bestimmten Endeinheit EE erhalten wird, wird anhand der vorher bereits ausgesuchten und geprüften Pfade geprüft, ob über die Brücken-Zertifikationsstelle CA_{bridge} zwischen der Terminal-Zertifikationsstelle CA für die betreffende Endeinheit EE und die die Anforderung für das Zertifikat ausgebende Terminal-Zertifikationsstelle CA ein Pfad ausgebildet werden kann, und es wird schließlich festgestellt, ob es für den betreffenden, ausgebildeten Pfad Einschränkungen (wie Namen für andere Zertifikationsstellen, denen nicht vertraut wird, oder eine maximale Pfadlänge bzw. maximal erlaubte Anzahl von Zertifikationsstellen auf dem Pfad oder die in einem von einer Zertifikationsstelle auf dem Pfad angegebene Vertrauenswürdigkeit) gibt. Es ist damit möglich, die Gültigkeit des betreffenden Zertifikats für einen öffentlichen Schlüssel besser zu beurteilen.

[0107] Die vorliegende Erfindung ist nicht auf die vorliegende Ausführungsform beschränkt, sondern kann im Rahmen der anhängenden Patentansprüche verschiedene Modifikationen aufweisen.

[0108] Zum Beispiel legt bei der vorstehenden Ausführungsform das Zertifikat-Prüfzentrum VC die Brücken-Zertifikationsstelle CA_{bridge} als Start-Zertifikationsstelle fest und sucht dann nach Pfaden, die sich von der Brücken-Zertifikationsstelle CA_{bridge} zu den einzelnen Terminal-Zertifikationsstellen CA erstrecken. Die vorliegende Erfindung ist darauf jedoch nicht beschränkt. Es kann auch jede andere Zertifikationsstelle CA als Start-Zertifikationsstelle festgelegt werden und nach Pfaden gesucht werden, die sich davon zu den einzelnen Terminal-Zertifikationsstellen CA erstrecken. Zum Beispiel kann bei einer Beziehung der Zertifikationsstellen CA wie in der **Fig. 2** jede der Quellen-Zertifikationsstellen CA_{11}, CA_{21} und CA_{31} der jeweiligen Sicherheitsdomain SD als Start-Zertifikationsstelle festgelegt werden, von der aus Pfade gesucht werden, die sich zu den einzelnen Terminal-Zertifikationsstellen CA erstrecken.

[0109] Bei der vorstehenden Ausführungsform wird der Kürze halber angenommen, daß wie in der **Fig. 2** gezeigt die Terminal-Zertifikationsstellen CA die Zertifikate für die öffentlichen Schlüssel nur an die Endeinheiten EE ausgeben, während die anderen Zertifikationsstellen CA die Zertifikate für die öffentlichen Schlüssel nur an die Zertifikationsstellen CA ausgeben. Selbstverständlich kann die vorliegende Erfindung jedoch gleichermaßen auf den Fall angewendet werden, daß ein PKI-System eine Zertifikationsstelle CA enthält, die Zertifikate für öffentliche Schlüssel sowohl an Endeinheiten EE als auch an andere Zertifikationsstellen CA ausgibt.

[0110] Bei der vorliegenden Ausführungsform wurde angegeben, daß die Zertifikationsstelle CA nur unter den Quellen-Zertifikationsstellen der einzelnen Sicherheitsdomains eine Kreuz-Zertifikation ausführt. Dies ist nicht auf die Quellen-Zertifikationsstellen beschränkt, es können auch andere Zertifikationsstellen eine Kreur-Zertifikation ausführen.

[0111] Wie angegeben kann erfindungsgemäß die Zeitspanne zwischen einer Anforderung zur Authentifizierung der Gültigkeit eines Zertifikats für einen öffentlichen Schlüssel bis zur Bestätigung der Gültigkeit verkürzt werden.

Patentansprüche

1. Verfahren zur Authentifizierung der Gültigkeit

eines Zertifikats in einem hierarchischen Zertifizierungssystem, wobei die Gültigkeit eines Zertifikats eines öffentlichen Schlüssels, das von einer anderen Zertifizierungsautorität CA' als der von einem Terminal (EE) vertrauten Zertifizierungsautorität CA ausgegeben wurde, auf eine Anfrage des Terminals (EE) hin authentifiziert wird, umfassend die folgenden Schritte:
eine Pfadsuche (S1002), bei der ein Verfahren ausgeführt wird, in dem mit einer beliebigen Zertifizierungsautorität als Anfangszertifizierungsautorität alle Besitzer eines von der Anfangszertifizierungsautorität ausgegebenen Zertifikats eines öffentlichen Schlüssels identifiziert werden und, wenn ein Besitzer eine andere Zertifizierungsautorität ist, alle Besitzer eines von dieser zweiten Zertifizierungsautorität ausgegebenen Zertifikats eines öffentlichen Schlüssels weiter identifiziert werden, wobei das Verfahren fortgesetzt wird, bis alle Besitzer der Zertifikate öffentlicher Schlüssel Terminals werden, wodurch Pfade gefunden werden, die sich von der Anfangszertifizierungsautorität bis zu Zertifizierungsautoritäten erstrecken, die Terminals zulassen und Zertifikate öffentlicher Schlüssel an Terminals ausgegeben haben,
eine Pfadverifizierung (S1003), bei der für jeden bei der Pfadsuche gefundenen Pfad ein Verfahren ausgeführt wird, in dem die Anfangszertifizierungsautorität ganz oben angeordnet ist und eine Signatur des Zertifikats eines öffentlichen Schlüssels, das von einer Terminals zulassenden Zertifizierungsautorität auf dem zugehörigen Pfad ausgegeben wurde, verifiziert wird im Hinblick auf das Zertifikat des öffentlichen Schlüssels, das von der direkt darüber angeordneten Zertifizierungsautorität ausgegeben wurde, und bei positiv ausgegangener Verifizierung eine Signatur des Zertifikats des öffentlichen Schlüssels, das von der direkt darüber liegenden Zertifizierungsautorität ausgegeben wurde, verifiziert wird im Hinblick auf das Zertifikat des öffentlichen Schlüssels, das von der wiederum darüber liegenden Zertifizierungsautorität ausgegeben wurde, wobei das Verfahren fortgesetzt wird, bis die direkt darüber liegende Zertifizierungsautorität die Anfangszertifizierungsautorität wird, wodurch die Pfade verifiziert werden,
gekennzeichnet durch die folgenden Schritte:
eine Pfadregistrierung (S1004), bei der solche Pfade, für die die Pfadverifizierung (S1003) positiv ausgegangen ist, in einer Datenbank registriert werden, und
eine Gültigkeitsauthentifizierung (S2002) auf eine Anfrage (S2001) des Terminals hin nach Authentifizierung der Gültigkeit eines Zertifikats eines öffentlichen Schlüssels, das von einer anderen Terminals zulassenden Zertifizierungsautorität CA' als der vom Terminal (EE) vertrauten Zertifizierungsautorität CA ausgegeben wurde, wobei die Gültigkeit des Zertifikats des öffentlichen Schlüssels als authentifiziert eingestuft wird, wenn der Pfad zwischen der vom Terminal (EE) vertrauten Zertifizierungsautorität CA und der Anfangs Zertifizierungsautorität sowie der Pfad zwischen der anderen Terminals zulassenden Zertifizierungsautorität CA' und der Anfangszertifizierungsautorität in der Datenbank registriert sind.

2. Verfahren zur Authentifizierung der Gültigkeit eines Zertifikats nach Anspruch 1, wobei
die Pfadsuche (S1002) periodisch ausgeführt wird,
die Pfadverifizierung (S1003) für den neuesten in der Pfadsuche (S1002) gefundenen Pfad ausgeführt wird, und
die Pfadregistrierung (S1004) die registrierten Inhalte der Datenbank bezüglich des neuesten Pfads, dessen Pfadverifizierung (S1003) gut ausgegangen ist, aufdatiert.

3. Verfahren zur Authentifizierung der Gültigkeit eines Zertifikats nach Anspruch 1, ferner umfassend die folgenden Schritte:
eine Untersuchung der Gültigkeitszeit (31005), bei der für jeden der in der Datenbank durch die Pfadregistrierung (S1004) registrierten Pfade Gültigkeitszeiten der Zertifikate öffentlicher Schlüssel, die die Zertifizierungsautoritäten auf dem dazugehörigen Pfad ihren jeweils direkt darunterliegenden Zertifizierungsautoritäten (den von den Terminals zulassenden Zertifizierungsautoritäten zugelassenen Terminals, falls die Ausgabeorte die Terminals zulassenden Zertifizierungsautoritäten sind) ausgegeben haben, und
eine erneute Pfadverifizierung, bei der jedes neue Zertifikat eines öffentlichen Schlüssels für einen Besitzer eines Zertifikats eines öffentlichen Schlüssels, dessen Gültigkeitszeit bei der Untersuchung der Gültigkeitszeit (S1005) als abgelaufen authentifiziert wurde, vom Ausgabeort des zeitlich abgelaufenen Zertifikats des öffentlichen Schlüssels erhalten wird (S1006) und zumindest eine Signatur des neuen Zertifikats des öffentlichen Schlüssels im Hinblick auf das Zertifikat des öffentlichen Schlüssels, das von der direkt über dem Ausgabeort liegenden Zertifizierungsautorität ausgegeben wurde, verifiziert wird (S1008),
wobei die Pfadregistrierung den Pfad, der den Ausgabeort und den Besitzer des Zertifikats des öffentlichen Schlüssels, dessen Gültigkeitszeit bei der Untersuchung der Gültigkeitszeit als abgelaufen authentifiziert wurde, enthält, aus der Datenbank löscht (S1007), wenn die Verifizierung der Signatur des neuen Zertifikats des Öffentlichen Schlüssels in der erneuten Pfadverifizierung nicht positiv ausgegangen ist oder der Erhalt eines neuen Zertifikats des öffentlichen Schlüssels gescheitert ist.

4. Verfahren zur Authentifizierung der Gültigkeit eines Zertifikats nach Anspruch 1, ferner umfassend die folgenden Schritte:
eine Untersuchung von Widerrufsinformation (S1012, S1013), bei der für jeden der bei der Pfadregistrierung in der Datenbank registrierten Pfade Widerrufsinformationen zu den Zertifikaten öffentlicher

Schlüssel, die die Zertifizierungsautoritäten auf dem dazugehörigen Pfad ausgegeben haben, untersucht wird;
wobei die Pfadregistrierung den Pfad, der den Ausgabeort und den Besitzer jeglicher Zertifikate öffentlicher Schlüssel, die bei der Untersuchung der Widerrufsinformation (S1012, S1013) als widerrufen authentifiziert wurden, aus der Datenbank löscht (S1016, S1017).

5. Verfahren zur Authentifizierung der Gültigkeit eines Zertifikats nach Anspruch 1, wobei
die Gültigkeitsauthentifizierung (S2002) die Anfrage des Terminals (EE) nach Authentifizierung der Gültigkeit des Zertifikats des öffentlichen Schlüssels, das von der anderen Terminals zulassenden Zertifizierungsautorität CA' als der vom Terminal (EE) vertrauten Zertifizierungsautorität CA ausgegeben wurde, beantwortet (S2001), indem die Authentifizierung der Gültigkeit des Zertifikats des öffentlichen Schlüssels als fehlgeschlagen eingestuft wird (S2005), falls eine Beschränkung, durch die keiner Zertifizierungsautorität auf den Pfaden zwischen der vom Terminal (EE) vertrauten Zertifizierungsautorität CA und der Anfangszertifizierungsautorität sowie zwischen der anderen Terminals zulassenden Zertifizierungsautorität CA' und der Anfangszertifizierungsautorität vertraut wird, in einem Zertifikat eines öffentlichen Schlüssels eingeschrieben ist (S2004), das irgendeine Zertifizierungsautorität auf den beiden Pfaden gegenüber der direkt darunterliegenden Zertifizierungsautorität (dem von der Terminals zulassenden Zertifizierungsautorität zugelassenen Terminal, falls der Ausgabeort eine Terminals zulassende Zertifizierungsautorität ist) auf dem Pfad, auf dem die Ausgabeortzertifizierungsautorität liegt, ausgegeben hat, auch wenn die beiden Pfade in der Datenbank registriert sind.

6. Verfahren zur Authentifizierung der Gültigkeit eines Zertifikats nach Anspruch 1, wobei
die Gültigkeitsauthentifizierung (S2002) die Anfrage (S2001) des Terminals (EE) nach Authentifizierung der Gültigkeit des von der anderen Terminals zulassenden Zertifizierungsautorität CA' als der vom Terminal (EE) vertrauten Zertifizierungsautorität CA ausgegebenen Zertifikats eines öffentlichen Schlüssels beantwortet, indem die Authentifizierung der Gültigkeit des Zertifikats des öffentlichen Schlüssels als fehlgeschlagen eingestuft wird (S2005), falls die Gesamtanzahl der Zertifizierungsautoritäten, die auf den Pfaden zwischen der vom Terminal (EE) vertrauten Zertifizierungsautorität CA und der Anfangszertifizierungsautorität sowie zwischen der anderen Terminals zulassenden Zertifizierungsautorität CA' und der Anfangszertifizierungsautorität liegen, eine Pfadlänge (die höchstens erlaubte Anzahl von auf den beiden Pfaden liegenden Zertifizierungsautoritäten) überschreitet, die in dem Zertifikat eines öffentlichen Schlüssels, das eine Zertifizierungsautorität auf den beiden Pfaden der direkt darunterliegenden Zertifizierungsautorität (dem von der Terminals zulassenden Zertifizierungsautorität zugelassenen Terminal, falls der Ausgabeort eine Terminals zulassende Zertifizierungsautorität ist) auf dem Pfad, auf dem die Ausgabeortzertifizierungsautorität liegt, ausgegeben hat, einschrieben ist, auch wenn die beiden Pfade in der Datenbank registriert sind.

7. Verfahren zur Authentifizierung der Gültigkeit eines Zertifikats nach Anspruch 1, wobei
die Gültigkeitsauthentifizierung (S2002) eine Anfrage des Terminals (EE) nach Authentifizierung der Gültigkeit des Zertifikats des öffentlichen Schlüssels, das von einer anderen Terminals zulassenden Zertifizierungsautorität CA' als der vom Terminal (EE) vertrauten Zertifizierungsautorität CA ausgegeben wurde, beantwortet, wobei die Anfrage begleitet wird von einer Darstellung der Vertrauenswürdigkeit, die von einer vom Terminal (EE) beabsichtigten elektronischen Prozedur verlangt wird, indem die Authentifizierung der Gültigkeit des Zertifikats des öffentlichen Schlüssels als fehlgeschlagen eingestuft wird (S2007), falls die Vertrauenswürdigkeit (Vorgehensweise), die in dem Zertifikat des öffentlichen Schlüssels eingeschrieben ist (S2006), das irgendeine Zertifizierungsautorität, die auf den Pfaden zwischen der vom Terminal (EE) vertrauten Zertifizierungsautorität CA und der Anfangszertifizierungsautorität sowie zwischen der anderen Terminals zulassenden Zertifizierungsautorität und der Anfangszertifizierungsautorität liegt, gegenüber der direkt darunterliegenden Zertifizierungsautorität (dem von der Terminals zulassenden Zertifizierungsautorität zugelassenen Terminal, falls der Ausgabeort eine Terminals zulassende Zertifizierungsautorität ist) auf dem Pfad, auf dem die Ausgabeortzertifizierungsautorität liegt, zugelassen hat, geringer ist als die von der elektronischen Prozedur verlangte Vertrauenswürdigkeit, auch wenn die beiden Pfade in der Datenbank registriert sind.

8. Verfahren zur Authentifizierung der Gültigkeit eines Zertifikats nach Anspruch 1, wobei die Anfangszertifizierungsautorität eine Brückenzertifizierungsautorität (CA_{bridge}) ist, die Kreuzzertifizierung mit den jeweiligen Rootzertifizierungsautoritäten von mindestens zwei Sicherheitsdomainen (SD) durchführt.

9. Vorrichtung zur Authentifizierung der Gültigkeit eines Zertifikats, wobei die Gültigkeit eines Zertifikats eines öffentlichen Schlüssels, das von einer anderen Zertifizierungsautorität CA' als der von einem Terminal (EE) vertrauten Zertifizierungsautorität CA ausgegeben wurde, auf eine vom Terminal (EE) getätigte Anfrage hin authentifiziert wird, umfassend
eine Pfadsuche-Einrichtung (**32**) zum Ausführen eines Verfahrens (S1002), bei dem mit irgendeiner Zertifizierungsautorität als Anfangszertifizierungsautorität alle Besitzer eines Zertifikats eines öffentlichen Schlüssels, das von der Anfangszertifizierungsautori-

tät ausgegeben wurde, identifiziert werden und, wenn ein Besitzer eine andere Zertifizierungsautorität ist, alle Besitzer eines Zertifikats eines öffentlichen Schlüssels, das von dieser zweiten Zertifizierungsautorität ausgegeben wurde, weiter identifiziert werden, wobei das Verfahren fortgesetzt wird, bis alle Besitzer der Zertifikate öffentlicher Schlüssel Terminals werden, wodurch Pfade gefunden werden, die sich von der Anfangszertifizierungsautorität bis zu den Terminals zulassenden Zertifizierungsautoritäten, die Zertifikate öffentlicher Schlüssel an Terminals ausgegeben haben, erstrecken,
eine Pfadverifizierungseinrichtung (**33**) zum Ausführen eines Verfahrens (S1003) für jeden der von der Pfadsuche-Einrichtung detektierten Pfade, bei dem mit der ganz oben angeordneten Anfangszertifizierungsautorität eine Signatur des Zertifikats des Öffentlichen Schlüssels, das von der Terminals zulassenden Zertifizierungsautorität auf dem dazugehörigen Pfad ausgegeben wurde, verifiziert wird im Hinblick auf das Zertifikat des öffentlichen Schlüssels, das von der direkt darunterliegenden Zertifizierungsautorität ausgegeben wurde, und bei positiv ausgegangener Verifizierung eine Signatur des von der direkt darüber liegenden Zertifizierungsautorität ausgegebenen Zertifikats des öffentlichen Schlüssels verifiziert wird im Hinblick auf das von der wiederum direkt darüber liegenden Zertifizierungsautorität ausgegebene Zertifikat des öffentlichen Schlüssels, wobei das Verfahren fortgesetzt wird, bis die direkt darüber liegende Zertifizierungsautorität die Anfangszertifizierungsautorität ist, wodurch beide Pfade verifiziert werden,
ferner gekennzeichnet durch
eine Pfadregistrierungseinrichtung (**30b**) zum Registrieren (S1004) solcher Pfade, deren Verifizierung durch die Pfadverifizierungseinrichtung (**33**) positiv ausgegangen sind, in einer Datenbank (**31**), und
eine Gültigkeitsauthentifizierungseinrichtung (**35**), die die Anfrage des Terminals (EE) nach Authentifizierung der Gültigkeit eines Zertifikats eines öffentlichen Schlüssels, das von einer anderen Terminals zulassenden Zertifizierungsautorität CA' als der vom Terminal (EE) vertrauten Zertifizierungsautorität CA ausgegeben wurde, beantwortet (S2001), indem die Gültigkeit des Zertifikats des öffentlichen Schlüssels als authentifiziert eingestuft wird (S2002), wenn die Pfade zwischen der vom Terminal (EE) vertrauten Zertifizierungsautorität CA und der Anfangszertifizierungsautorität sowie zwischen der anderen Terminals zulassenden Zertifizierungsautorität CA' und der Anfangszertifizierungsautorität in der Datenbank (**31**) registriert sind.

10. Speichermedium, auf dem ein Programm gespeichert ist zur Authentifizierung der Gültigkeit eines Zertifikats eines öffentlichen Schlüssels, das von einer anderen Zertifizierungsautorität CA' als der von einem Terminal (EE) vertrauten Zertifizierungsautorität CA ausgegeben wurde, auf eine vom Terminal (EE) getätigte Anzeige hin,
wobei das Programm von einem elektronischen Computer gelesen und ausgeführt wird, wodurch auf dem elektronischen Computer gebildet werden:
eine Pfadsuche-Einrichtung (**32**) zum Ausführen eines Verfahrens (S1002), bei dem mit irgendeiner Zertifizierungsautorität als Anfangszertifizierungsautorität alle Besitzer eines Zertifikats eines öffentlichen Schlüssels, das von der Anfangs Zertifizierungsautorität ausgegeben wurde, identifiziert werden und, wenn ein Besitzer eine andere Zertifizierungsautorität ist, alle Besitzer eines Zertifikats eines öffentlichen Schlüssels, das von dieser zweiten Zertifizierungsautorität ausgegeben wurde, weiter identifiziert werden, wobei das Verfahren fortgesetzt wird, bis alle Besitzer der Zertifikate öffentlicher Schlüssel Terminals werden, wodurch Pfade gefunden werden, die sich von der Anfangszertifizierungsautorität bis zu den Terminals zulassenden Zertifizierungsautoritäten, die Zertifikate öffentlicher Schlüssel an Terminals ausgegeben haben, erstrecken,
eine Pfadverifizierungseinrichtung (**33**) zum Ausführen eines Verfahrens (S1003) für jeden der von der Pfadsuche-Einrichtung detektierten Pfade, bei dem mit der ganz oben angeordneten Anfangszertifizierungsautorität eine Signatur des Zertifikats des öffentlichen Schlüssels, das von der Terminals zulassenden Zertifizierungsautorität auf dem dazugehörigen Pfad ausgegeben wurde, verifiziert wird im Hinblick auf das Zertifikat des öffentlichen Schlüssels, das von der direkt darunterliegenden Zertifizierungsautorität ausgegeben wurde, und bei positiv ausgegangener Verifizierung eine Signatur des von der direkt darüber liegenden Zertifizierungsautorität ausgegebenen Zertifikats des öffentlichen Schlüssels verifiziert wird im Hinblick auf das von der wiederum direkt darüber liegenden Zertifizierungsautorität ausgegebene Zertifikat des öffentlichen Schlüssels, wobei das Verfahren fortgesetzt wird, bis die direkt darüber liegende Zertifizierungsautorität die Anfangszertifizierungsautorität ist, wodurch beide Pfade verifiziert werden,
eine Pfadregistrierungseinrichtung (**30b**) zum Registrieren (S1004) solcher Pfade, deren Verifizierung durch die Pfadverifizierungseinrichtung (**33**) positiv ausgegangen sind, in einer Datenbank (**31**), und
eine Gültigkeitsauthentifizierungseinrichtung (**35**), die die Anfrage des Terminals (EE) nach Authentifizierung der Gültigkeit eines Zertifikats eines öffentlichen Schlüssels, das von einer anderen Terminals zulassenden Zertifizierungsautorität CA' als der vom Terminal (EE) vertrauten Zertifizierungsautorität CA ausgegeben wurde, beantwortet (S2001), indem die Gültigkeit des Zertifikats des öffentlichen Schlüssels als authentifiziert eingestuft wird (S2002), wenn die Pfade zwischen der vom Terminal (EE) vertrauten Zertifizierungsautorität CA und der Anfangszertifizierungsautorität sowie zwischen der anderen Terminals zulassenden Zertifizierungsautorität CA' und der Anfangszertifizierungsautorität in der Datenbank (**31**)

registriert sind.

Es folgen 12 Blatt Zeichnungen

Anhängende Zeichnungen

FIG.1

PKI SYSTEM

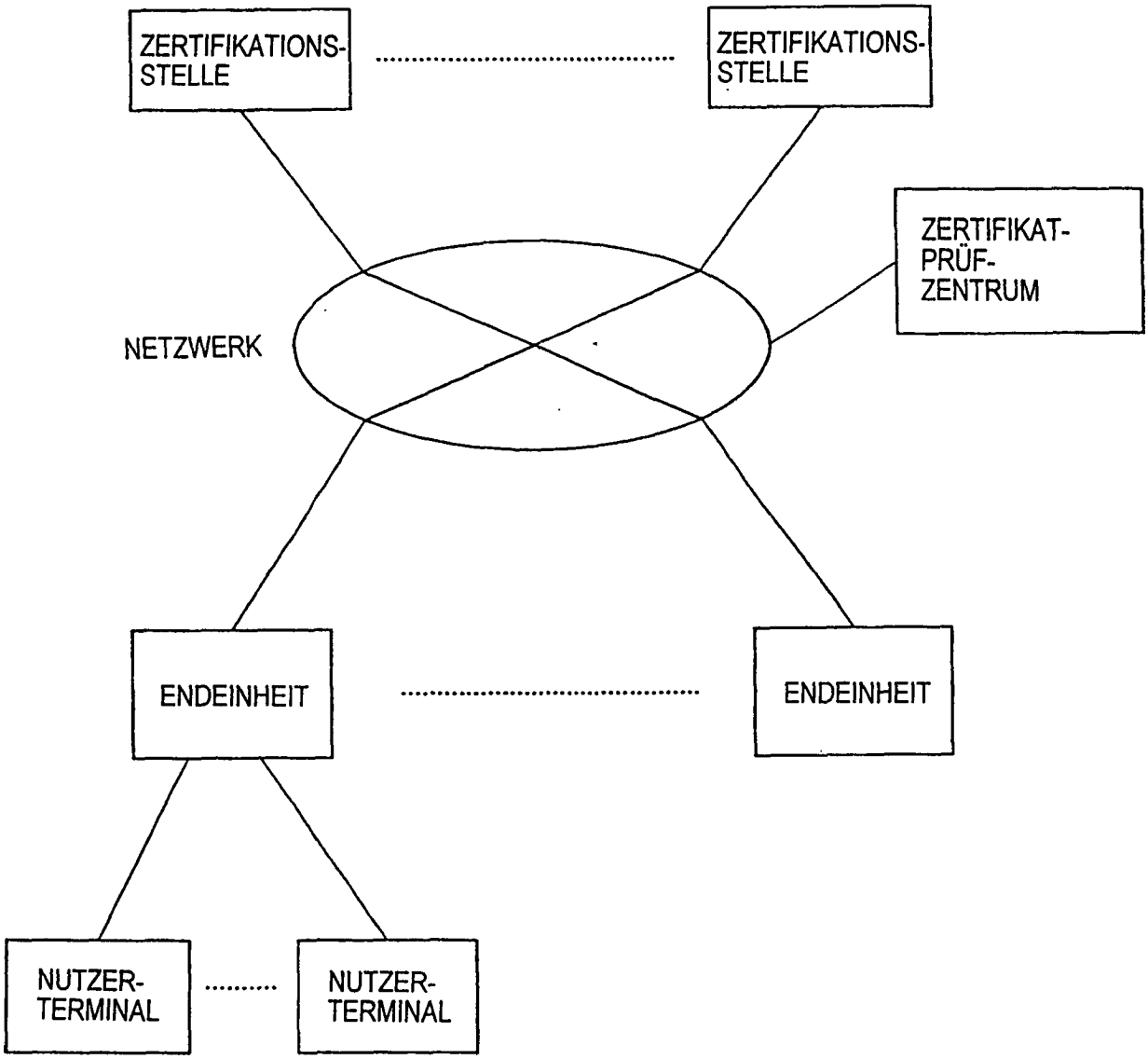
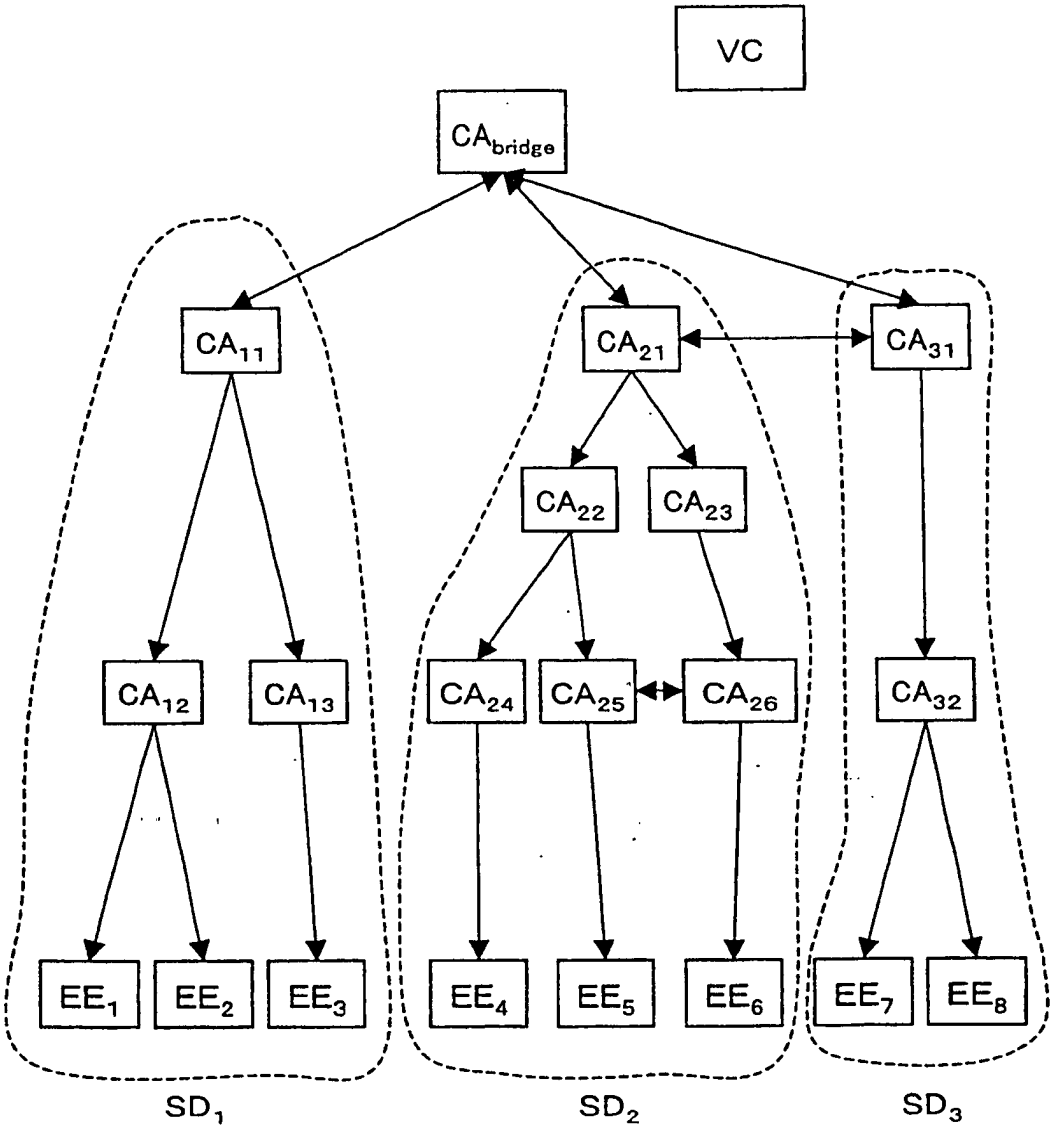


FIG.2



→ : FLUSS DES ZERTIFIKATS FÜR DEN ÖFFENTLICHEN SCHLÜSSEL

CA : ZERTIFIKATIONSSTELLE

EE : ENDEINHEIT

VC : ZERTIFIKATIONSPRÜFZENTRUM

SD : SICHERHEITSDOMAIN

FIG.3

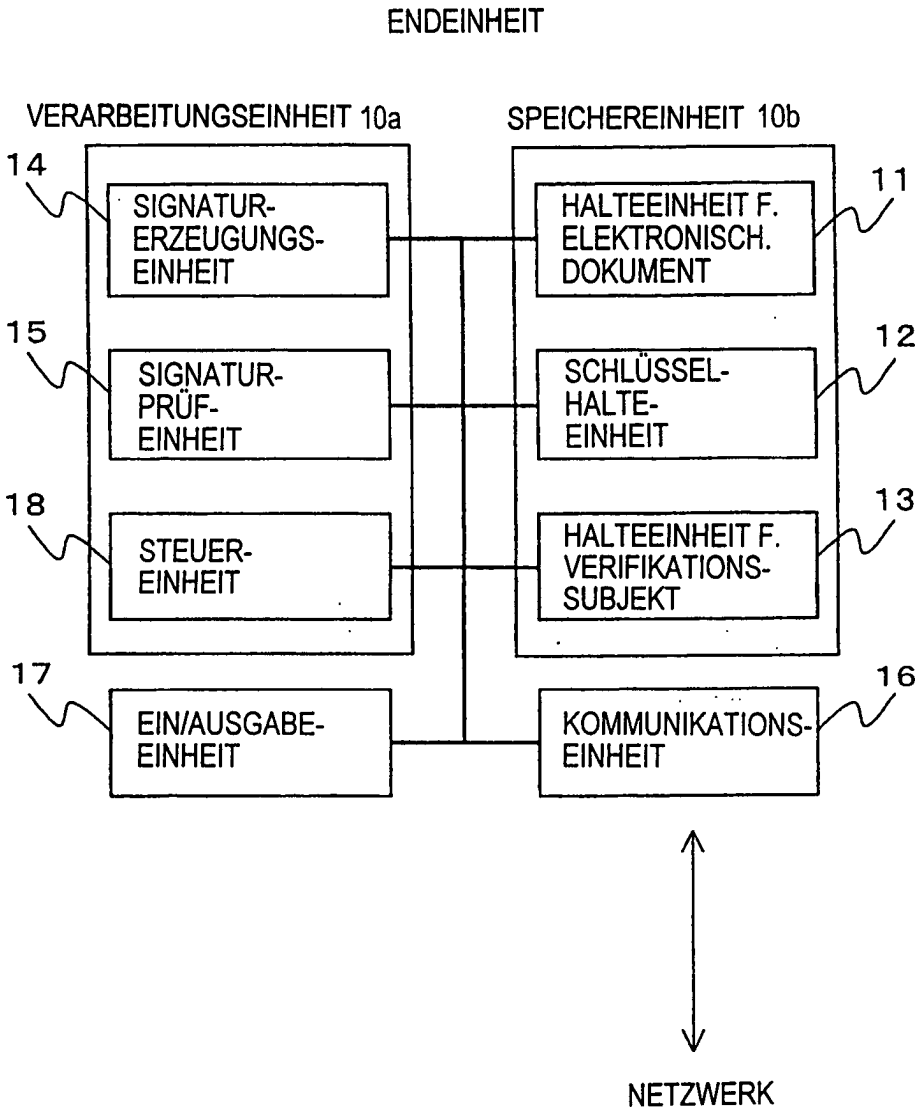

ENDEINHEIT
VERARBEITUNGSEINHEIT 10a
SPEICHEREINHEIT 10b
14
SIGNATUR-ERZEUGUNGS-EINHEIT
15
SIGNATUR-PRÜF-EINHEIT
18
STEUER-EINHEIT
17
EIN/AUSGABE-EINHEIT
11
HALTEEINHEIT F. ELEKTRONISCH. DOKUMENT
12
SCHLÜSSEL-HALTE-EINHEIT
13
HALTEEINHEIT F. VERIFIKATIONS-SUBJEKT
16
KOMMUNIKATIONS-EINHEIT
NETZWERK

FIG.4

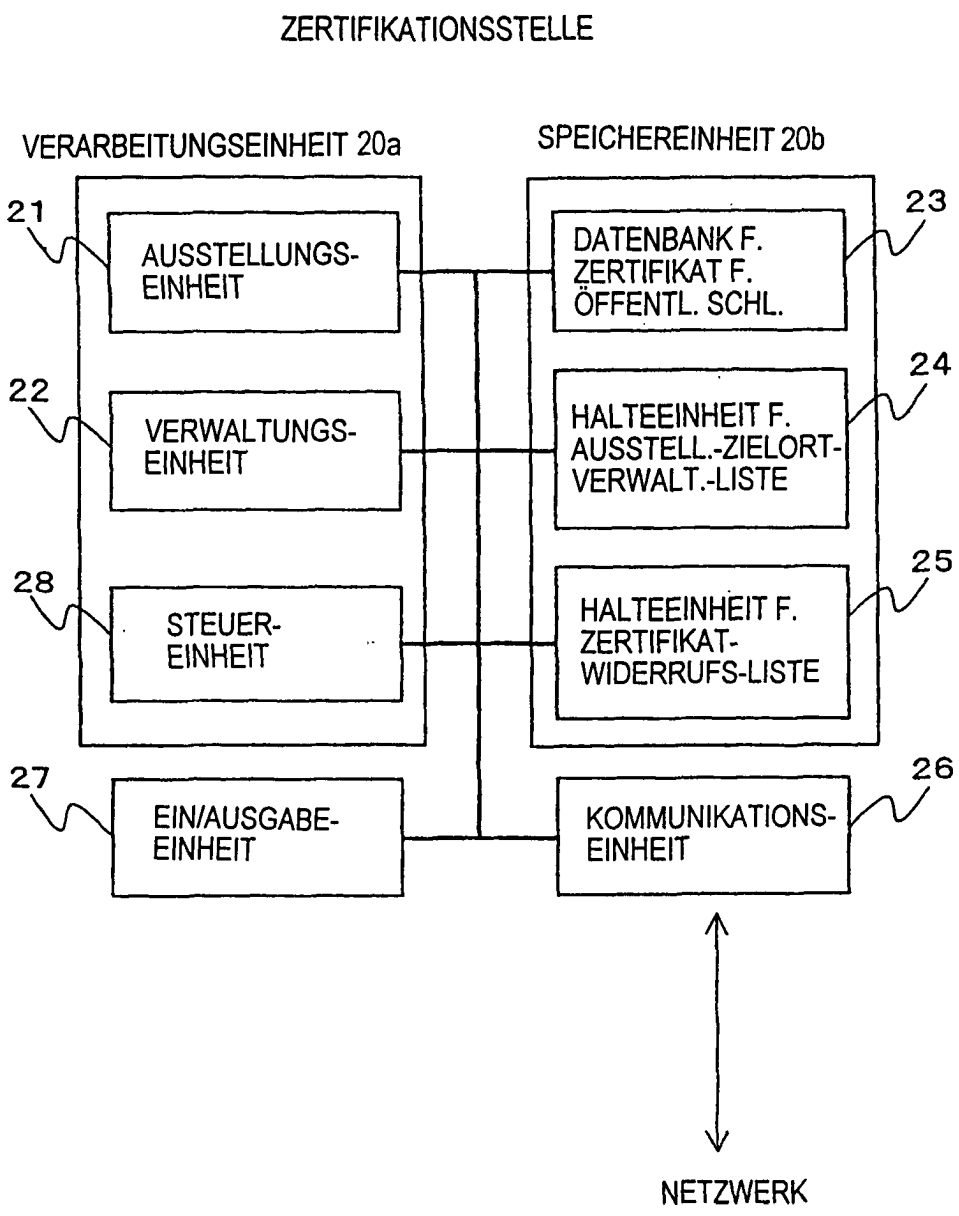

ZERTIFIKATIONSSTELLE
VERARBEITUNGSEINHEIT 20a
SPEICHEREINHEIT 20b
21
AUSSTELLUNGS-EINHEIT
22
VERWALTUNGS-EINHEIT
28
STEUER-EINHEIT
27
EIN/AUSGABE-EINHEIT
23
DATENBANK F. ZERTIFIKAT F. ÖFFENTL. SCHL.
24
HALTEEINHEIT F. AUSSTELL.-ZIELORT-VERWALT.-LISTE
25
HALTEEINHEIT F. ZERTIFIKAT-WIDERRUFS-LISTE
26
KOMMUNIKATIONS-EINHEIT
NETZWERK

FIG.5

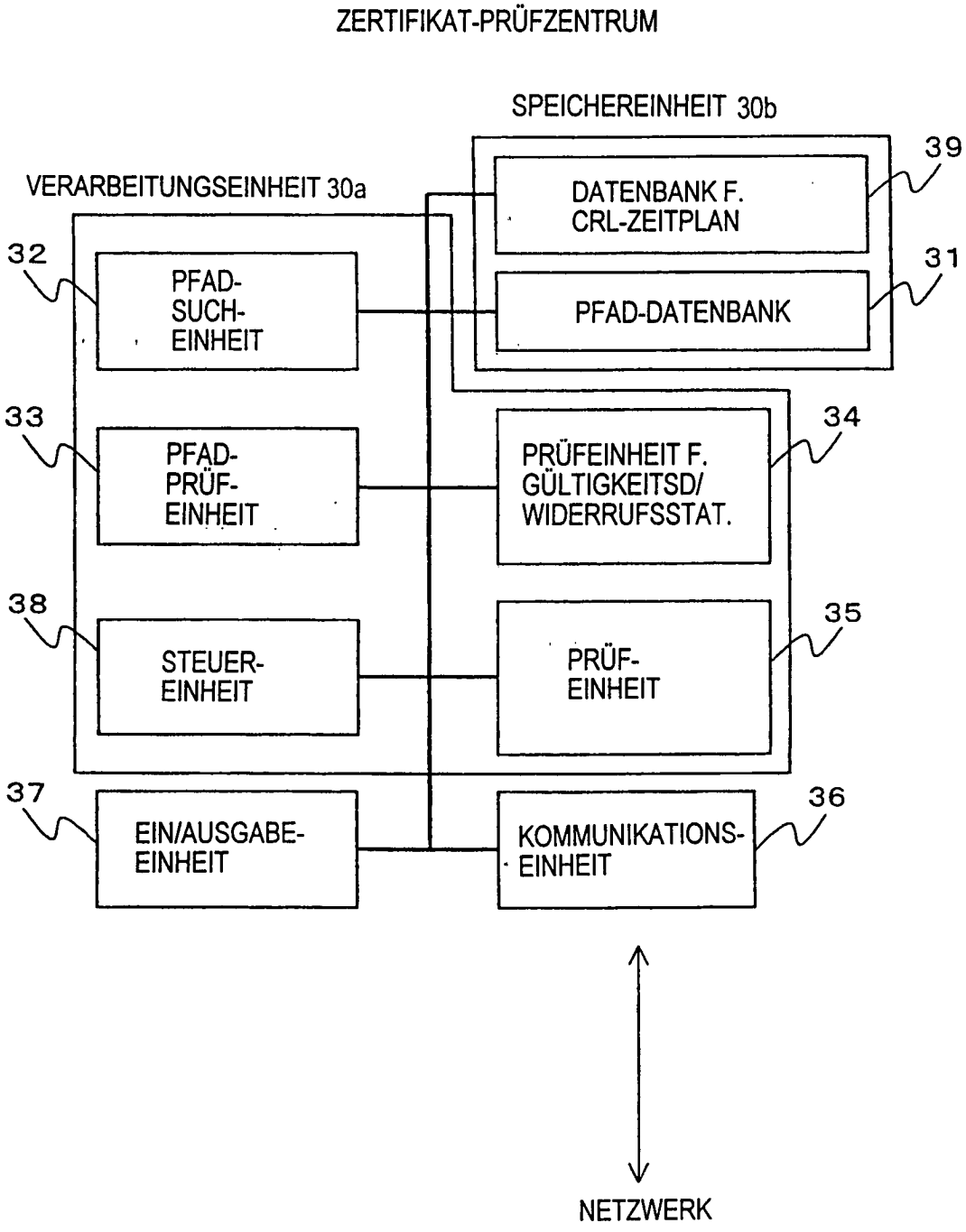

ZERTIFIKAT-PRÜFZENTRUM
SPEICHEREINHEIT 30b
VERARBEITUNGSEINHEIT 30a
39
DATENBANK F. CRL-ZEITPLAN
31
PFAD-DATENBANK
32
PFAD-SUCH-EINHEIT
33
PFAD-PRÜF-EINHEIT
34
PRÜFEINHEIT F. GÜLTIGKEITSD/ WIDERRUFSSTAT.
38
STEUER-EINHEIT
35
PRÜF-EINHEIT
37
EIN/AUSGABE-EINHEIT
36
KOMMUNIKATIONS-EINHEIT
NETZWERK

FIG.6

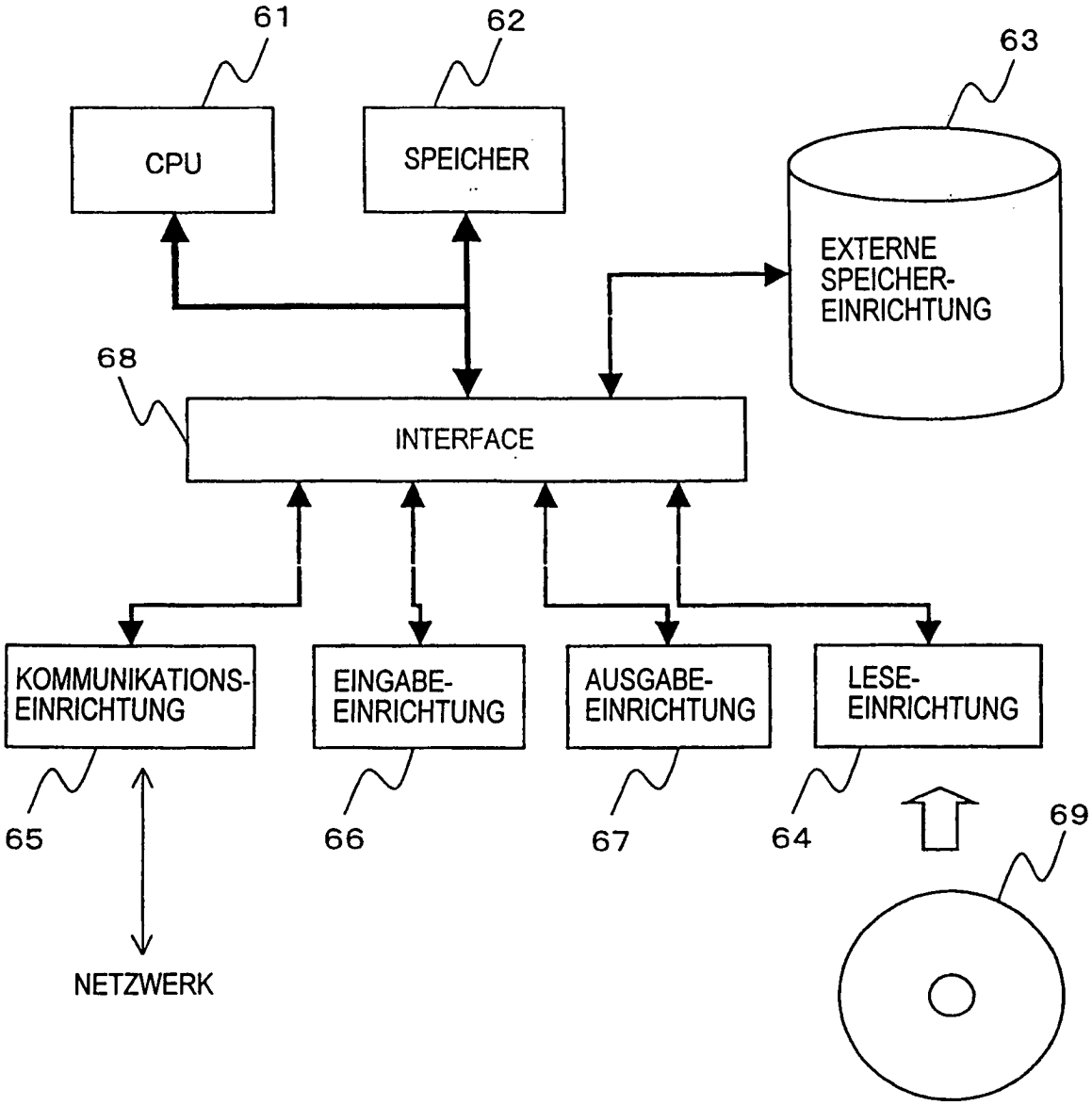

61
62
63
CPU
SPEICHER
EXTERNE SPEICHER-EINRICHTUNG
68
INTERFACE
KOMMUNIKATIONS-EINRICHTUNG
EINGABE-EINRICHTUNG
AUSGABE-EINRICHTUNG
LESE-EINRICHTUNG
65
66
67
64
69
NETZWERK

FIG.7

OPERATION ZUM SUCHEN NACH, PRÜFEN UND VERWALTEN VON PFADEN

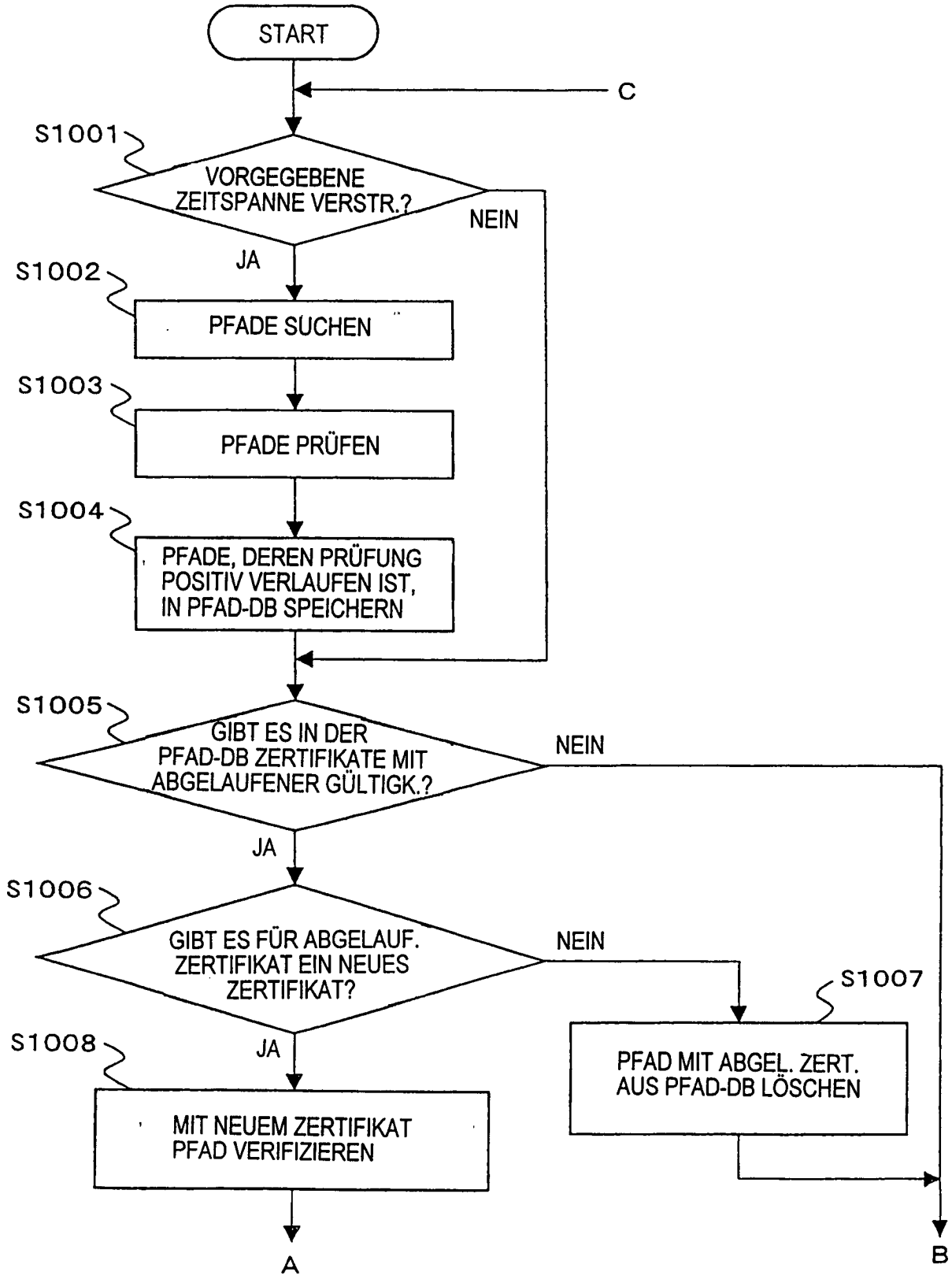


FIG.8

OPERATION ZUM SUCHEN NACH, PRÜFEN UND VERWALTEN VON PFADEN

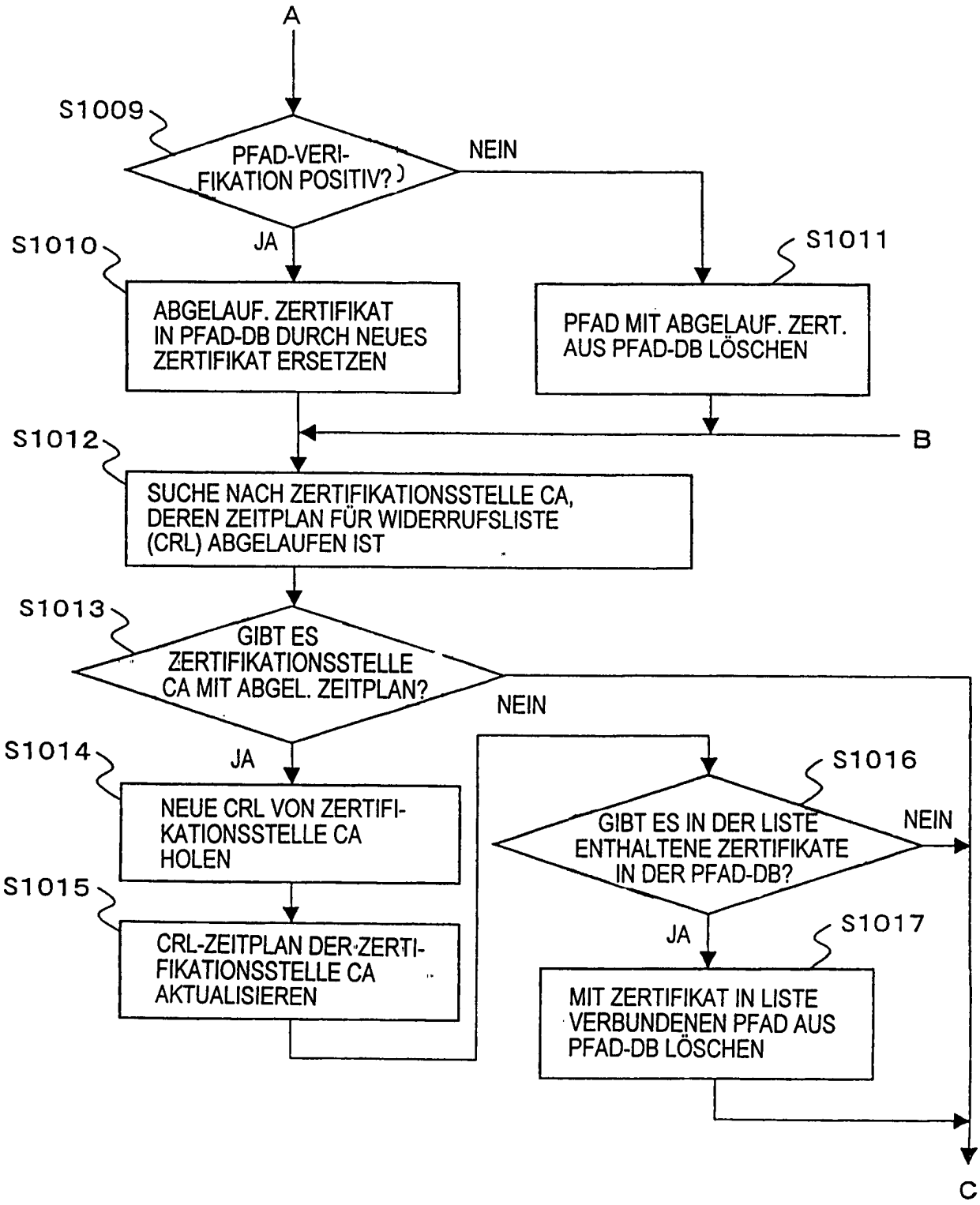


FIG.9

PFADSUCHERGEBNIS (FÜR DIE FIG. 2)

TERMINAL-ZERTIFIKATIONS-STELLE	PFAD
CA_{12}	CA_{bride}–CA_{11}–CA_{12}
CA_{13}	CA_{bride}–CA_{11}–CA_{13}
CA_{24}	CA_{bride}–CA_{21}–CA_{22}–CA_{24}
	CA_{bride}–CA_{31}–CA_{21}–CA_{22}–CA_{24}
CA_{25}	CA_{bride}–CA_{21}–CA_{22}–CA_{25}
	CA_{bride}–CA_{21}–CA_{23}–CA_{26}–CA_{25}
	CA_{bride}–CA_{31}–CA_{21}–CA_{22}–CA_{25}
	CA_{bride}–CA_{31}–CA_{21}–CA_{23}–CA_{26}–CA_{25}
CA_{26}	CA_{bride}–CA_{21}–CA_{23}–CA_{26}
	CA_{bride}–CA_{21}–CA_{22}–CA_{25}–CA_{26}
	CA_{bride}–CA_{31}–CA_{21}–CA_{23}–CA_{26}
	CA_{bride}–CA_{31}–CA_{21}–CA_{22}–CA_{25}–CA_{26}
CA_{32}	CA_{bride}–CA_{31}–CA_{32}
	CA_{bride}–CA_{21}–CA_{31}–CA_{32}

FIG.10

OPERATION ZUM PRÜFEN DER GÜLTIGKEIT VON ZERTIFIKATEN F. ÖFFENTL. SCHLÜSSEL

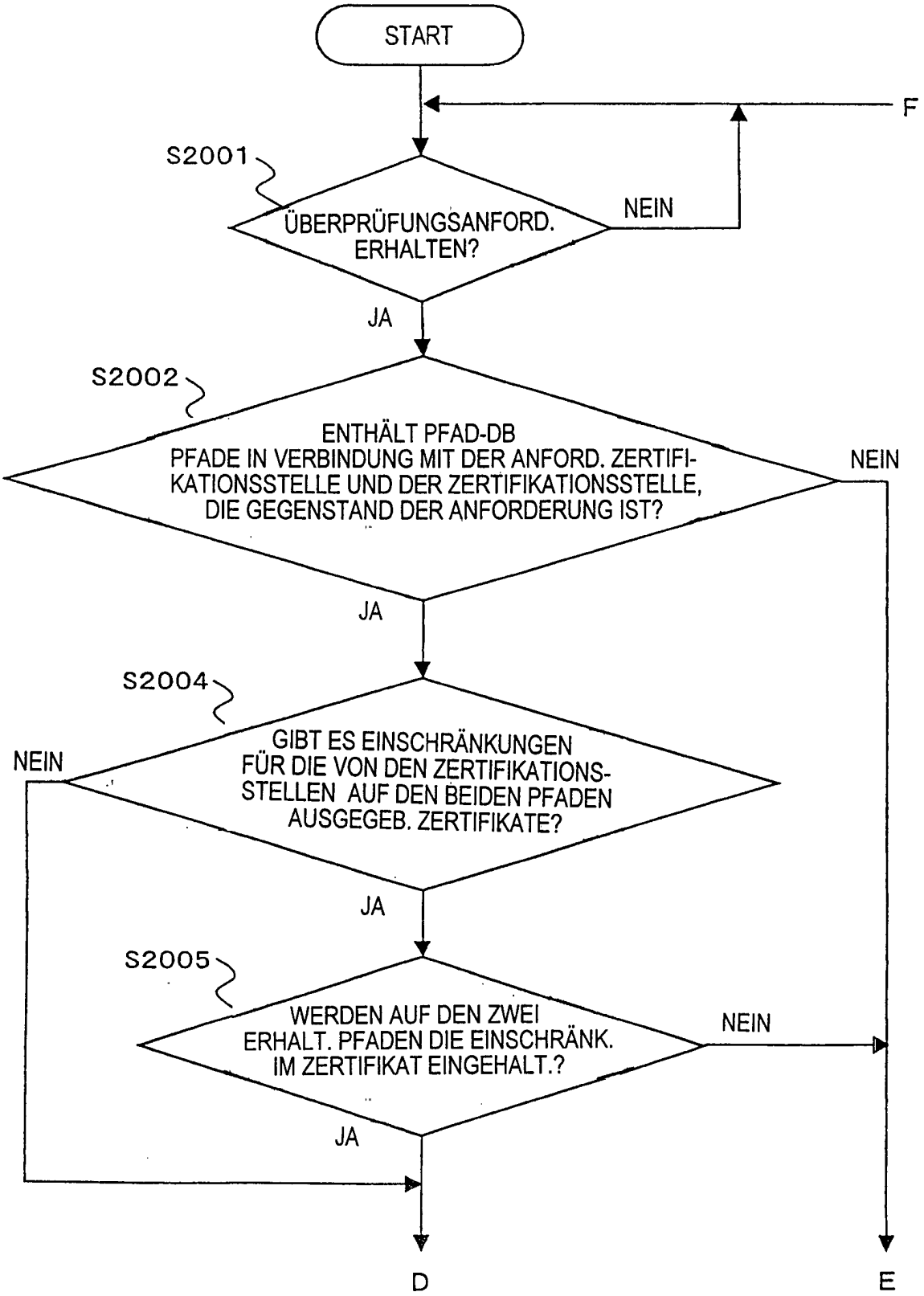


FIG.11

OPERATION ZUM PRÜFEN DER GÜLTIGKEIT VON ZERTIFIKATEN F. ÖFFENTL. SCHLÜSSEL

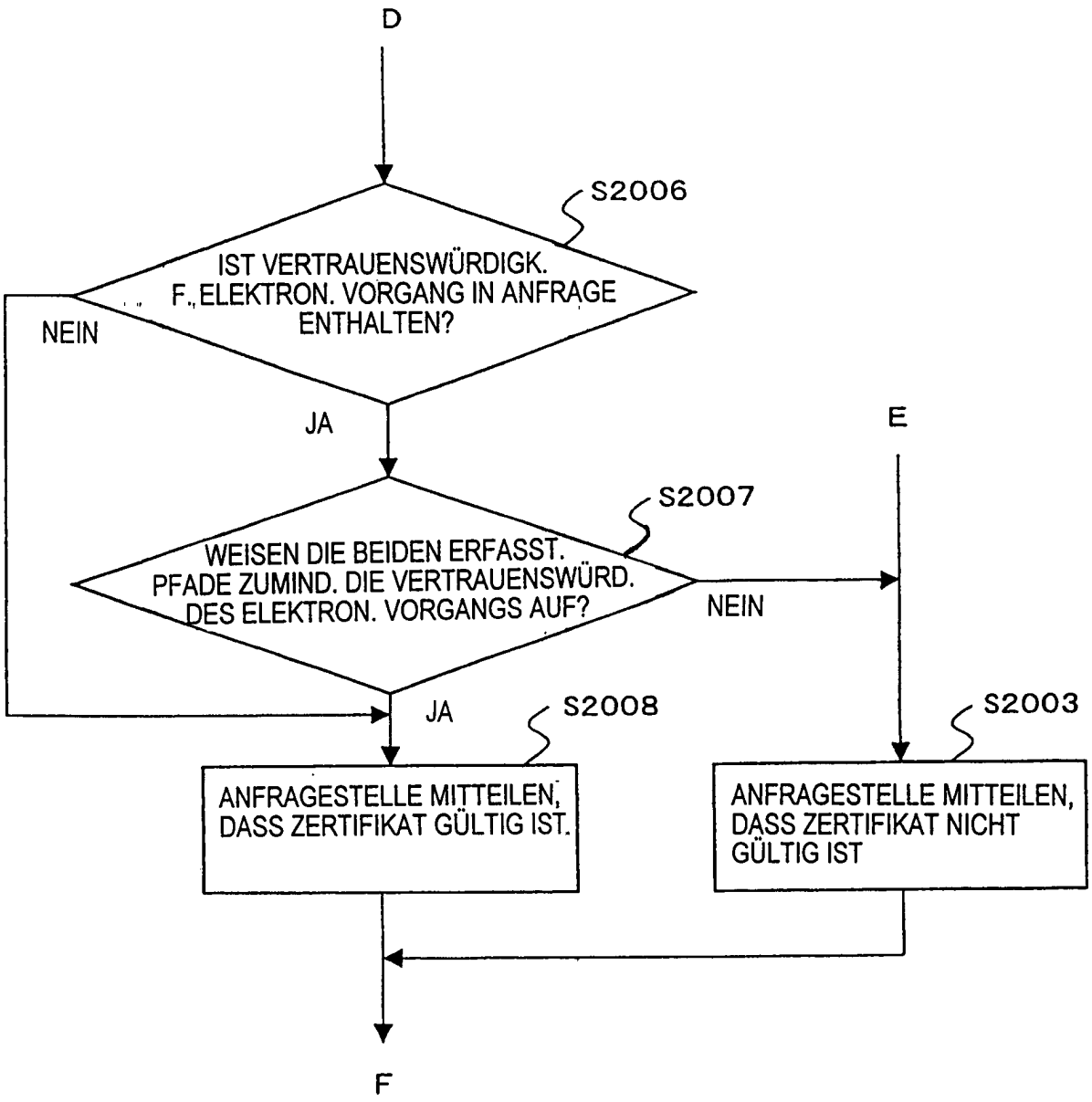
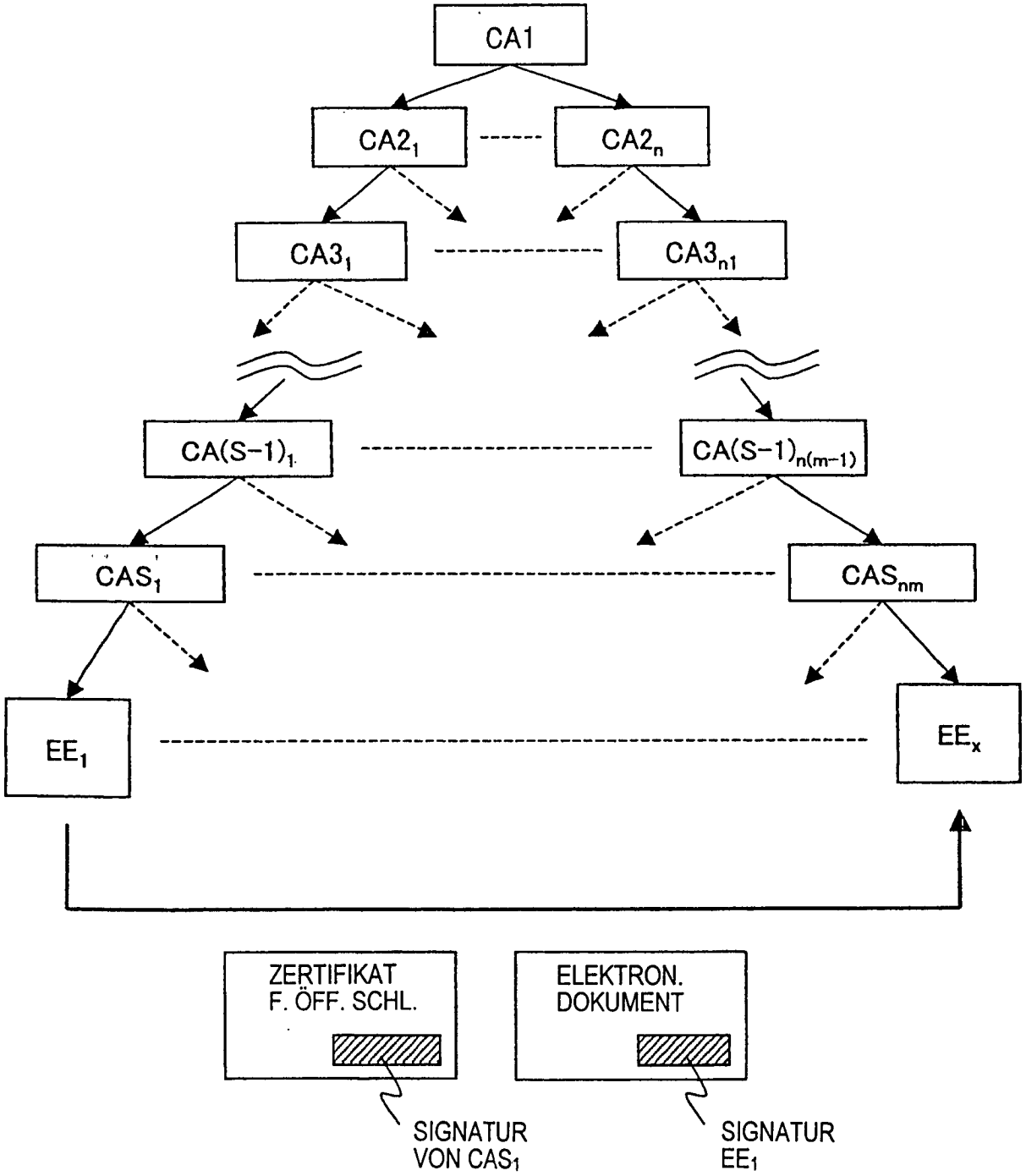


FIG.12



CA : ZERTIFIKATIONSSTELLE

EE : ENDEINHEIT

→ : FLUSS DES ZERTIFIKATS FÜR DEN ÖFFENTLICHEN SCHLÜSSEL