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

(10) **DE 600 26 468 T2** 2006.08.31

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 130 491 B1**
(21) Deutsches Aktenzeichen: **600 26 468.8**
(96) Europäisches Aktenzeichen: **00 310 771.1**
(96) Europäischer Anmeldetag: **04.12.2000**
(97) Erstveröffentlichung durch das EPA: **05.09.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **08.03.2006**
(47) Veröffentlichungstag im Patentblatt: **31.08.2006**

(51) Int Cl.[8]: ***G06F 21/00*** (2006.01)
***H04L 9/32*** (2006.01)

(30) Unionspriorität:
**483189** **14.01.2000** **US**

(73) Patentinhaber:
**Hewlett-Packard Development Company, 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: **Digitales Zertifikat mit Berechtigungsdaten**

## Beschreibung

**[0001]** Diese Patentanmeldung ist mit den folgenden Patentanmeldungen verwandt: EP 11172004 A2 mit dem Titel „AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY", US 6763459-B1 mit dem Titel „LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING DISPOSABLE CERTIFICATES", JP 2001217829-A mit dem Titel "LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE USING CERTIFICATES WITH NO SIGNATURE" und WO 0152476-A2 mit dem Titel "PUBLIC KEY VALIDATION SERVICE", die alle zum selben Datum wie die vorliegende Anmeldung eingereicht wurden und an dieselbe Anmelderin wie die vorliegende Anmeldung übertragen wurden.

**[0002]** Die vorliegende Erfindung bezieht sich darauf, die Identität und/oder die Fähigkeiten einer Entität in einem Datennetzwerk zu verifizieren, und bezieht sich insbesondere auf eine Vorrichtung und ein Verfahren zum Verwenden von hierarchisch strukturierten digitalen Zertifikaten, die Autorisierungsinformationen enthalten, um die Identität und/oder Fähigkeiten einer Entität in einem Datennetzwerk zu verifizieren.

**[0003]** Im Alltag entsteht Vertrauen zwischen einzelnen Personen auf der Grundlage von Charakteristika, die die Beziehung der Einzelpersonen und die Identität der betreffenden Einzelperson definieren, z. B. Bekanntheit, Beschäftigung, Status der betreffenden Einzelperson und Bezeugungen durch Dritte. Jedoch entsteht Vertrauen zwischen Einzelpersonen, die in einem öffentlichen Internet kommunizieren, üblicherweise nicht auf derart einfache und unkomplizierte Weise, da Einzelpersonen im Cyberspace fast jede beliebige Identität annehmen können. Obwohl das öffentliche Internet Flexibilität und Freiheit bietet, ist das öffentliche Internet auch in hohem Maße eine Quelle des Misstrauens, insbesondere wenn einer Einzelperson Befugnisse erteilt werden oder wenn persönliche, sensible oder vertrauliche Informationen übermittelt werden.

**[0004]** Im öffentlichen Internet wird ein digitales Zertifikat üblicherweise dazu verwendet, die Identität und/oder Fähigkeiten eines Subjekts oder Absenders des digitalen Zertifikats, das einem Empfänger oder einem sich auf das digitale Zertifikat Verlassenden präsentiert wird, zu verifizieren. Ein Dritter, der als Zertifikat-Befugnisstelle oder Aussteller des digitalen Zertifikats bezeichnet wird, stellt Nachforschungen bezüglich des eine Zertifizierung wünschenden Subjekts/Absenders an und stellt dem Subjekt/Absender ein digitales Zertifikat aus, um zu bezeugen, dass das Subjekt/der Absender der Nachricht in der Tat dasjenige bzw. derjenige ist, für das bzw. den es bzw. er sich ausgibt. Die Zertifikat-Befugnisstelle signiert das digitale Zertifikat auf digitale Weise. Das Subjekt des digitalen Zertifikats präsentiert das signierte digitale Zertifikat des sich Verlassenden, die der Zertifikat-Befugnisstelle vertraut. Der sich Verlassende berechnet einen kryptographischen Hash des Inhalts des digitalen Zertifikats und verwendet den kryptographischen Hash zusammen mit einem öffentlichen Schlüssel der Zertifikat-Befugnisstelle, der ohne weiteres verfügbar ist, um die digitale Signatur zu verifizieren. Die Verifizierung der digitalen Signatur verifiziert, dass das digitale Zertifikat durch die Zertifikat-Befugnisstelle erstellt wurde.

**[0005]** Elementare digitale Öffentlicher-Schlüssel-Zertifikate enthalten einen öffentlichen Schlüssel und einen dem Absender zugeordneten Namen. Erweiterte Öffentlicher-Schlüssel-Zertifikate enthalten in der Regel zusätzliche Autorisierungsinformationsfelder, die bei den elementaren Öffentlicher-Schlüssel-Zertifikaten nicht zu finden sind. Autorisierungszertifikate lassen den Namen weg und binden den öffentlichen Schlüssel direkt an Autorisierungsinformationen. Attributszertifikate lassen den öffentlichen Schlüssel weg und binden den Namen an Autorisierungsinformationen.

**[0006]** Derzeit ist der führende Standard bei digitalen Zertifikaten X.509, Version 3 (X.509v3). Der X.509v3-Standard ist ein Erweitertes-Öffentlicher-Schlüssel-Zertifikat-Standard, der zusätzliche Autorisierungsinformationsfelder enthalten kann, die bei den elementaren Öffentlicher-Schlüssel-Zertifikaten nicht zu finden sind. Der X.509v3-Standard unterstützt eine Secure Sockets Layer 3.0-Verschlüsselung zusammen mit anderen Verschlüsselungsschemata. Sowohl Netscape Communicator 4.0 als auch Internet Explorer 4.0 von Microsoft unterstützen X.509v3-Zertifikate.

**[0007]** Bei digitalen X.509v3-Zertifikaten weist jedes Erweiterungsfeld ein Kritikalitätsflag auf. Das Kritikalitätsflag wird in Situationen verwendet, in denen dem Empfänger eines digitalen Zertifikats ein oder mehrere Erweiterungsfelder in dem digitalen Zertifikat präsentiert werden, die der Empfänger nicht versteht, vielleicht weil das Erweiterungsfeld neuer ist als das durch den Empfänger verwendete Computerprogramm. Wenn das Kritikalitätsflag nicht gesetzt ist, kann der Empfänger das unbekannte Erweiterungsfeld ignorieren. Wenn das Kritikalitätsflag gesetzt ist, muss der sich Verlassende das digitale Zertifikat zurückweisen.

**[0008]** In bestimmten Situationen ist es zweckmäßig, Informationen, die für mehrere Nutzungszwecke gedacht sind, in demselben digitalen Zertifikat zu sammeln, indem zwei oder mehr nicht aufeinander bezogene Felder in dem digitalen Zertifikat verwendet werden. Dieser Lösungsansatz liefert die Einfachheit eines einzigen digitalen Zertifikats für eine große Bandbreite an Authentisierungs- und Autori-

sierungserfordernissen. Jedoch beeinträchtigt dieser Lösungsansatz die Vertraulichkeit, da alle Empfänger auf alle Felder Zugriff haben, ob sie auf die Erfordernisse des Empfängers bezogen sind oder nicht. Beispielsweise kann ein einziges digitales Zertifikat einen Zugriff auf eine Unix-Plattform gewähren und außerdem die Erlaubnis erteilen, Bestellungen bzw. Aufträge zu signieren. Bei diesem Beispiel weist das digitale Zertifikat Felder eines ersten Typs, die eine Benutzer-ID und eine Gruppen-ID für die Unix-Plattform festlegen, sowie Felder eines zweiten Typs auf, die eine Grenze des Werts von Aufträgen festlegen, die zu signieren der Empfänger des digitalen Zertifikats autorisiert ist. Wenn das digitale Zertifikat verwendet wird, um auf die Unix-Plattform zuzugreifen, sind somit die Felder des zweiten Typs (d. h. die Auftragsgrenze) nicht auf die Anforderungen des Empfängers bezogen und können für den Unix-Administrator sichtbar werden, z. B. indem sie in dem Systemprotokoll aufgezeichnet werden. Der Unix-Administrator hat keinen Bedarf daran, die Grenze des Werts von Aufträgen zu kennen, und es wäre am besten, wenn diese Auftragsinformationen nicht unnötigerweise offenbart würden.

**[0009]** Alternative Lösungsansätze wurden entwickelt, um das Vertraulichkeitsproblem, das sich aus zwei oder mehr nicht aufeinander bezogenen Feldern, die in demselben digitalen Zertifikat vorliegen, ergibt, zu umschiffen. Bei einem ersten alternativen Lösungsansatz wird Vertraulichkeit dadurch erzielt, dass manche oder alle Felder des digitalen Zertifikats verschlüsselt werden. Der erste alternative Lösungsansatz liefert lediglich einen Schutz vor einem Dritten, der die Übertragung des digitalen Zertifikats an den sich Verlassenden belauscht. Dieser erste alternative Lösungsansatz kann keine Vertraulichkeit gegenüber dem Empfänger selbst liefern, da der Empfänger einen Zugriff auf den Klartext des gesamten digitalen Zertifikats benötigt, um einen kryptographischen Hash zu berechnen, der notwendig ist, um das digitale Zertifikat zu validieren.

**[0010]** Bei einem zweiten alternativen Lösungsansatz verwendet der Absender separate digitale Zertifikate, statt Informationen in mehrere, nicht aufeinander bezogene Felder in einem einzigen digitalen Zertifikat zu platzieren. Anstatt beispielsweise ein digitales Zertifikat, das den öffentlichen Schlüssel und den Namen des Absenders enthält, zusammen mit drei Arten von Feldern zu verwenden, die Autorisierungsinformationen für drei nicht verwandte Anwendungen enthalten, verwendet der zweite alternative Lösungsansatz vier separate digitale Zertifikate. Die vier separaten digitalen Zertifikate umfassen ein erstes elementares Öffentlicher-Schlüssel-Zertifikat, das den öffentlichen Schlüssel an den Absendernamen bindet, und drei Attributszertifikate. Jedes Attributszertifikat bindet den Absendernamen an die in dem Feldtyp des gegebenen Attributszertifikats enthaltenen entsprechenden Autorisierungsinformationen. Dieser zweite alternative Lösungsansatz weist insofern einen Vorteil auf, als die vier digitalen Zertifikate durch vier unabhängige Zertifikat-Befugnisstellen signiert werden können. Dagegen weist der zweite alternative Lösungsansatz den Nachteil auf, dass er vier digitale Signaturen statt einer und vier Transaktionen über ein Netzwerk statt einer erfordert, wenn die Zertifikat-Befugnisstelle das digitale Zertifikat an das Subjekt ausstellt. Somit ist der zweite Lösungsansatz rechentechnisch aufwendiger und führt zu mehr Netzwerkverkehr, als wenn die Zertifikat-Befugnisstelle dem Subjekt ein einziges digitales Zertifikat ausstellt.

**[0011]** Bei einem anderen Lösungsansatz, wie er in der SET Secure Electronic Specification, Buch 1: Business Description, Version 1.0 (31. Mai 1997), erörtert wird, werden geschützte Felder unter Verwendung eines „duale Signatur"-Schemas verschlüsselt, bei dem einzelne „Nachrichtensammlungen" miteinander verkettet, signiert und an einen Verifizierer geliefert werden. Die duale Signatur wird unter Verwendung des privaten Schlüssels des Benutzers berechnet, weshalb die Empfänger dem Benutzer vertrauen müssen. Bei einem weiteren Lösungsansatz, der bei J. Press, Secure Transfer of Identity and Privilege Attributes in an Open Systems Environment, Computers & Security, 10 bei 117–27 (1991), erörtert wird, werden geschützte Felder verschlüsselt, bevor das digitale Zertifikat ausgestellt wird, entweder mit dem kryptographischen Schlüssel des Endsystems oder mit einem kryptographischen Schlüssel, den der Aussteller des Zertifikats und eine Entscheidungseinheit, die Vertrauen genießt, gemeinsam verwenden. Bei diesem letzteren Lösungsansatz müssen sich die Feldschutzeinrichtungen bei der Ausstellung des digitalen Zertifikats an Ort und Stelle befinden, und nach dem Ausstellen des digitalen Zertifikats sind die Feldzugriffserlaubnisse nicht rekonfigurierbar.

**[0012]** Die vorliegende Erfindung liefert ein verbessertes digitales Zertifikat.

**[0013]** Gemäß einem Aspekt der vorliegenden Erfindung ist ein System zum Befähigen mehrerer Empfänger eines strukturellen digitalen Zertifikats, ein Subjekt des strukturierten digitalen Zertifikats zu autorisieren, gemäß Anspruch 1 vorgesehen.

**[0014]** Gemäß einem weiteren Aspekt der vorliegenden Erfindung ist ein Verfahren zum Liefern einer Vertraulichkeit von Autorisierungsinformationen gemäß Anspruch 3 vorgesehen.

**[0015]** Die bevorzugten Ausführungsbeispiele können einen verbesserten Typ eines digitalen Zertifikats und entsprechende verbesserte Verfahren zum Verwenden des digitalen Zertifikats liefern, so dass, wenn der Absender eines digitalen Zertifikats das di-

gitale Zertifikat dem Empfänger des digitalen Zertifikats für einen gegebenen Zweck präsentiert, lediglich diejenigen Felder des digitalen Zertifikats, die durch den Empfänger geprüft werden müssen, dem Empfänger gegenüber offengelegt werden. Das bevorzugte gewünschte digitale Zertifikat liefert diesen Empfängervertraulichkeitsschutz ohne den zusätzlichen Mehraufwand an Rechenleistung und Netzwerkverkehr, der sich aus dem Ausstellen digitaler Zertifikate ergibt.

**[0016]** Gemäß dem bevorzugten Ausführungsbeispiel ist ein strukturiertes digitales Zertifikat zum Befähigen eines ersten Empfängers des strukturierten digitalen Zertifikats, einen Absender des strukturierten digitalen Zertifikats zu autorisieren, vorgesehen. Das strukturierte digitale Zertifikat umfasst einen ersten Typ eines Feldes von Autorisierungsinformationen, die für den ersten Empfänger relevant und für den ersten Empfänger lesbar sind. Das strukturierte digitale Zertifikat umfasst einen ersten kryptographischen Ordner, der einen zweiten Typ eines Feldes von Autorisierungsinformationen enthält, die für einen zweiten Empfänger relevant sind. Der zweite Typ eines Feldes von Autorisierungsinformationen ist für den ersten Empfänger nicht lesbar.

**[0017]** Bei einem Ausführungsbeispiel umfasst das strukturierte digitale Zertifikat einen zweiten kryptographischen Ordner, der das Feld des ersten Typs enthält. Bei einem Ausführungsbeispiel ist das Feld des ersten Typs nicht in einem Ordner enthalten. Bei einem Ausführungsbeispiel liegen in dem strukturierten digitalen Zertifikat mehrere Felder des ersten Typs vor.

**[0018]** Bei einem Ausführungsbeispiel umfasst das strukturierte digitale Zertifikat einen Absendernamen und einen dem Absender zugeordneten öffentlichen Schlüssel.

**[0019]** Bei einem Ausführungsbeispiel der vorliegenden Erfindung sind die kryptographischen Ordner von Autorisierungsinformationen strukturierte Felder, die eine Mehrzahl verschachtelter Felder enthalten. Jedes der Mehrzahl verschachtelter Felder kann selbst ein Ordner sein. Bei einem Ausführungsbeispiel ist das digitale Zertifikat ein digitales X.509v3-Zertifikat. Das digitale X.509v3-Zertifikat kann Erweiterungsfelder umfassen, die beschreiben, wie die Zertifizierung verwendet werden kann. Die Erweiterungsfelder umfassen ein oder mehrere Kritikalitätsflags. Bei einem Ausführungsbeispiel enthalten die nicht aufeinander bezogenen kryptographischen Ordner einen verschlüsselten Hashwert.

**[0020]** Das bevorzugte Ausführungsbeispiel sieht ferner ein Verfahren zum Bereitstellen einer Vertraulichkeit von Autorisierungsinformationen in einem digitalen Zertifikat vor, das von mehreren Empfängern gemeinsam verwendet wird. Das Verfahren sieht kryptographische Ordner in dem digitalen Zertifikat vor. Zumindest ein kryptographischer Ordner eines ersten Typs enthält zumindest ein Feld, eines ersten Typs, von Autorisierungsinformationen, die für einen ersten Empfänger relevant sind. Zumindest ein kryptographischer Ordner eines zweiten Typs enthält zumindest ein Feld, eines zweiten Typs, von Autorisierungsinformationen, die für einen zweiten Empfänger relevant sind. Die Zertifikat-Befugnisstelle erstellt das digitale Zertifikat, indem sie das digitale Zertifikat signiert und das signierte digitale Zertifikat an das Subjekt sendet. Das Subjekt übermittelt anschließend das signierte digitale Zertifikat an den ersten Empfänger. Das zumindest eine Feld, des ersten Typs, von Autorisierungsinformationen ist für den ersten Empfänger lesbar. Das zumindest eine Feld, des zweiten Typs, von Autorisierungsinformationen ist für den ersten Empfänger nicht lesbar. Der erste Empfänger verifiziert die Authentizität des signierten digitalen Zertifikats.

**[0021]** Gemäß einem weiteren Aspekt der vorliegenden Erfindung ist ein Verfahren zum Signieren eines digitalen Zertifikats bei einer Zertifikatsbefugnisstelle vorgesehen. Das Verfahren sieht kryptographische Ordner in dem digitalen Zertifikat vor, die Autorisierungsinformationen aufweisen. Die Zertifikatsbefugnisstelle schließt alle kryptographischen Ordner in dem digitalen Zertifikat. Ein kryptographischer Hash des digitalen Zertifikats wird berechnet, wenn alle Ordner geschlossen sind. Eine Digitales-Zertifikat-Signatur wird mit dem berechneten kryptographischen Hash des digitalen Zertifikats und einem privaten Schlüssel der Zertifikatsbefugnisstelle berechnet.

**[0022]** Bei einem Ausführungsbeispiel wird ein gegebener kryptographischer Ordner X gemäß der vorliegenden Erfindung auf folgende Weise geschlossen. Alle verschachtelten Ordner in dem Ordner X werden rekursiv geschlossen. Aus dem Inhalt des Ordners X, einschließlich aller rekursiv geschlossenen verschachtelten Ordner in dem Ordner X, wird ein kryptographischer Hash berechnet. Der Inhalt des Ordners X wird durch den berechneten kryptographischen Hash des Inhalts des Ordners X ersetzt. In dem Anfangsblock des Ordners X wird ein Flag gesetzt, um anzuzeigen, dass der Ordner X geschlossen ist.

**[0023]** Gemäß einem weiteren Aspekt der vorliegenden Erfindung ist ein Verfahren zum Liefern eines digitalen Zertifikats von einem Subjekt des digitalen Zertifikats an einen Empfänger des digitalen Zertifikats vorgesehen. Das Verfahren sieht kryptographische Ordner in dem digitalen Zertifikat vor, die Autorisierungsinformationen aufweisen. Eine Digitales-Zertifikat-Signatur wird von einer Zertifikatsbefugnisstelle an das Subjekt des Zertifikats übermittelt. Eine unsignierte Kopie des digitalen Zertifikats wird

von der Zertifikatsbefugnisstelle an das Subjekt des Zertifikats übermittelt. Jegliche Ordner in der unsignierten Kopie des digitalen Zertifikats, die keine für den Empfänger relevanten Autorisierungsinformationen aufweisen, werden geschlossen. Die unsignierte Kopie des digitalen Zertifikats und die Digitales-Zertifikat-Signatur werden von dem Subjekt des digitalen Zertifikats an den Empfänger übermittelt.

**[0024]** Bei einem Ausführungsbeispiel der vorliegenden Erfindung wird der Schritt des Übermittelns einer Kopie des unsignierten digitalen Zertifikats von der Zertifikatsbefugnisstelle an das Subjekt des Zertifikats über einen sicheren Zustellungskanal durchgeführt. Bei einem Ausführungsbeispiel wird der sichere Zustellungskanal über Internet Protocol Security (IPSEC) geschützt. Bei einem anderen Ausführungsbeispiel wird der sichere Zustellungskanal durch Secure Sockets Layer (SSL) geschützt.

**[0025]** Gemäß einem weiteren Aspekt der vorliegenden Erfindung ist ein Verfahren zum Verifizieren einer Signatur für ein digitales Zertifikat vorgesehen, das durch ein Subjekt des digitalen Zertifikats an einen Empfänger des digitalen Zertifikats gesendet wird. Das Verfahren sieht kryptographische Ordner in dem digitalen Zertifikat vor, die Autorisierungsinformationen aufweisen. Der Empfänger erhält einen öffentlichen Schlüssel der Zertifikatsbefugnisstelle, der einem privaten Schlüssel entspricht, der durch die Zertifikatsbefugnisstelle verwendet wird, um das digitale Zertifikat zu signieren. Der Empfänger schließt jegliche kryptographischen Ordner, die in dem digitalen Zertifikat durch das Subjekt des digitalen Zertifikats offen gelassen wurden. Der Empfänger berechnet einen kryptographischen Hash des digitalen Zertifikats. Der Empfänger authentifiziert die Signatur für das digitale Zertifikat.

**[0026]** Das strukturierte digitale Zertifikat und entsprechende Verfahren zum Verwenden des strukturellen digitalen Zertifikats gemäß den beschriebenen Ausführungsbeispielen bieten im Vergleich zu herkömmlichen digitalen Zertifikaten mehrere Vorteile. Ein einziges strukturiertes digitales Zertifikat gemäß der vorliegenden Erfindung kann für mehrere, nicht aufeinander bezogene Zwecke verwendet werden und trotzdem einen Empfängervertraulichkeitsschutz ohne den zusätzlichen rechentechnischen und Netzwerkverkehr-Mehraufwand, der sich aus einem Senden mehrerer digitaler Zertifikate ergibt, liefern. Die hierarchische Struktur von kryptographischen Ordnern, die bei der vorliegenden Erfindung verwendet werden, ermöglicht, dass lediglich diejenigen Felder des strukturierten digitalen Zertifikats offengelegt werden, die durch den Empfänger zu einem gegebenen spezifischen Zweck geprüft werden müssen. Da in der Regel alle Ordner eines strukturierten digitalen Zertifikats bis auf einen geschlossen werden (d. h. der Inhalt des durch einen kryptographischen Hash ersetzten Ordners), wird weniger Zeit benötigt, das digitale Zertifikat über das Netzwerk zu übermitteln, wenn das digitale Zertifikat über ein Netzwerk von dem Absender an den Empfänger übermittelt wird.

**[0027]** Ein Ausführungsbeispiel der vorliegenden Erfindung wird nachstehend lediglich beispielhaft unter Bezugnahme auf die beiliegenden Zeichnungen beschrieben. Es zeigen:

**[0028]** Fig. 1 ein Blockdiagramm eines Ausführungsbeispiels eines strukturierten digitalen Zertifikats;

**[0029]** Fig. 2 ein Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens zum Liefern einer Feldvertraulichkeit bei digitalen Zertifikaten veranschaulicht;

**[0030]** Fig. 3A ein Flussdiagramm, das ein Ausführungsbeispiel und ein Verfahren zum Signieren strukturierter digitaler Zertifikate bei einer Zertifikat-Befugnisstelle veranschaulicht;

**[0031]** Fig. 3B ein Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens zum Schließen eines gegebenen kryptographischen Ordners X veranschaulicht;

**[0032]** Fig. 4 ein Block- und Datenflussdiagramm, das veranschaulicht, wie eine Signatur für ein strukturiertes digitales Zertifikat bei einer Zertifikat-Befugnisstelle erzeugt wird;

**[0033]** Fig. 5 ein Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens zum Liefern eines strukturierten digitalen Zertifikats und einer entsprechenden verschlüsselten Nachricht an einen Nachrichtenempfänger veranschaulicht;

**[0034]** Fig. 6 ein Block- und Datenflussdiagramm, das veranschaulicht, wie ein strukturiertes digitales Zertifikat über das Subjekt des Zertifikats von einer Zertifikat-Befugnisstelle an einen Nachrichtenempfänger geliefert wird;

**[0035]** Fig. 7 ein Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens zum Verifizieren der Authentizität einer Signatur eines strukturierten digitalen Zertifikats veranschaulicht;

**[0036]** Fig. 8 ein Block- und Datenflussdiagramm, das veranschaulicht, wie ein Ausführungsbeispiel eines Nachrichtenempfängers die Authentizität eines strukturierten digitalen Zertifikats verifiziert; und

**[0037]** Fig. 9 ein Blockdiagramm eines Computersystems und ein entsprechendes computerlesbares Medium, die eine Funktion zum Bereitstellen einer Feldvertraulichkeit bei digitalen Zertifikaten beinhal-

ten.

**[0038]** Bei der folgenden ausführlichen Beschreibung der bevorzugten Ausführungsbeispiele wird auf die beiliegenden Zeichnungen, die einen Teil des vorliegenden Dokuments bilden, und in denen auf veranschaulichende Weise spezifische Ausführungsbeispiele, bei denen die Erfindung praktiziert werden kann, gezeigt sind, Bezug genommen. Es versteht sich, dass auch andere Ausführungsbeispiele verwendet werden können und strukturelle oder logische Änderungen vorgenommen werden können, ohne von dem Schutzumfang der Patentansprüche abzuweichen. Somit ist die folgende ausführliche Beschreibung nicht in einem einschränkenden Sinne zu verstehen.

**[0039]** Fig. 1 ist ein Blockdiagramm eines Ausführungsbeispiels eines strukturierten digitalen Zertifikats **30**. Das strukturierte digitale Zertifikat **30** ist eine seitens eines Ausstellers (d. h. einer Zertifikat-Befugnisstelle) digital signierte Datenstruktur, die Autorisierungsinformationen über eine andere Entität, die als Subjekt (d. h. Absender) bezeichnet wird, umfasst. Das Subjekt des strukturierten digitalen Zertifikats **30** präsentiert das strukturierte digitale Zertifikat Dritten, die dem Aussteller des strukturierten digitalen Zertifikats **30** vertrauen. Die Dritten werden als sich Verlassende (d. h. Empfänger) bezeichnet. Der sich Verlassende berechnet einen kryptographischen Hash des strukturierten digitalen Zertifikats **30** und verwendet diesen Hash zusammen mit dem öffentlichen Schlüssel des Ausstellers, der ohne weiteres verfügbar ist, um die digitale Signatur des strukturierten digitalen Zertifikats **30** zu verifizieren.

**[0040]** Bei einem Ausführungsbeispiel ist das strukturierte digitale Zertifikat **30** ein elementares Öffentlicher-Schlüssel-Zertifikat und umfasst einen öffentlichen Schlüssel **32** und einen Absendernamen **34**, der dem Subjekt des strukturierten digitalen Zertifikats **30** zugeordnet ist. Bei einem anderen Ausführungsbeispiel ist das strukturierte digitale Zertifikat **30** ein erweitertes Öffentlicher-Schlüssel-Zertifikat und umfasst zusätzlich zu dem öffentlichen Schlüssel **32** und dem Absendernamen **34** zusätzliche Felder **36**, **37** und/oder kryptographische Ordner **38**, **40**, **42** und **44**, die Autorisierungsinformationen enthalten. Ein Beispiel eines erweiterten Öffentlicher-Schlüssel-Zertifikats ist ein X.509v3-Zertifikat, das zuvor in dem Abschnitt Hintergrund der Erfindung der vorliegenden Spezifikation beschrieben wurde.

**[0041]** Bei einem Ausführungsbeispiel umfasst das strukturierte digitale Zertifikat **30** Autorisierungsfelder **36** und **37**, die Autorisierungsinformationen enthalten, die für mehrere, nicht aufeinander bezogene Zwecke verwendet werden. Wenn das strukturierte digitale Zertifikat **30** für einen bestimmten Zweck verwendet wird, ist es wünschenswert, die in nicht aufeinander bezogenen Feldern enthaltenen Informationen zu verstecken. Ein beispielhaftes strukturiertes digitales Zertifikat **30** kann verwendet werden, um Zugriff auf eine UNIX-Plattform zu gewähren und um ferner eine Erlaubnis zu gewähren, Aufträge zu signieren. Folglich weist das beispielhafte strukturierte digitale Zertifikat **30** ein Autorisierungsfeld **37** eines ersten Typs, das eine Benutzer-ID und eine Gruppen-ID für die UNIX-Plattform spezifiziert, sowie ein Autorisierungsfeld **36** eines zweiten Typs, das eine Grenze des Werts der Aufträge, die zu signieren das Subjekt autorisiert ist, festlegt, auf. Wenn das beispielhafte strukturierte digitale Zertifikat **30** verwendet wird, um auf die UNIX-Plattform zuzugreifen, werden eventuell alle Autorisierungsfelder **36** und **37** des strukturierten digitalen Zertifikats **30** für den UNIX-Administrator sichtbar, z. B. indem sie in dem Systemprotokoll aufgezeichnet werden. Jedoch besteht für den UNIX-Administrator kein Bedarf, die Grenze des Werts von Aufträgen, die in dem Autorisierungsfeld **36** des zweiten Typs enthalten sind, zu kennen. Somit ist es wünschenswert, die in dem Authentifizierungsfeld **36** des zweiten Typs enthaltenen Informationen zu verstecken, wenn der UNIX-Administrator das strukturierte digitale Zertifikat **30** untersucht.

**[0042]** Bei einem Ausführungsbeispiel wird ein Autorisierungsfeld (oder Autorisierungsfelder) vertraulich gehalten, indem das Autorisierungsfeld in einen der kryptographischen Ordner **38**, **40**, **42** und **44** platziert wird und indem die Autorisierungsinformationen des kryptographischen Ordners durch einen kryptographischen Hash der Autorisierungsinformationen ersetzt werden. Dies wird bewerkstelligt, ohne die Fähigkeit des Empfängers des strukturierten digitalen Zertifikats **30**, die digitale Signatur zu verifizieren, zu beinträchtigen.

**[0043]** Die kryptographischen Ordner **38**, **40**, **42** und **44** sind jeweils ein strukturiertes Feld, das eine beliebige Anzahl verschachtelter Felder enthält. Die verschachtelten Felder können selbst kryptographische Ordner sein. Bei dem veranschaulichten Beispiel enthält das strukturierte digitale Zertifikat **30** vier kryptographische Ordner **38**, **40**, **42** und **44**. Der kryptographische Ordner **42** enthält zwei zusätzliche kryptographische Ordner **46** und **48** zusammen mit dem Autorisierungsfeld **50**. Der kryptographische Ordner **48** enthält einen zusätzlichen kryptographischen Ordner **52** zusammen mit einem Autorisierungsfeld **54**.

**[0044]** Bei einem Ausführungsbeispiel können die kryptographischen Ordner **38**, **40**, **42**, **44**, **46**, **48** und **52** einen von zwei Zuständen, offen oder geschlossen, aufweisen. Der aktuelle Zustand wird durch ein Flag in dem Anfangsblock des kryptographischen Ordners angegeben. Bei digitalen X.509v3-Zertifikaten weist jedes Erweiterungsfeld (d. h. Autorisie-

rungsfeld) ein Kritikalitätsflag auf. Das Kritikalitätsflag wird in Situationen eingesetzt, in denen einem Empfänger (d. h. einem sich Verlassenden) ein oder mehrere Erweiterungsfelder präsentiert werden, die er nicht versteht, vielleicht weil die Erweiterung neuer ist als das Computerprogramm, das der sich Verlassende verwendet. Wenn das Kritikalitätsflag nicht gesetzt ist, kann der sich Verlassende die unbekannte Erweiterung ignorieren. Wenn das Kritikalitätsflag gesetzt ist, weist der sich Verlassende das strukturierte digitale Zertifikat **30** zurück.

**[0045]** Kryptographische Ordner liefern eine erhöhte Flexibilität bei der Verwendung von Kritikalitätsflags; das Zusammenwirken von kryptographischen Ordnern und Kritikalitätsflags muss jedoch umsichtig gehandhabt werden. Ein Autorisierungsfeld ist rekursiv als sichtbar definiert, wenn es sich nicht in einem kryptographischen Ordner befindet oder wenn es sich in einem offenen kryptographischen Ordner befindet, der selbst sichtbar ist. Eine Anwendung muss ein digitales Zertifikat zurückweisen, wenn es ein sichtbares Feld enthält, in dem das Kritikalitätsflag gesetzt ist.

**[0046]** Der Aussteller des strukturierten digitalen Zertifikats **30** muss gewährleisten, dass ein kritisches Feld nicht in einen irrelevanten kryptographischen Ordner platziert wird. Wenn also ein kritisches Feld für einen sich Verlassenden relevant ist, so muss in der Ordnerhierarchie auch jeder kryptographische Ordner, der das Autorisierungsfeld enthält, für diesen sich Verlassenden relevant sein. Diese kryptographischen Ordner müssen offen sein, wenn das strukturierte digitale Zertifikat **30** dem sich Verlassenden präsentiert wird, und das kritische Authentifizierungsfeld muss sichtbar sein.

**[0047]** Fig. 2 ist ein Flussdiagramm eines allgemein bei **100** veranschaulichten Verfahrens zum Bereitstellen einer Feldvertraulichkeit bei strukturierten digitalen Zertifikaten, z. B. dem in Fig. 1 veranschaulichten strukturierten digitalen Zertifikat **30**. Bei Block **102** beginnt das Verfahren **100**, indem das strukturierte digitale Zertifikat **30** bei einer Zertifikat-Befugnisstelle signiert wird. Die Zertifikat-Befugnisstelle (d. h. der Aussteller) des strukturierten digitalen Zertifikats **30** schließt alle kryptographischen Ordner in dem strukturierten digitalen Zertifikat, um eine Signatur für das strukturierte digitale Zertifikat zu erzeugen. Der bei Block **102** angegebene Verfahrensschritt zum Signieren des strukturierten digitalen Zertifikats **30** wird unter Bezugnahme auf Fig. 3A ausführlicher beschrieben.

**[0048]** Nachdem das strukturierte digitale Zertifikat **30** bei Block **102** signiert wurde, werden die Digitales-Zertifikat-Signatur und eine Kopie des digitalen Zertifikats mit zumindest einem kryptographischen offenen Ordner über das Subjekt des digitalen Zertifikats an den Empfänger geliefert, wie bei Block **104** angegeben ist. Lediglich Autorisierungsinformationen, die für den Empfänger relevant sind, sind für den Empfänger in dem signierten digitalen Zertifikat (d. h. über offene Ordner) sichtbar. Der bei Block **104** angegebene Verfahrensschritt zum Liefern des strukturierten digitalen Zertifikats **30** an den Empfänger wird unter Bezugnahme auf Fig. 5 ausführlicher beschrieben.

**[0049]** Auf den Empfang des signierten strukturierten digitalen Zertifikats **30** hin verifiziert der Empfänger die Authentizität des signierten digitalen Zertifikats, wie bei Block **106** angegeben ist. Bevor er das signierte digitale Zertifikat verifiziert, schließt der Empfänger jegliche kryptographischen Ordner, die durch das Subjekt des digitalen Zertifikats offen gelassen wurden. Somit ist der sich Verlassende in der Lage, die Verifikation der Signatur unabhängig von dem Zustand der kryptographischen Ordner in der Kopie des durch das Subjekt präsentierten strukturierten digitalen Zertifikats durchzuführen. Der bei Block **106** angegebene Verfahrensschritt zum Verifizieren der Authentizität des strukturierten digitalen Zertifikats **30** wird unter Bezugnahme auf Fig. 7 ausführlicher beschrieben.

**[0050]** Fig. 3A ist ein Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens **102** zum Signieren strukturierter digitaler Zertifikate **30** bei einer Zertifikat-Befugnisstelle veranschaulicht. Wie zuvor erwähnt wurde, werden jegliche in dem strukturierten digitalen Zertifikat **30** vorhandene kryptographischen Ordner geschlossen, bevor das strukturierte digitale Zertifikat **30** signiert oder verifiziert wird. Das Verfahren **102** beginnt, indem alle kryptographischen Ordner in dem strukturierten digitalen Zertifikat **30** geschlossen werden, wie bei Block **110** angegeben ist. Als nächstes wird ein kryptographischer Hash des strukturierten digitalen Zertifikats **30** berechnet, wie bei Block **112** angegeben ist. Der kryptographische Hash kann anhand vieler verschiedener Verfahren berechnet werden. Bei einem Ausführungsbeispiel wird der kryptographische Hash anhand von SHA-1 berechnet. Bei Block **114** wird die Digitales-Zertifikat-Signatur mit dem berechneten kryptographischen Hash des digitalen Zertifikats und einem privaten Schlüssel der Zertifikat-Befugnisstelle berechnet.

**[0051]** Fig. 3B ist ein Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens **115** zum Schließen eines kryptographischen Ordners X veranschaulicht. Wie bei Block **116** angegeben ist, werden alle verschachtelten Ordner in dem Ordner X rekursiv geschlossen. Wie bei Block **117** angegeben ist, wird ein kryptographischer Hash aus dem Inhalt des Ordners X, einschließlich aller rekursiv geschlossenen verschachtelten Ordner in dem Ordner X, berechnet. Wie bei Block **118** angegeben ist, wird der Inhalt des Ordners X durch den berechneten kryptographischen

Hash des Inhalts des Ordners X ersetzt. Wie bei Block **119** angegeben ist, wird ein Flag in dem Anfangsblock des Ordners X gesetzt, um anzugeben, dass der Ordner X geschlossen ist.

**[0052]** Fig. 4 ist ein Block- und Datenflussdiagramm, das eine Operation **118** veranschaulicht, bei der eine Signatur für das strukturierte digitale Zertifikat **30** bei der Zertifikat-Befugnisstelle erzeugt wird. Wie bei Block **110** der Fig. 3A angegeben ist, müssen alle kryptographischen Ordner in dem strukturierten digitalen Zertifikat **30** geschlossen werden, bevor eine Signatur erzeugt werden kann. Bei der Operation **118** wird der Autorisierungsinformationsinhalt eines offenen kryptographischen Ordners **52** (d. h. des in der Hierarchie kryptographischer Ordner auf der niedrigsten Ebene befindlichen kryptographischen Ordners) durch einen kryptographischen Hashwert ersetzt, und der kryptographische Ordner **52** wird geschlossen, wie bei **120** in Fig. 4 angegeben ist. Als nächstes wird der Autorisierungsinformationsinhalt der offenen kryptographischen Ordner **46** und **48** durch entsprechende kryptographische Hashwerte ersetzt, und die kryptographischen Ordner **46** und **48** werden geschlossen, wie bei **122** angegeben ist. Der Autorisierungsinformationsinhalt der offenen, auf höchster Ebene befindlichen kryptographischen Ordner **38**, **40**, **42** und **44** in dem strukturierten digitalen Zertifikat **30** wird anschließend durch entsprechende kryptographische Hashwerte ersetzt, und die kryptographischen Ordner **38**, **40**, **42** und **44** werden geschlossen, wie bei **124** angegeben ist. An diesem Punkt wurde die Hierarchie der kryptographischen Ordner in dem strukturierten digitalen Zertifikat **30** „abgeflacht", so dass eine Signatur für das strukturierte digitale Zertifikat **30** erzeugt werden kann, wie bei **126** angegeben ist.

**[0053]** Fig. 5 ist ein Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens **104** zum Liefern eines strukturierten digitalen Zertifikats **30** an einen Empfänger des digitalen Zertifikats veranschaulicht. Das Verfahren **104** beginnt, indem die Digitales-Zertifikat-Signatur von der Zertifikat-Befugnisstelle (d. h. dem Aussteller) an das Subjekt des digitalen Zertifikats gesendet wird, wie bei Block **130** angegeben ist. Bei Block **132** wird eine Kopie des unsignierten digitalen Zertifikats von der Zertifikat-Befugnisstelle an das Subjekte des digitalen Zertifikats gesendet. Das Subjekt des digitalen Zertifikats schließt dann jegliche kryptographischen Ordner in der Kopie des unsignierten digitalen Zertifikats, die der Empfänger nicht sehen muss (d. h. Ordner, die keine für den Nachrichtenempfänger relevanten Autorisierungsinformationen enthalten), wie bei Block **134** angegeben ist. Schließlich werden die Kopie des unsignierten digitalen Zertifikats und die durch die Zertifikat-Befugnisstelle erzeugte Digitales-Zertifikat-Signatur von dem Subjekt des digitalen Zertifikats an den Empfänger des digitalen Zertifikats gesendet, wie bei Block **136** angegeben ist.

**[0054]** Fig. 6 ist ein Block- und Datenflussdiagramm, das eine Operation **150** veranschaulicht, bei der ein durch eine Zertifikat-Befugnisstelle signiertes strukturiertes digitales Zertifikat über das Subjekt des Zertifikats an einen Empfänger geliefert wird. Wie zuvor beschrieben wurde, schließt die Zertifikat-Befugnisstelle **152** alle kryptographischen Ordner in dem strukturierten digitalen Zertifikat **30**, bevor sie das strukturierte digitale Zertifikat **30** signiert. Nachdem das strukturierte digitale Zertifikat signiert wurde, wird die Digitales-Zertifikat-Signatur **126** an ein Subjekt **154** des digitalen Zertifikats geliefert. Zusätzlich zu der Digitales-Zertifikat-Signatur **126** liefert die Zertifikat-Befugnisstelle **152** auch eine Kopie des strukturierten digitalen Zertifikats **158**, bei der alle kryptographischen Ordner offen sind, an das Subjekt **154** des digitalen Zertifikats. Wenn die Kopie des strukturierten digitalen Zertifikats **158** sensible Informationen enthält, wird es notwendig, einem Zustellungskanal **159** zwischen der Zertifikat-Befugnisstelle **152** und dem Subjekt **154** des Zertifikats Sicherheit zu verleihen. Bei einem Ausführungsbeispiel wird der Zustellungskanal **159** durch Internet Protocol Security (IPSEC) gesichert. Bei einem alternativen Ausführungsbeispiel wird der Zustellungskanal **159** mittels Secure Sockets Layer (SSL) gesichert.

**[0055]** Das Subjekt **154** des digitalen Zertifikats leitet die Digitales-Zertifikat-Signatur **126** an den Empfänger **156** weiter. Bevor dem Empfänger **156** die Kopie des strukturierten digitalen Zertifikats **158** unterbreitet wird, schließt das Subjekt **154** des digitalen Zertifikats jegliche kryptographischen Ordner, die der Empfänger **156** nicht sehen muss, wie bei **160** angegeben ist.

**[0056]** Fig. 7 ist ein Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens **106** zum Verifizieren der Authentizität einer Signatur eines strukturierten digitalen Zertifikats **30** veranschaulicht. Bei dem Verfahren **106** erhält der Empfänger **156** einen öffentlichen Schlüssel der Zertifikat-Befugnisstelle **152**, der einem privaten Schlüssel entspricht, der durch die Zertifikat-Befugnisstelle verwendet wird, um das digitale Zertifikat zu signieren, und der durch die Zertifikat-Befugnisstelle **152** ohne Weiteres zur Verfügung gestellt wird, wie bei Block **178** angegeben ist. Das Verfahren **106** schließt jegliche kryptographischen Ordner, die in der Kopie des strukturierten digitalen Zertifikats durch das Subjekt **154** des digitalen Zertifikats offen gelassen wurden, wie bei Block **180** angegeben ist. Wie bei Block **182** angegeben ist, berechnet der Empfänger **156** einen kryptographischen Hash des strukturierten digitalen Zertifikats **158**, wobei alle Ordner geschlossen sind. Wie bei Block **184** angegeben ist, verifiziert der Empfänger **156** die Signatur für das digitale Zertifikat mit dem öffentlichen Schlüssel und dem berechneten kryptographischen

Hash des digitalen Zertifikats.

**[0057]** Fig. 8 ist ein Block- und Datenflussdiagramm, das eine Operation **210** veranschaulicht, bei der ein Nachrichtenempfänger die Authentizität eines strukturierten digitalen Zertifikats verifiziert. Bei der Operation **210** erhält der Empfänger **156** einen öffentlichen Schlüssel **214** der Zertifikat-Befugnisstelle **152**, wie bei **178** angegeben ist. Bevor er das signierte digitale Zertifikat **126** verifiziert, schließt der Empfänger **156** alle kryptographischen Ordner, die seitens des Subjekts **154** des Zertifikats **154** bei der Kopie des digitalen Zertifikats **160** offengelassen wurden, wie bei Block **180** angegeben ist. Wie bei Block **182** angegeben ist, berechnet der Empfänger **156** einen kryptographischen Hash **216** des digitalen Zertifikats **212**, wobei alle kryptographischen Ordner geschlossen sind. Wie bei Block **184** angegeben ist, verifiziert der Empfänger **156** die Signatur des digitalen Zertifikats **126** mit dem öffentlichen Schlüssel **214** und dem berechneten kryptographischen Hash **216** des digitalen Zertifikats.

**[0058]** Fig. 9 veranschaulicht ein Ausführungsbeispiel eines Computersystems **250** und eines externen computerlesbaren Mediums **252**, das verwendet werden kann, um bei digitalen Zertifikaten bei einer Zertifikat-Befugnisstelle eine Feldvertraulichkeit zu liefern, um ein Verfahren eines Signierens eines digitalen Zertifikats zu beinhalten; bei einem Subjekt des digitalen Zertifikats, um ein Verfahren zum Liefern des digitalen Zertifikats von dem Subjekt an einen Empfänger des digitalen Zertifikats zu beinhalten; oder bei dem Empfänger des digitalen Zertifikats, um ein Verfahren zum Verifizieren einer Signatur für das digitale Zertifikat zu beinhalten. Ausführungsbeispiele des externen computerlesbaren Mediums **252** umfassen folgende, sind aber nicht auf diese beschränkt: einen CD-ROM, eine Floppy-Disk und eine Plattenkassette. Jedes der obigen Verfahren zum Bereitstellen einer Feldvertraulichkeit bei digitalen Zertifikaten kann in einer Vielzahl von kompilierten und interpretierten Computersprachen implementiert werden. Das externe computerlesbare Medium **252** speichert Quellcode, Objektcode, Maschinencode, Bedienoberflächenskripte und/oder DLL (dynamic link libraries) für jegliches der obigen Verfahren zum Bereitstellen einer Feldvertraulichkeit bei digitalen Zertifikaten. Eine Eingabevorrichtung **254** liest das externe computerlesbare Medium **252** und liefert diese Daten an das Computersystem **250**. Ausführungsbeispiele der Eingabevorrichtung **254** umfassen folgende, sind aber nicht auf diese beschränkt: eine CD-ROM-Lesevorichtung, ein Floppy-Diskettenlaufwerk und eine Datenkassettenlesevorrichtung.

**[0059]** Das Computersystem **250** umfasst eine Zentralverarbeitungseinheit **256** zum Ausführen eines jeglichen der obigen Verfahren zum Bereitstellen einer Feldvertraulichkeit bei digitalen Zertifikaten. Ferner umfasst das Computersystem **250** einen lokalen Plattenspeicher **262** zum lokalen Speichern eines Beliebigen der obigen Verfahren zum Bereitstellen einer Feldvertraulichkeit bei digitalen Zertifikaten vor, während und nach der Ausführung. Jegliches der obigen Verfahren zum Bereitstellen einer Feldvertraulichkeit bei digitalen Zertifikaten verwendet während der Ausführung ferner einen Speicher **260** in dem Computersystem. Nach einer Ausführung eines der obigen Verfahren zum Bereitstellen einer Feldvertraulichkeit bei digitalen Zertifikaten werden Ausgabedaten erzeugt und an eine Ausgabevorrichtung **258** geleitet. Ausführungsbeispiele der Ausgabevorrichtung **258** umfassen folgende, sind aber nicht auf diese beschränkt: eine Computeranzeigevorrichtung, einen Drucker und/oder eine Plattenspeichervorrichtung.

**[0060]** Es ist ein Verfahren vorgesehen, mittels dessen das Subjekt (d. h. der Absender) eines digitalen Zertifikats bestimmte Felder in dem digitalen Zertifikat vertraulich halten kann, während der Absender das digitale Zertifikat einem sich Verlassenden (d. h. dem Empfänger) präsentiert. Diese spezifische Feldvertraulichkeit wird durch ein strukturiertes digitales Zertifikat bewerkstelligt, das eine hierarchische Struktur kryptographischer Ordner umfasst. Zusätzlich dazu, dass sie eine Feldvertraulichkeit liefern, können die beschriebenen Ausführungsbeispiele die Geschwindigkeit der Signaturverifizierung durch den Empfangenden verbessern, den Netzwerkverkehr reduzieren und den rechnerischen Mehraufwand verringern.

## Patentansprüche

1. Ein System zum Befähigen mehrerer Empfänger eines strukturierten digitalen Zertifikats, ein Subjekt des digitalen Zertifikats zu autorisieren, wobei das System folgende Merkmale aufweist:
ein strukturiertes digitales Zertifikat (**30**), das ein Feld, eines ersten Typs, von Autorisierungsinformationen (**37**), die für einen ersten Empfänger relevant sind, ein Feld, eines zweiten Typs, von Autorisierungsinformationen (**50**), die für einen zweiten Empfänger relevant sind, einen ersten kryptographischen Ordner (**42**), der das Feld, des zweiten Typs, von Autorisierungsinformationen (**50**) enthält, und einen zweiten kryptographischen Ordner (**38**–**44**), der das Feld, des ersten Typs, von Autorisierungsinformationen enthält, aufweist, wobei die Felder, des ersten und des zweiten Typs, von Autorisierungsinformationen jeweils lesbar sind, wenn sich der jeweilige kryptographische Ordner, der das jeweilige Feld von Informationen enthält, in einem offenen Zustand befindet, jedoch nicht lesbar sind, wenn sich der jeweilige kryptographische Ordner in einem geschlossenen Zustand befindet;
eine Einrichtung zum Schließen eines kryptographischen Ordners, die eine Einrichtung zum Ersetzen

seines Inhalts durch den berechneten kryptographischen Hash seines Inhalts umfasst; und
**dadurch gekennzeichnet**, dass es eine digitale Signatur einer Drittpartei-Zertifikat-Befugnisstelle aufweist, die das strukturierte digitale Zertifikat ausstellt, wobei die digitale Signatur das digitale Zertifikat ungeachtet des Zustands des ersten und des zweiten kryptographischen Ordners zertifiziert.

2. Ein System gemäß Anspruch 1, bei dem das digitale Zertifikat ferner eines bzw. einen oder mehrere der folgenden umfasst:
eine Mehrzahl verschachtelter Felder und/oder Ordner in einem oder beiden des ersten oder zweiten kryptographischen Ordners (**46**–**54**); einen Subjektnamen; und/oder
einen dem Subjekt zugeordneten öffentlichen Schlüssel.

3. Ein Verfahren zum Bereitstellen einer Vertraulichkeit von Autorisierungsinformationen in einem digitalen Zertifikat (**30**), das von mehreren Empfängern gemeinsam verwendet wird, wobei das Verfahren folgende Schritte umfasst:
Bereitstellen eines digitalen Zertifikats, das zumindest ein Feld, eines ersten Typs, von Autorisierungsinformationen (**36**), die für einen ersten Empfänger relevant sind, und zumindest ein Feld, eines zweiten Typs, von Autorisierungsinformationen (**38**–**54**), die für einen zweiten Empfänger relevant sind, umfasst;
Bereitstellen eines ersten kryptographischen Ordners (**42**) in dem digitalen Zertifikat, wobei der erste kryptographische Ordner das zumindest eine Feld, des zweiten Typs, von Autorisierungsinformationen (**46**–**54**), die für den zweiten Empfänger relevant sind, enthält, wobei das zumindest eine Feld des zweiten Typs lesbar ist, wenn sich der erste kryptographische Ordner in einem offenen Zustand befindet, jedoch nicht lesbar ist, wenn sich der erste kryptographische Ordner in einem geschlossenen Zustand befindet;
Bereitstellen eines zweiten kryptographischen Ordners (**38**–**44**) in dem digitalen Zertifikat, wobei der zweite kryptographische Ordner das zumindest eine Feld, des ersten Typs, von Autorisierungsinformationen (**36**), die für den ersten Empfänger relevant sind, enthält, wobei das zumindest eine Feld des ersten Typs lesbar ist, wenn sich der zweite kryptographische Ordner in einem offenen Zustand befindet, jedoch nicht lesbar ist, wenn sich der zweite kryptographische Ordner in einem geschlossenen Zustand befindet;
Erstellen des digitalen Zertifikats bei einer Drittpartei-Zertifikat-Befugnisstelle;
Erzeugen einer digitalen Signatur auf der Basis eines berechneten kryptographischen Hash des digitalen Zertifikats;
Senden der digitalen Signatur und des digitalen Zertifikats an ein Subjekt, wobei der erste und der zweite kryptographische Ordner offen sind;
Schließen des ersten kryptographischen Ordners bei dem Subjekt, wodurch ein Lesezugriff auf das zumindest eine Feld, des zweiten Typs, des digitalen Zertifikats verhindert wird;
Liefern der digitalen Signatur und des digitalen Zertifikats, das den geschlossenen ersten kryptographische Ordner aufweist, von dem Subjekt an den ersten Empfänger, wobei das zumindest eine Feld, des ersten Typs, von Autorisierungsinformationen (**37**) für den ersten Empfänger lesbar ist und das zumindest eine Feld, des zweiten Typs, von Autorisierungsinformationen (**36**) für den ersten Empfänger nicht lesbar ist;
Verifizieren der Authentizität des digitalen Zertifikats (**30**) durch den ersten Empfänger; und
wobei der Schritt des Schließens eines kryptographischen Ordners X den Schritt des Ersetzens des Inhalts des Ordners X durch den berechneten kryptographischen Hash des Inhalts des Ordners X umfasst.

4. Ein Verfahren gemäß Anspruch 3, bei dem der Schritt des Verifizierens der Authentizität des digitalen Zertifikats ein Erhalten eines öffentlichen Schlüssels von der Drittpartei-Zertifikat-Befugnisstelle, ein Schließen jeglicher offener kryptographischer Ordner in dem empfangenen digitalen Zertifikat, ein Berechnen eines kryptographischen Hashs des empfangenen digitalen Zertifikats, wobei alle Ordner geschlossen sind, und ein Verifizieren der digitalen Signatur des digitalen Zertifikats mit dem öffentlichen Schlüssel und dem berechneten kryptographischen Hash des empfangenen digitalen Zertifikats umfasst.

5. Ein Verfahren zum Signieren des digitalen Zertifikats gemäß Anspruch 1 oder 2, das folgende Schritte umfasst:
Schließen aller kryptographischen Ordner in dem digitalen Zertifikat;
Berechnen eines kryptographischen Hash des digitalen Zertifikats; und
Berechnen einer digitalen Signatur mit dem berechneten kryptographischen Hash des digitalen Zertifikats und einem privaten Schlüssel der Drittpartei-Zertifikat-Befugnisstelle.

6. Ein Verfahren zum Liefern des digitalen Zertifikats gemäß Anspruch 1 oder 2 von einem Subjekt des digitalen Zertifikats an einen Empfänger des digitalen Zertifikats, wobei das Verfahren folgende Schritte umfasst:
Senden einer digitalen Signatur von der Drittpartei-Zertifikat-Befugnisstelle an das Subjekt des Zertifikats;
Senden des digitalen Zertifikats, bei dem alle kryptographischen Ordner offen sind, von der Zertifikat-Befugnisstelle an das Subjekt des Zertifikats;
Schließen eines oder mehrerer kryptographischer Ordner des digitalen Zertifikats, die keine für den Empfänger relevanten Autorisierungsinformationen aufweisen; und

Senden des digitalen Zertifikats, das einen oder mehrere geschlossene kryptographische Ordner und die digitale Signatur aufweist, von dem Subjekt des digitalen Zertifikats an den Empfänger.

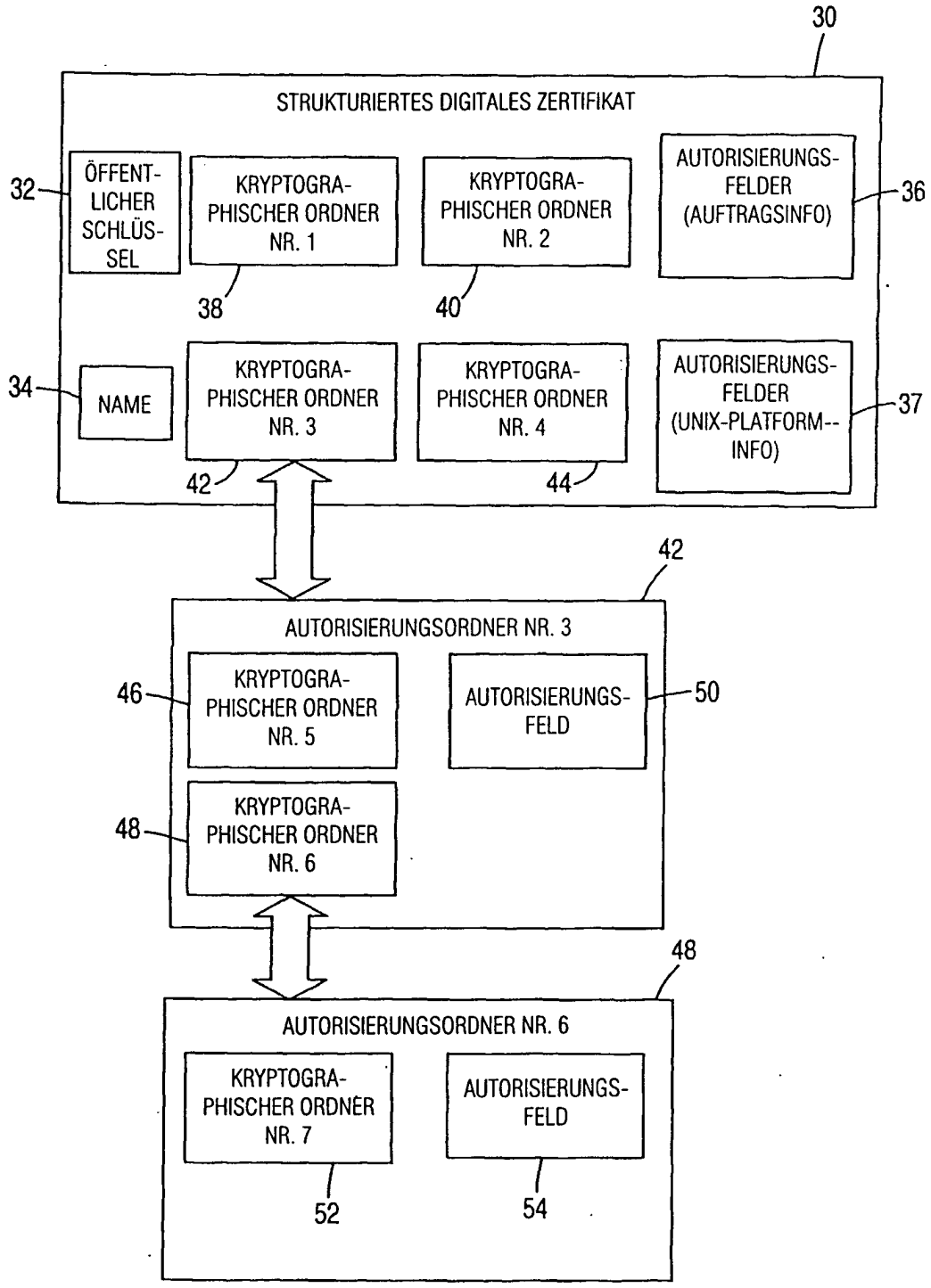
7. Ein Verfahren zum Verifizieren einer digitalen Signatur für das digitale Zertifikat gemäß Anspruch 1 oder 2, das an einen Empfänger des digitalen Zertifikats gesendet wurde, wobei das Verfahren folgende Schritte umfasst:
Erhalten eines öffentlichen Schlüssels der Drittpartei-Zertifikat-Befugnisstelle, der einem privaten Schlüssel entspricht, der durch die Zertifikat-Befugnisstelle verwendet wird, um die digitale Signatur zu erzeugen;
Schließen jeglicher offener kryptographischer Ordner in dem digitalen Zertifikat (**30**);
Berechnen eines kryptographischen Hash des digitalen Zertifikats, wobei alle kryptographischen Ordner geschlossen sind; und
Verifizieren der digitalen Signatur für das digitale Zertifikat mit dem öffentlichen Schlüssel und dem berechneten kryptographischen Hash des digitalen Zertifikats.

8. Das Verfahren gemäß einem der Ansprüche 3 bis 7, bei dem der Schritt des Schließens eines kryptographischen Ordners X folgende Schritte umfasst:
rekursives Schließen aller verschachtelten Ordner in dem Ordner X;
Berechnen des kryptographischen Hash des Inhalts des Ordners X;
Ersetzen des Inhalts des Ordners X durch den berechneten kryptographischen Hash des Inhalts des Ordners X; und
Angeben, in dem digitalen Zertifikat, dass der Ordner X geschlossen ist.

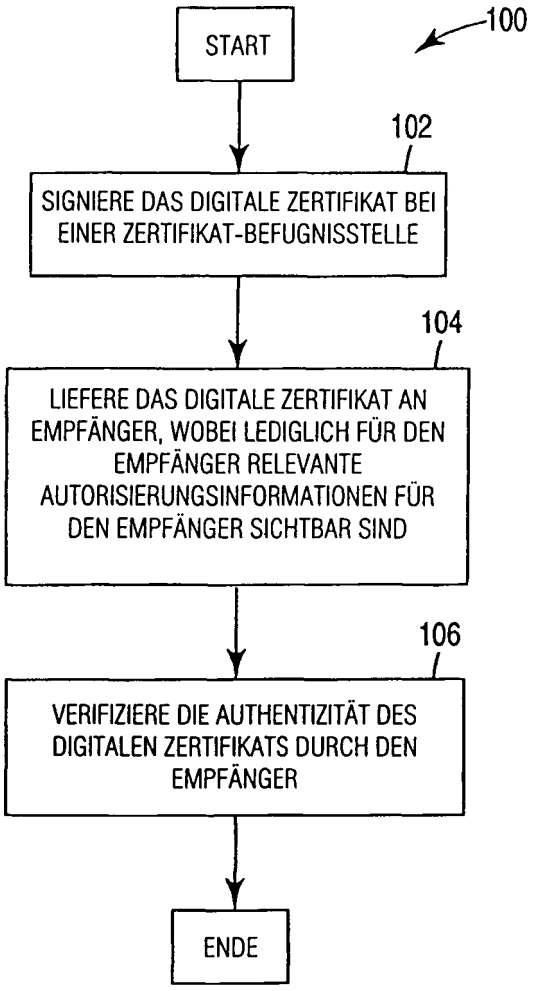
Es folgen 10 Blatt Zeichnungen

**Anhängende Zeichnungen**

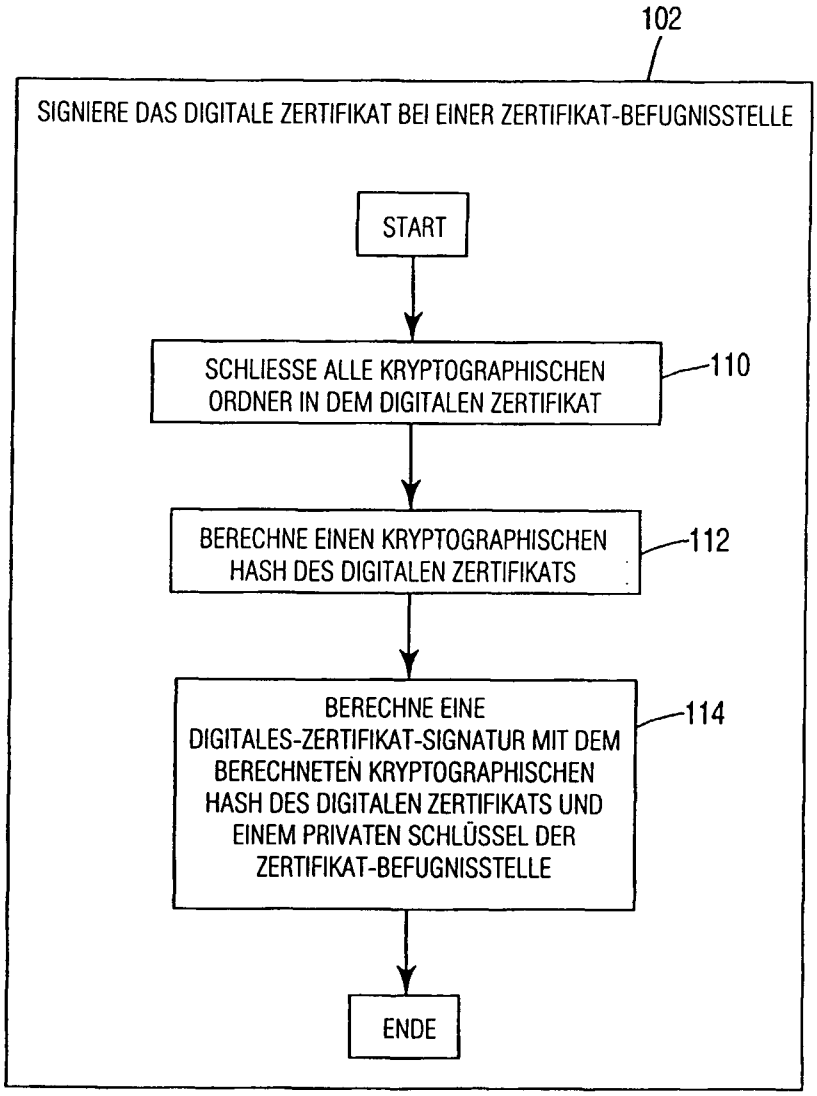
Europäisches Aktenzeichen: 00310771.1



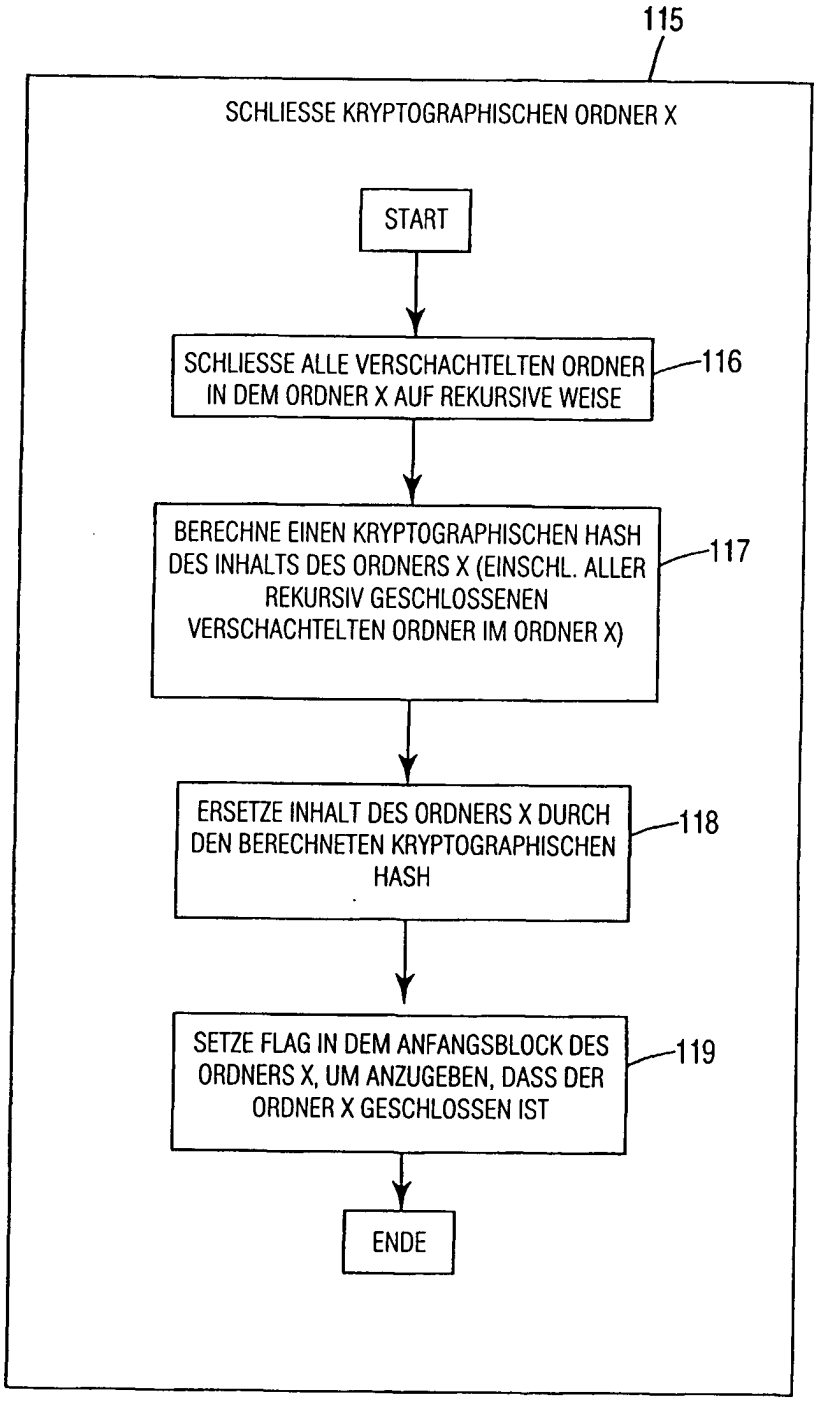

FIGUR 1


100
START
102
SIGNIERE DAS DIGITALE ZERTIFIKAT BEI EINER ZERTIFIKAT-BEFUGNISSTELLE
104
LIEFERE DAS DIGITALE ZERTIFIKAT AN EMPFÄNGER, WOBEI LEDIGLICH FÜR DEN EMPFÄNGER RELEVANTE AUTORISIERUNGSINFORMATIONEN FÜR DEN EMPFÄNGER SICHTBAR SIND
106
VERIFIZIERE DIE AUTHENTIZITÄT DES DIGITALEN ZERTIFIKATS DURCH DEN EMPFÄNGER
ENDE

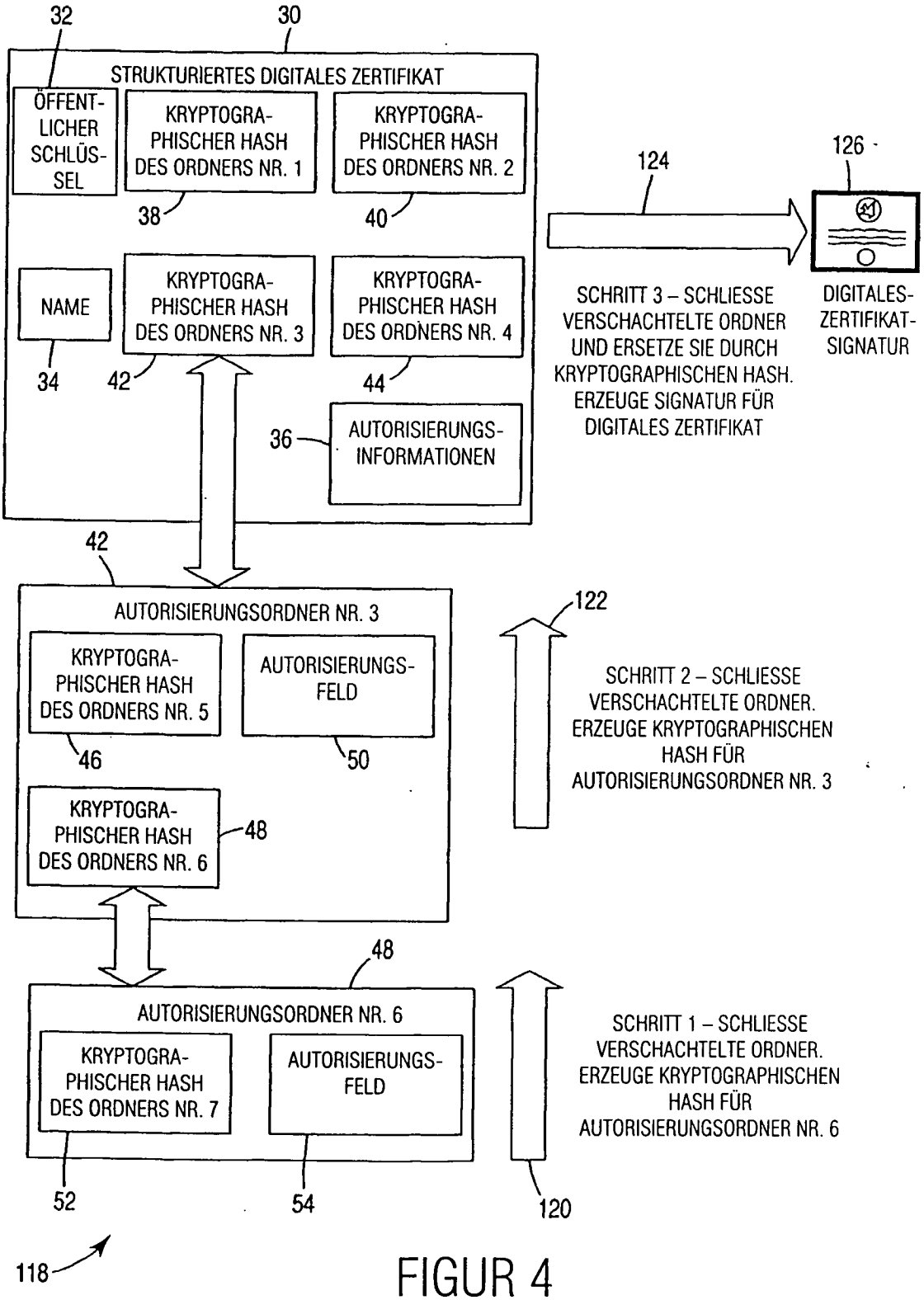
FIGUR 2


102
SIGNIERE DAS DIGITALE ZERTIFIKAT BEI EINER ZERTIFIKAT-BEFUGNISSTELLE
START
SCHLIESSE ALLE KRYPTOGRAPHISCHEN ORDNER IN DEM DIGITALEN ZERTIFIKAT
110
BERECHNE EINEN KRYPTOGRAPHISCHEN HASH DES DIGITALEN ZERTIFIKATS
112
BERECHNE EINE DIGITALES-ZERTIFIKAT-SIGNATUR MIT DEM BERECHNETEN KRYPTOGRAPHISCHEN HASH DES DIGITALEN ZERTIFIKATS UND EINEM PRIVATEN SCHLÜSSEL DER ZERTIFIKAT-BEFUGNISSTELLE
114
ENDE

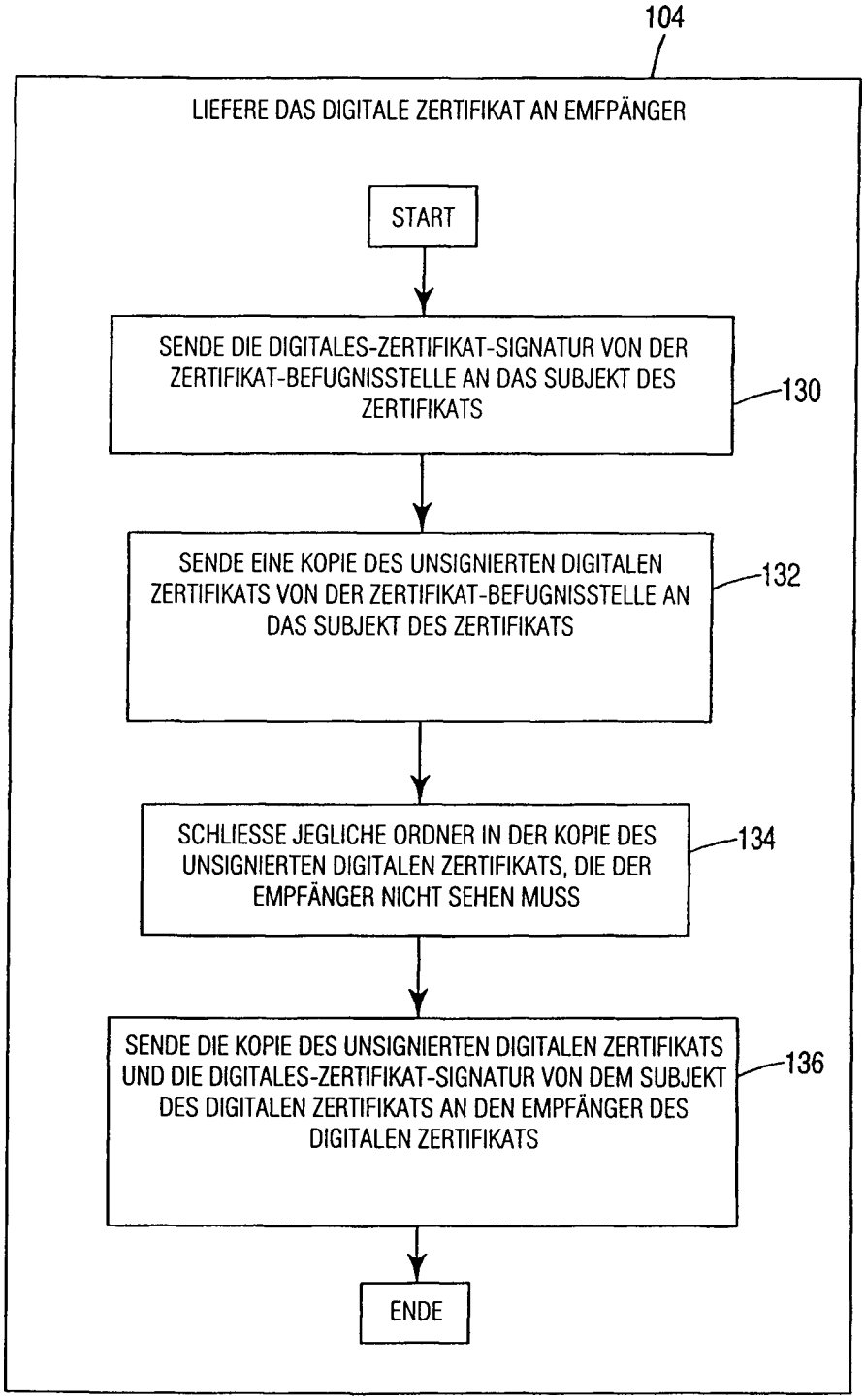
FIGUR 3A


115
SCHLIESSE KRYPTOGRAPHISCHEN ORDNER X
START
SCHLIESSE ALLE VERSCHACHTELTEN ORDNER IN DEM ORDNER X AUF REKURSIVE WEISE
116
BERECHNE EINEN KRYPTOGRAPHISCHEN HASH DES INHALTS DES ORDNERS X (EINSCHL. ALLER REKURSIV GESCHLOSSENEN VERSCHACHTELTEN ORDNER IM ORDNER X)
117
ERSETZE INHALT DES ORDNERS X DURCH DEN BERECHNETEN KRYPTOGRAPHISCHEN HASH
118
SETZE FLAG IN DEM ANFANGSBLOCK DES ORDNERS X, UM ANZUGEBEN, DASS DER ORDNER X GESCHLOSSEN IST
119
ENDE

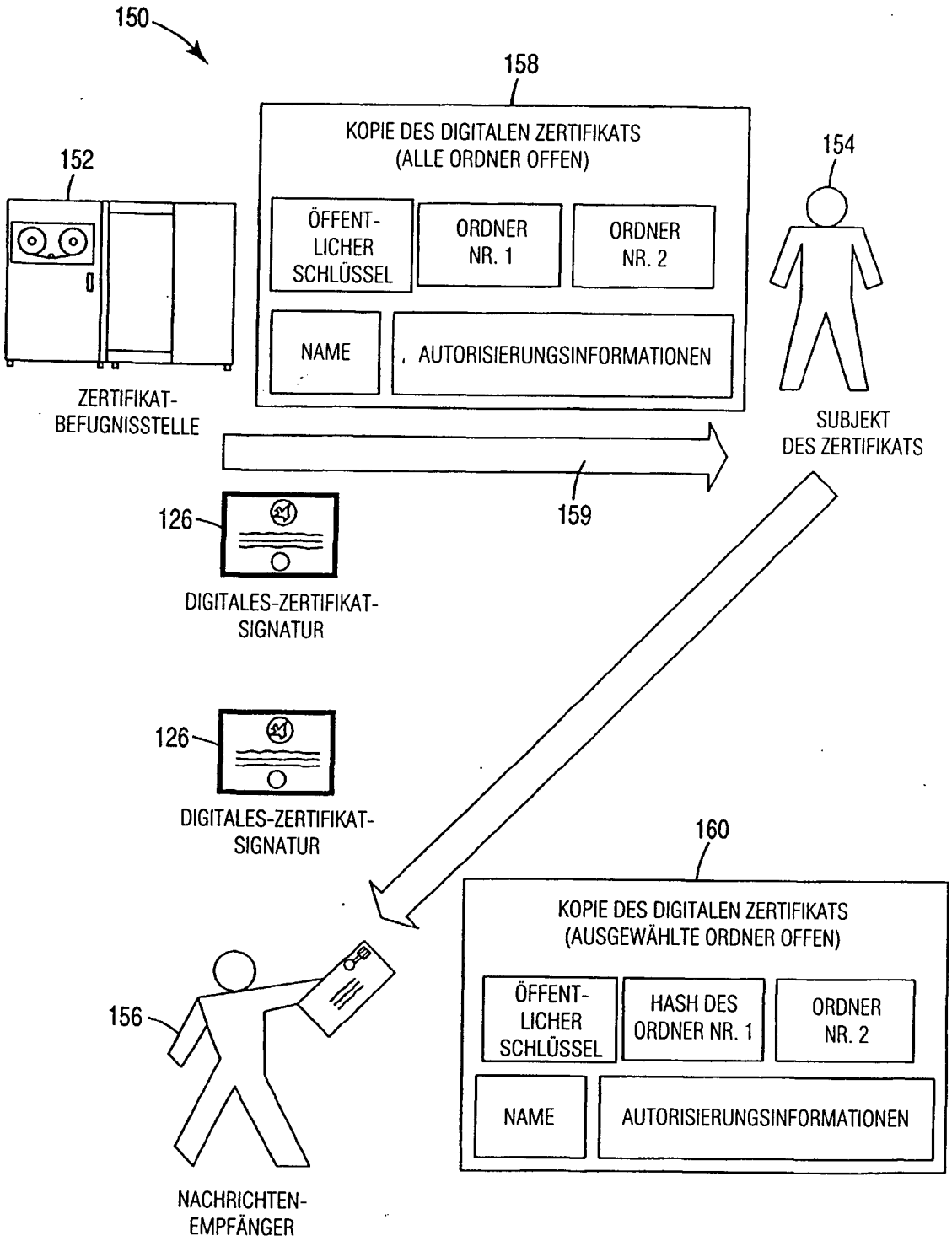
FIGUR 3B


32
30
STRUKTURIERTES DIGITALES ZERTIFIKAT
ÖFFENT-LICHER SCHLÜS-SEL
KRYPTOGRA-PHISCHER HASH DES ORDNERS NR. 1
KRYPTOGRA-PHISCHER HASH DES ORDNERS NR. 2
38
40
124
126
NAME
KRYPTOGRA-PHISCHER HASH DES ORDNERS NR. 3
KRYPTOGRA-PHISCHER HASH DES ORDNERS NR. 4
34
42
44
SCHRITT 3 – SCHLIESSE VERSCHACHTELTE ORDNER UND ERSETZE SIE DURCH KRYPTOGRAPHISCHEN HASH. ERZEUGE SIGNATUR FÜR DIGITALES ZERTIFIKAT
DIGITALES-ZERTIFIKAT-SIGNATUR
36
AUTORISIERUNGS-INFORMATIONEN
42
AUTORISIERUNGSORDNER NR. 3
122
KRYPTOGRA-PHISCHER HASH DES ORDNERS NR. 5
AUTORISIERUNGS-FELD
46
50
SCHRITT 2 – SCHLIESSE VERSCHACHTELTE ORDNER. ERZEUGE KRYPTOGRAPHISCHEN HASH FÜR AUTORISIERUNGSORDNER NR. 3
KRYPTOGRA-PHISCHER HASH DES ORDNERS NR. 6
48
48
AUTORISIERUNGSORDNER NR. 6
KRYPTOGRA-PHISCHER HASH DES ORDNERS NR. 7
AUTORISIERUNGS-FELD
52
54
120
SCHRITT 1 – SCHLIESSE VERSCHACHTELTE ORDNER. ERZEUGE KRYPTOGRAPHISCHEN HASH FÜR AUTORISIERUNGSORDNER NR. 6
118

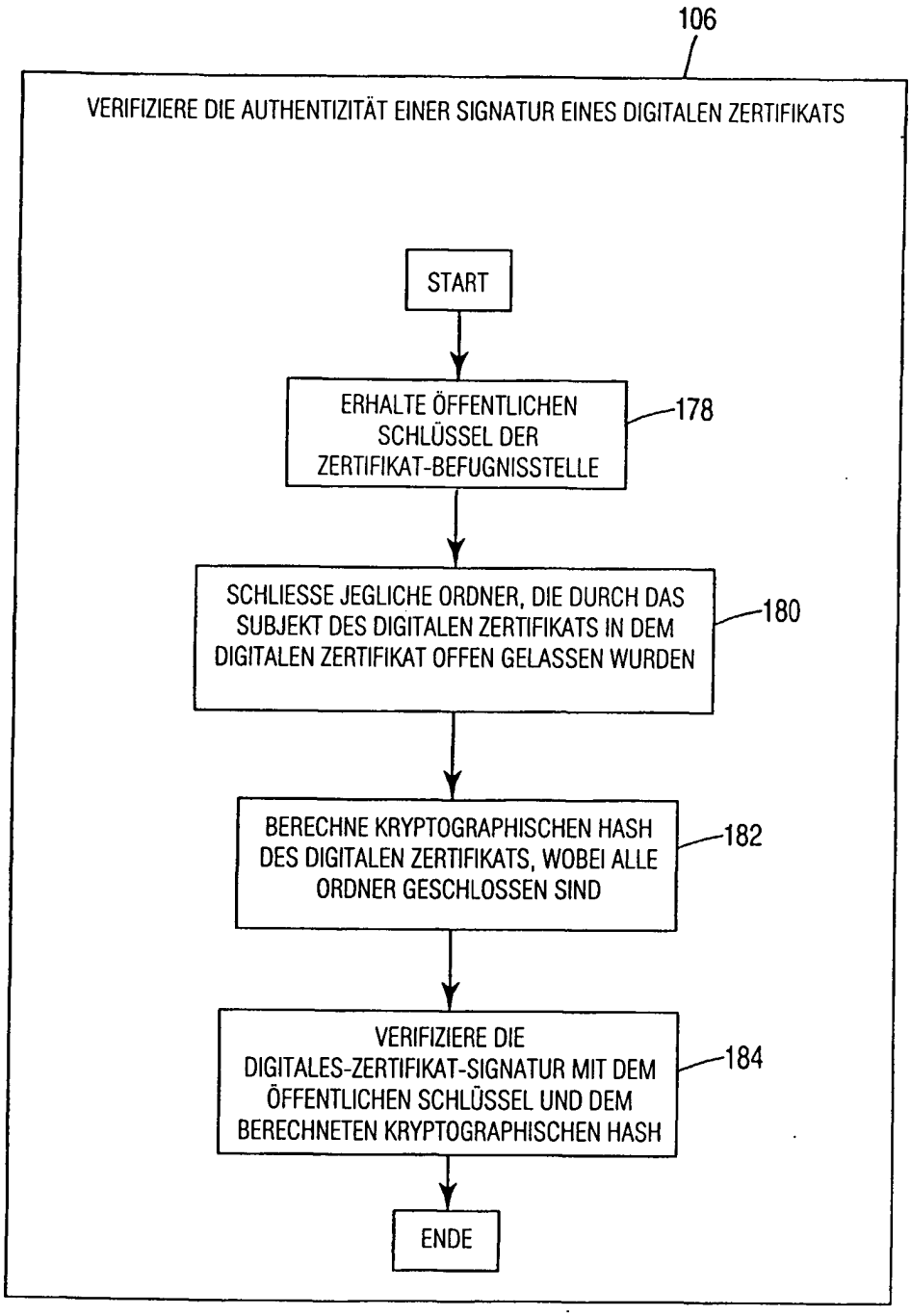
FIGUR 4


104
LIEFERE DAS DIGITALE ZERTIFIKAT AN EMFPÄNGER
START
SENDE DIE DIGITALES-ZERTIFIKAT-SIGNATUR VON DER ZERTIFIKAT-BEFUGNISSTELLE AN DAS SUBJEKT DES ZERTIFIKATS
130
SENDE EINE KOPIE DES UNSIGNIERTEN DIGITALEN ZERTIFIKATS VON DER ZERTIFIKAT-BEFUGNISSTELLE AN DAS SUBJEKT DES ZERTIFIKATS
132
SCHLIESSE JEGLICHE ORDNER IN DER KOPIE DES UNSIGNIERTEN DIGITALEN ZERTIFIKATS, DIE DER EMPFÄNGER NICHT SEHEN MUSS
134
SENDE DIE KOPIE DES UNSIGNIERTEN DIGITALEN ZERTIFIKATS UND DIE DIGITALES-ZERTIFIKAT-SIGNATUR VON DEM SUBJEKT DES DIGITALEN ZERTIFIKATS AN DEN EMPFÄNGER DES DIGITALEN ZERTIFIKATS
136
ENDE

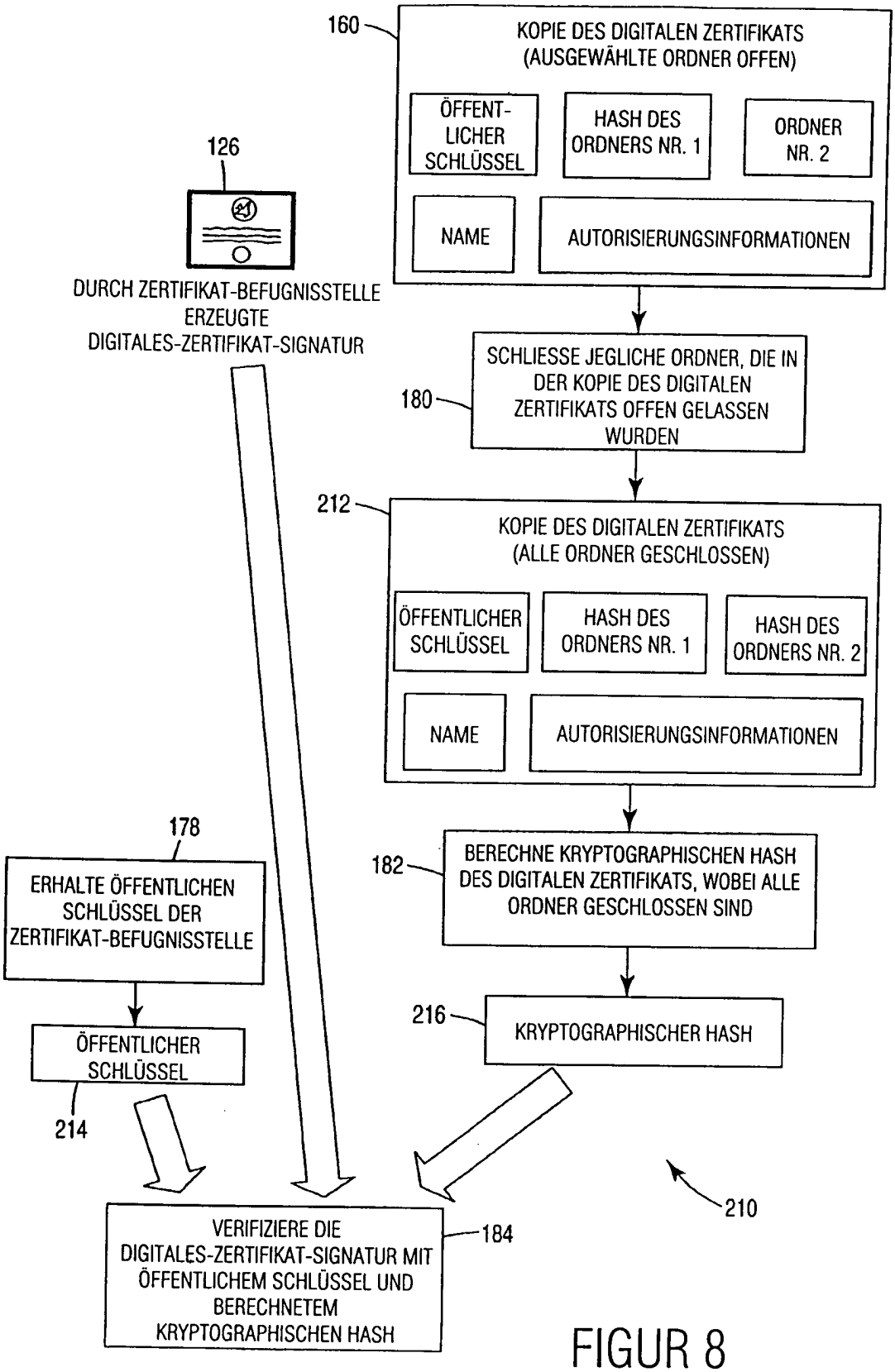
FIGUR 5


150
158
KOPIE DES DIGITALEN ZERTIFIKATS
(ALLE ORDNER OFFEN)
ÖFFENT-
LICHER
SCHLÜSSEL
ORDNER
NR. 1
ORDNER
NR. 2
NAME
AUTORISIERUNGSINFORMATIONEN
152
154
ZERTIFIKAT-
BEFUGNISSTELLE
SUBJEKT
DES ZERTIFIKATS
159
126
DIGITALES-ZERTIFIKAT-
SIGNATUR
126
DIGITALES-ZERTIFIKAT-
SIGNATUR
160
KOPIE DES DIGITALEN ZERTIFIKATS
(AUSGEWÄHLTE ORDNER OFFEN)
ÖFFENT-
LICHER
SCHLÜSSEL
HASH DES
ORDNER NR. 1
ORDNER
NR. 2
NAME
AUTORISIERUNGSINFORMATIONEN
156
NACHRICHTEN-
EMPFÄNGER

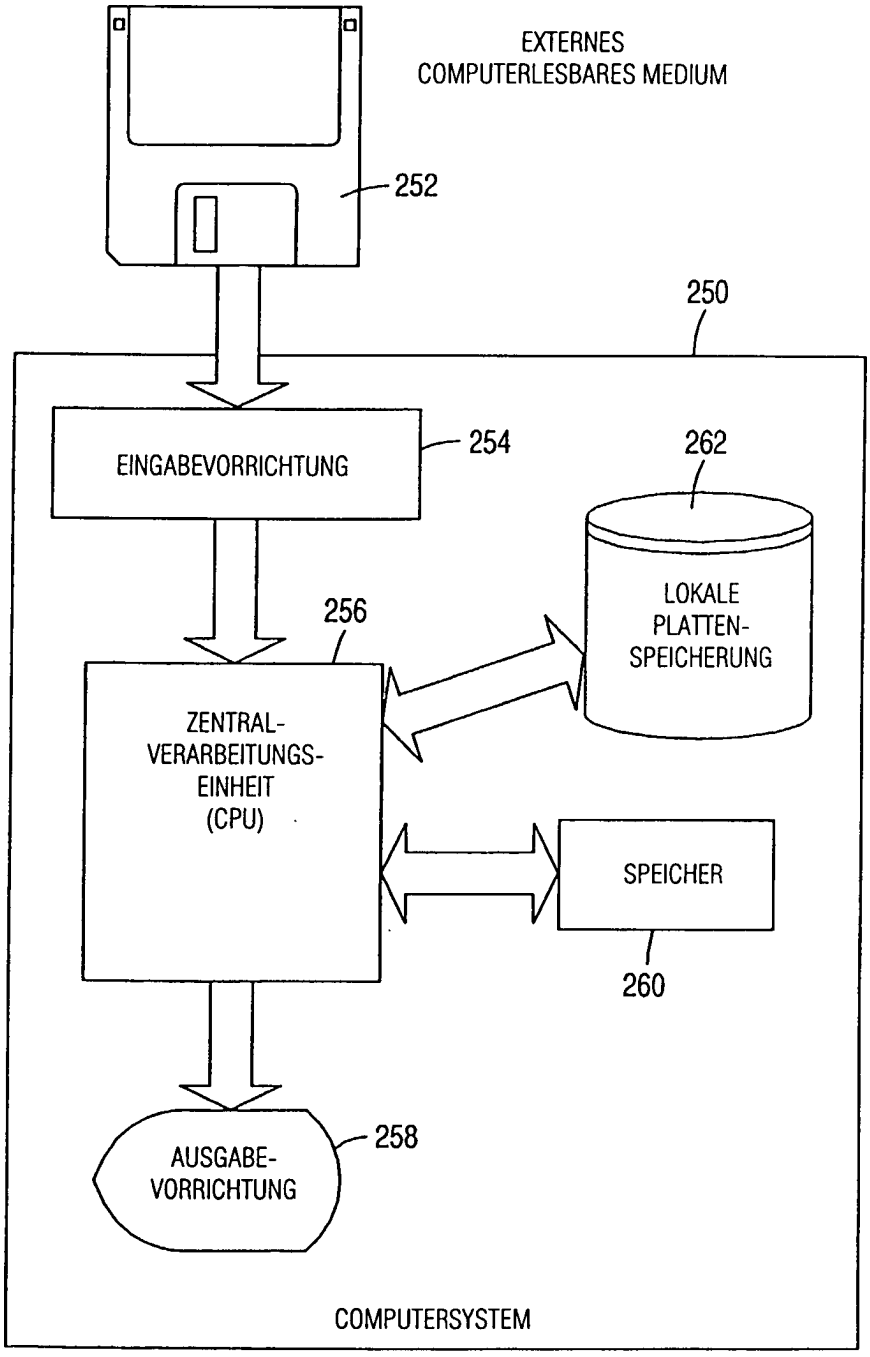
FIGUR 6


106
VERIFIZIERE DIE AUTHENTIZITÄT EINER SIGNATUR EINES DIGITALEN ZERTIFIKATS
START
ERHALTE ÖFFENTLICHEN SCHLÜSSEL DER ZERTIFIKAT-BEFUGNISSTELLE
178
SCHLIESSE JEGLICHE ORDNER, DIE DURCH DAS SUBJEKT DES DIGITALEN ZERTIFIKATS IN DEM DIGITALEN ZERTIFIKAT OFFEN GELASSEN WURDEN
180
BERECHNE KRYPTOGRAPHISCHEN HASH DES DIGITALEN ZERTIFIKATS, WOBEI ALLE ORDNER GESCHLOSSEN SIND
182
VERIFIZIERE DIE DIGITALES-ZERTIFIKAT-SIGNATUR MIT DEM ÖFFENTLICHEN SCHLÜSSEL UND DEM BERECHNETEN KRYPTOGRAPHISCHEN HASH
184
ENDE

FIGUR 7


160
KOPIE DES DIGITALEN ZERTIFIKATS
(AUSGEWÄHLTE ORDNER OFFEN)
ÖFFENT-
LICHER
SCHLÜSSEL
HASH DES
ORDNERS NR. 1
ORDNER
NR. 2
NAME
AUTORISIERUNGSINFORMATIONEN
126
DURCH ZERTIFIKAT-BEFUGNISSTELLE
ERZEUGTE
DIGITALES-ZERTIFIKAT-SIGNATUR
SCHLIESSE JEGLICHE ORDNER, DIE IN
DER KOPIE DES DIGITALEN
ZERTIFIKATS OFFEN GELASSEN
WURDEN
180
212
KOPIE DES DIGITALEN ZERTIFIKATS
(ALLE ORDNER GESCHLOSSEN)
ÖFFENTLICHER
SCHLÜSSEL
HASH DES
ORDNERS NR. 1
HASH DES
ORDNERS NR. 2
NAME
AUTORISIERUNGSINFORMATIONEN
178
ERHALTE ÖFFENTLICHEN
SCHLÜSSEL DER
ZERTIFIKAT-BEFUGNISSTELLE
182
BERECHNE KRYPTOGRAPHISCHEN HASH
DES DIGITALEN ZERTIFIKATS, WOBEI ALLE
ORDNER GESCHLOSSEN SIND
216
KRYPTOGRAPHISCHER HASH
ÖFFENTLICHER
SCHLÜSSEL
214
210
VERIFIZIERE DIE
DIGITALES-ZERTIFIKAT-SIGNATUR MIT
ÖFFENTLICHEM SCHLÜSSEL UND
BERECHNETEM
KRYPTOGRAPHISCHEN HASH
184

FIGUR 8


EXTERNES
COMPUTERLESBARES MEDIUM
252
250
EINGABEVORRICHTUNG
254
262
LOKALE
PLATTEN-
SPEICHERUNG
256
ZENTRAL-
VERARBEITUNGS-
EINHEIT
(CPU)
SPEICHER
260
AUSGABE-
VORRICHTUNG
258
COMPUTERSYSTEM

FIGUR 9