(19) Deutsches Patent- und Markenamt

(10) **DE 10 2009 031 817 A1** 2011.01.05

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2009 031 817.8**
(22) Anmeldetag: **03.07.2009**
(43) Offenlegungstag: **05.01.2011**

(51) Int Cl.[8]: ***H04L 9/30*** (2006.01)
H04L 9/32 (2006.01)

(71) Anmelder:
Charismathics GmbH, 80331 München, DE

(74) Vertreter:
Patentanwälte Eder & Schieschke, 80796 München

(72) Erfinder:
Gossel, Sven, 80634 München, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

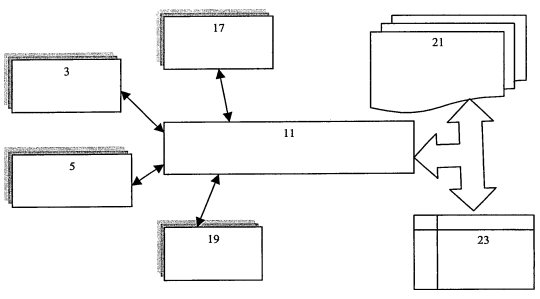
US 2009/01 72 776 A1
US 2003/00 28 470 A1
WO 2009/0 36 511 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Verfahren zur Ausstellung, Überprüfung und Verteilung von digitalen Zertifikaten für die Nutzung in Public-Key-Infrastrukturen**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Ausstellung, Überprüfung und Verteilung von digitalen Zertifikaten für die Nutzung in Public-Key-Infrastrukturen, bei dem ein Antragsteller 3, 5 bei einer digitalen Zertifizierungsstelle 11 ein digitales Zertifikat beantragt, wobei zur Bewertung eines Vertrauensstatus für das Zertifikat eines Zertifikatsinhabers (3) wenigstens eine Information 21 Dritter über den Zertifikatsinhaber 3 herangezogen wird. Weiterhin betrifft die Erfindung eine digitale Zertifizierungsstelle sowie eine Anordnung aus einer solchen und wenigstens einer hiermit über ein digitales Netzwerk verbundenen Teilnehmerstation eines Zertifikatsbenutzers 5 zur Durchführung eines derartigen Verfahrens.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Ausstellung, Überprüfung und Verteilung von digitalen Zertifikaten für die Nutzung in Public-Key-Infrastrukturen (PKI). Derartige Verfahren finden in der rechnergestützten Kommunikation in digitalen Netzen, insbesondere im Internet Verwendung, beispielsweise zum sicheren Aufruf von Webseiten, für die sichere Übertragung von Emails oder anderen Daten und zur sicheren Ausführung von entsprechenden Anwendungen oder Objekten.

[0002] Beispielsweise können mit Hilfe eines asymmetrischen Kryptosystems Nachrichten in einem Netzwerk bei geeigneter Wahl der Verschlüsselungsparameter, insbesondere der Schlüssellänge, derart digital signiert und verschlüsselt werden, dass auch bei Kenntnis des Verfahrens ein Missbrauch zumindest innerhalb einer angemessenen Zeit verhindert werden kann.

[0003] Zur Verschlüsselung einer Nachricht benötigt der Sender den Public-Key bzw. Schlüssel des Empfängers, welcher beispielsweise von einer Webseite heruntergeladen oder per Email versendet werden kann. Zur Authentifizierung dienen digitale Zertifikate, welche die Authentizität des öffentlichen Schlüssel, dessen zulässigen Anwendungs- und Geltungsbereich bestätigen.

[0004] Digitale Zertifikate zum Nachweis der Echtheit von Objekten im Allgemeinen werden von digitalen Zertifizierungsstellen, also einem entsprechenden Server (Rechner) bzw. darauf laufendem System ausgestellt.

[0005] Trotz der durch PKI-Systeme erreichbaren hohen Sicherheit gegen Missbrauch finden diese in der rechnergestützten Kommunikation leider keine große und schnelle Verbreitung.

[0006] Grund hierfür ist, dass sich Public-Keys sowohl im Falle hierarchischer PKI-Systeme (zum Beispiels der X.509 Standard) als auch im sogenannten Web of Trust-Ansatz (selbst bei regelmäßiger Teilnahme von Key-Signing-Parties) nicht einfach, schnell und komfortabel sowie ausreichend gesichert gegen Missbrauch verbreiten lassen.

[0007] Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zu schaffen, das eine schnelle und komfortable Ausbreitung einer Public-Key-Infrastruktur ermöglicht.

[0008] Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den Merkmalen des Anspruchs 1, sowie durch eine digitale Zertifizierungsstelle mit den Merkmalen des Anspruchs 9 und eine Anordnung aus einer derartigen digitalen Zertifizierungsstelle nach Anspruch 9 und wenigstens einer hiermit über ein digitales Netzwerk verbundenen Teilnehmerstation nach Anspruch 10 gelöst.

[0009] Nach der Erfindung werden Zertifikate in Form eines hierarchischen PKI-Systems zur Authentifizierung von Public-Keys, beispielsweise für den verschlüsselten Email-Versand, zur besseren Absicherung im Internet-shopping (e-Store), Anwendungen, welche zur Absicherung (Signatur, Verschlüsselung, o. ä.) Zertifikate benötigen, etc., einfacher von einer zentralen digitalen Zertifizierungsstelle ausgestellt und dennoch mit einer ausreichenden Vertrauensstufe bzw. Vertrauensstatus im digitalen Netzwerk verteilt, indem zur Bewertung eines Vertrauensstatus für das Zertifikat wenigstens eine Information Dritter über den Zertifikatsinhaber herangezogen wird. Dritte können (im Unterschied zu einem Zertifikatsinhaber und der Zertifizierungsstelle bei der das Zertifikat beantragt und ausgestellte werden soll) hierbei Zertifikatsbenutzer und/oder andere Personen oder Einrichtungen, wie beispielsweise andere digitale Zertifizierungsstellen, soziale Netzwerke, etc. bzw. die diesbezüglichen Server sein.

[0010] Als Informationen Dritter über den Zertifikatsinhaber allgemein oder dessen Zertifikat direkt kommen beispielsweise Zertifikate anderer Zertifizierungsstellen desselben Inhabers (identifiziert über seine Email-Adresse oder über andere Identitätsangaben, wie Name und Vorname, etc.) in Frage. Auch können sich Dritte bei der Zertifizierungsbehörde über Spar, welche vom Zertifikatsinhaber ausgesendet wurde, beschweren, so dass das entsprechende Zertifikat als ungültig eingestuft bzw. dessen Ausstellung abgelehnt wird. Zudem kann ein von Dritten bewertetes Verhalten bzw. ein von Dritten erlangter Vertrauensstatus des Zertifikatsinhabers in anderen Bereichen, wie beispielsweise bei Webauktionen, Diskussionsforen, etc. als Information zur Bewertung eines Vertrauensstatus von der Zertifizierungsstelle für das Zertifikat herangezogen werden. So ist es auch denkbar, als Information Dritter Informationen eines Telefonnetzbetreibers, wie die individuelle Telefonnummer, oder andere eindeutige Teilnehmerkennungen (wie beispielsweise im Mobilfunk neben der Telefonnummer die IMSI, CCID, oder gar die Gerätekennung IMEI im Falle limitierter Geräte, etc.) heranzuziehen, um einen in anderen Bereichen erlangten Vertrauensstatus darzulegen.

[0011] Derartige Informationen (Bestätigungen Dritter) können vom Zertifikatsinhaber selbst bei der Antragsstellung mitgeliefert werden oder nachträglich, möglicherweise auch auf Anfrage der Zertifizierungsstelle, übermittelt werden, um den Vertrauensstatus zu erhöhen. Auch ist es denkbar, dass die Zertifizierungsstelle zumindest mit übermittelter oder auf Anforderung erteilter Erlaubnis bei anderen digitalen webbasierten Zertifizierungsstellen (im digitalen

Netz) und/oder digitalen bzw. webbasierten sozialen Netzwerken (beispielsweise Facebook, LinkedIN, XING, MySpace, etc.) dort vorhandene Informationen (Historie, Rang, Beschwerden, Bestätigungen, etc.) über den Zertifikatsinhaber abruft.

[0012] Die Informationen können auch zur Bestätigung von nur Teilen der Identität (Attributen) des Zertifikatsinhabers, wie beispielsweise dessen Adresse, dienen.

[0013] Nach der Erfindung ist es auch denkbar, dass sich Dritte bei der Zertifizierungsstelle über Missbrauch eines Zertifikats oder Fehlverhalten des Zertifikatsinhabers nach Ausstellung beschweren oder ein konformes Verhalten bestätigen bzw. beglaubigen, so dass diese Informationen direkt zu einer neuen Bewertung und damit einer Aktualisierung der Vertrauensstufe des Zertifikats führen. Im Falle von Beschwerden ist es vorstellbar, dass zuerst ein Disput eröffnet wird, in welchem auch dem Zertifikatsinhaber als Beschwerdegegner eine Gelegenheit eingeräumt wird, zu den Beschwerden Stellung zu nehmen, bevor diese in eine (Neu-)Bewertung der Vertrauensstufe einfließen.

[0014] Bei der Bewertung der Informationen Dritter kann je nach Qualität der Information, Vertrauensstatus des Informierenden, etc. unterschieden werden, so dass sich eine hohe Wahrscheinlichkeit des Wahrheitsgehalts einer Information (Vertrauensstufe der Information) in Abhängigkeit einer entsprechenden von gleichlautenden Informationen unterschiedlicher Quellen oder von einer Information einer Quelle mit besonders hoher Vertrauensstufe einstellt. Selbstverständlich kann auch die Wichtigkeit einer Information bei der Bewertung des Vertrauensstatus des Zertifikats berücksichtigt werden, wobei es denkbar ist, unterschiedlichen bekannten Arten von Quellen Dritter und deren Informationen einen entsprechenden Rang zuzuordnen.

[0015] In bevorzugter Ausgestaltung der Erfindung führen die Information Dritter mittels eines geeigneten Bewertungs-Algorithmus zur Bewertung eines Rangs innerhalb einer Rangliste, wobei auch nach Ausstellung des Zertifikats eine Neubewertung anhand dieses Bewertungs-Algorithmus vorzugsweise möglich ist und damit ein aktueller Rang ermittelt wird.

[0016] Ein derartiger Rang wird nach der Erfindung vorzugsweise von der Zertifizierungsstelle auf Abfrage online für Zertifikats-Benutzer jederzeit oder in vorbestimmten Intervallen zur Verfügung gestellt oder aktiv an diese übermittelt. Hierbei ist es auch denkbar, dass insbesondere für Anwendungen, welche einen Rang einer Rangliste mit mehr als zwei Rängen nicht verwerten können, ein aktueller Rang in Abhängigkeit einer vorbestimmten Schwelle als bekannte Zertifikatsstatusinformation „Gültig" oder „Ungültig" umgesetzt wird.

[0017] Auch wenn ein Zertifikat für einen Schlüssel bzw. in der Regel für ein Schlüsselpaar (public und private key) meist vom Inhaber selbst bei der Zertifizierungsstelle beantragt wird, ist es nach der Erfindung auch möglich, dass das Zertifikat von einem Dritten für den Inhaber beantragt wird. In diesem Fall ist es denkbar, dass – falls erwünscht – eine Zustimmung des (zukünftigen) Zertifikatsinhabers von der Zertifizierungsstelle eingeholt oder bei Antrag gleich mitübermittelt wird. Durch die Beantragung eines Zertifikats für einen Dritten ist es vorteilhafterweise möglich, mit dem Dritten verschlüsselt zu kommunizieren, ohne dass dieser bereits Inhaber eines Zertifikats war. Gerade diese Möglichkeit vereinfacht die rechnergestützte Kommunikation in digitalen Netzen, da selbst Dritte, welche bis dato noch kein entsprechendes Zertifikat besitzen, ohne eigene Aktivitäten an einer verschlüsselten Kommunikation teilnehmen können. Insbesondere im Email-Verkehr oder bei eStore-Anwendungen wird der Kontakt mit neuen Partnern hierdurch erleichtert.

[0018] In weiterer Ausgestaltung der Erfindung werden nach Ausstellung eines Zertifikats kontinuierlich weiter Informationen Dritter gesammelt und zu einer Neubewertung des Rangs des Vertrauensstatus herangezogen, so dass ein aktueller Vertrauensstatus online vom Zertifikatsbenutzer jederzeit abgefragt werden kann.

[0019] In bevorzugter Ausgestaltung der Erfindung fordern digitale Anwendungen auf einer Teilnehmerstation (Frontend) Informationen über den aktuellen Vertrauensstatus eines Zertifikats von der digitalen Zertifizierungsstelle (CA) vor und/oder während der Ausführung online an, so dass nur bei Bestätigung der Gültigkeit die Anwendung weiter ausgeführt wird. Hierdurch erhöht sich die Sicherheit gegen Missbrauch weiter im Vergleich zu Anwendungen, welche nur einmalig oder selten ein Zertifikat online anfordern bzw. überprüfen.

[0020] Nach der Erfindung weist eine digitale Zertifizierungsstelle in Form eines Servers (CA-Server) bzw. ein auf einem Computer laufendes CA-System zur Durchführung eines vorstehend erläuterten Verfahrens, welche über ein digitales Netzwerk mit Teilnehmerstationen Informationen austauschen kann, Programmmittel auf, welche vor und/oder nach der Ausstellung eines Zertifikats eine Übermittlung von Informationen Dritter über den Zertifikatsinhaber und eine deren Bewertung hinsichtlich eines hiervon abhängigen Rang eines Vertrauensstatus des Zertifikats ermöglicht und diesen Vertrauensstatus online zur Verfügung stellt. Eine derartige Eingabe-Möglichkeit für Informationen Dritter ist bei bekannten CA-Systemen in der PKI-Welt nicht gegeben, so dass

erst durch ein CA-System mit den Merkmalen nach Anspruch 9 eine Bewertung durch Informationen und damit eine Erhöhung der Verbreitungsgeschwindigkeit von Zertifikaten mit ausreichender und vorzugsweise dynamisch veränderbarer Vertrauensstufe ermöglicht wird.

[0021] Weist eine mit der digitalen Zertifizierungsstelle über ein digitales Netzwerk verbundene Teilnehmerstation Programmmittel auf, welche vor und/oder während jeder Ausführung einer Anwendung online den aktuellen Vertrauensstatus des für die Anwendung benötigten Zertifikats bei der Zertifizierungsstelle abfragt und nur bei Bestätigung des entsprechenden Rangs die Anwendung weiter ausführt, so erhöht sich auf einfache und komfortable Weise die Sicherheit gegen Missbrauch bei der Ausführung entsprechender Anwendungen.

[0022] Weitere vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

[0023] Die Erfindung wird nachfolgend anhand in der Zeichnung dargestellter Ausführungsbeispiele näher erläutert.

[0024] In der Zeichnung zeigen:

[0025] Fig. 1 ein schematisches Blockdiagramm einer bekannten Zertifizierungsstelle und

[0026] Fig. 2 ein schematisches Blockdiagramm einer Zertifizierungsstelle nach der Erfindung.

[0027] Die Erfindung wird nachfolgend anhand eines Vergleichs zwischen einer bekannten digitalen Zertifizierungsstelle **1**, wie in Fig. 1 dargestellt, und einer digitalen Zertifizierungsstelle **11** nach der Erfindung, wie in Fig. 2 dargestellt, jeweils in Form eines entsprechenden Servers bzw. einer auf einem Rechner laufenden Server-Applikation und deren rechnergestützter Kommunikation mit anderen Teilnehmern erläutert.

[0028] Mit einer herkömmlichen Zertifizierungsstelle **1** bestehen, wie dargestellt, zwei Arten von Kommunikationen. Der (zukünftige) Zertifikatsinhaber stellt eine Anfrage für die Ausstellung eines Zertifikats an die Zertifizierungsstelle **1**. Eine derartige Anfrage kann über das Internet mit einer Email-Feedback oder in einer anderen Weise erfolgen.

[0029] Die Anwendung bzw. der Zertifikatsbenutzer **5**, welcher das Zertifikat nutzten möchte, kommuniziert mit der Zertifizierungsstelle **1**, um Informationen über das Zertifikat zu erhalten. Diese Kommunikation erfolgt über ein Online-Zertifikatsstatusprotokoll (OCSP) oder durch Erhalt einer Zertifikatssperrliste (CRL), welche periodisch übertragen wird.

[0030] Die Zertifizierungsstelle **11** weist abgesehen von den bidirektionalen Kommunikationswegen (in Fig. 1 und Fig. 2 durch die entsprechenden Doppelpfeile dargestellt) zu den Zertifikatsinhabern **3** und Zertifikatsbenutzern **5** zusätzlich bidirektionale Kommunikationswege, nämlich zu anderen sogenannten digitalen Partnerzertifizierungsstellen **17** und zu digitalen sozialen Netzwerken **19** auf, mit welchen Informationen über das Zertifikat und/oder den Zertifikatsinhaber an die Zertifizierungsstelle **11** übermittelt oder gar untereinander ausgetauscht werden können.

[0031] Wie in Fig. 2 dargestellt, werden nach der Erfindung die gesammelten Informationen über die Zertifikate bzw. über die Zertifikatsinhaber in einer Datenbank **21** je Zertifikat abgespeichert, wobei diese Informationen nicht nur zur Ausstellung eines Zertifikats verwendet werden, sondern für andere, mit der digitalen Zertifizierungsstelle **11** über ein digitales Netzwerk online verbundene Partnerzertifizierungsstellen **17**, soziale Netzwerke **19**, Zertifikatsinhaber **3** und insbesondere Zertifikatsbenutzer **5** zur Verfügung stehen. Entsprechend werden auch nach Ausstellung eines Zertifikats weiter kontinuierlich Informationen über das Zertifikat von der digitalen Zertifizierungsstelle **11** gesammelt und gespeichert, wobei, wie in Fig. 2 ersichtlich, nach einem entsprechend geeigneten Bewertungsalgorithmus **23** ein jeweiliger Rang eines Vertrauensstatus innerhalb einer entsprechenden Rangfolge bzw. -liste mit mehr als zwei Rängen (also mehr als die Attribute „gültig” oder „nicht gültig”) den Zertifikaten zugeordnet wird.

[0032] Die neue Bewertung des Ranges bzw. der Vertrauensstufe eines Zertifikats kann hierbei in Abhängigkeit von dem Erhalt neuer Informationen über das jeweilige Zertifikat und/oder in vorgegebenen Zeitintervallen erfolgen. Hieraus resultiert, vorzugsweise in Abhängigkeit vom Zeitpunkt des Eingangs neuer Informationen, ein aktueller, erneut bewerteter Rang der Vertrauensstufe eines Zertifikats, welcher unmittelbar nach der Bewertung online den mit der digitalen Zertifizierungsstelle **11** verbundenen Teilnehmern, insbesondere den Zertifikatsbenutzern **5**, zur Verfügung steht.

[0033] Im Unterschied zur Kommunikation mit einer herkömmlichen Zertifizierungsstelle **1** wird daher mit dieser nicht nur zur Ausstellung eines Zertifikats kommuniziert, sondern auch an die digitale Zertifizierungsstelle **11** weiter Informationen über das Zertifikat nach Ausstellung ermittelt, dort gesammelt, hinsichtlich eines Vertrauensrangs bewertet und online den mit der Zertifizierungsstelle **11** verbundenen Teilnehmern **3**, **5**, **17**, **19** jederzeit zur Verfügung gestellt.

[0034] Statt einer Sperrliste, welche bisher ein Sperren eines Zertifikats und damit eines Schlüssels bzw. eines Schlüsselpaares aufgrund des zeitlichen Ab-

laufs des Zertifikats oder aufgrund anderer interner Informationen der Zertifizierungsstelle **1**, wie beispielsweise Verlassen eines Mitarbeiters einer Firma und damit Verlust seiner Berechtigung beinhaltet, und welche einem Zertifikatsbenutzer **3** nicht jederzeit online, sondern allenfalls in größeren Zeitabständen periodisch zur Verfügung gestellt wird, liegen nach dem erfindungsgemäßen Verfahren nunmehr unterschiedliche Ränge für einen Vertrauensstatus aus einer Rangliste mit mehr als zwei Stufen jederzeit online zur Nutzung vor, so dass ein Zertifikatsbenutzer **5**, beispielsweise ein Email-Versender oder eine Anwendung auf einer Teilnehmerstation, den aktuellen Vertrauensstatus vorzugsweise vor und/oder während jeder Ausführung einer Anwendung abfragen kann und die entsprechende Aktion nur bei ausreichender aktueller Vertrauensstufe des Zertifikats erfolgt.

[0035] Hierdurch wird vorteilhafterweise die Sicherheit gegen Missbrauch gesteigert. Zudem wird nach dem erfindungsgemäßen Verfahren sowie dem Aufbau einer erfindungsgemäßen digitalen Zertifizierungsstelle **11** die Kommunikation mit den Teilnehmern **3**, **5**, **17** und **19** nicht nur vor, sondern auch nach Ausstellung eines Zertifikats ermöglicht und erweitert, so dass diese Informationen auch für andere Teilnehmer schneller zur Verfügung stehen, was entsprechend zu einer schnelleren Verbreitung und Aktualisierung von digitalen Zertifikaten führt.

[0036] Im Folgenden werden anhand von zwei Beispielen einer typischen Zertifizierung die sich aus der Erfindung ergebenden Vorteile näher erläutert.

1. Beispiel

[0037] Ein (zukünftiger) Zertifikatsinhaber **3**, beispielsweise ein Kunde einer e-Store-Anwendung, ein Versender oder Empfänger einer Email, welcher bisher noch kein Zertifikat besitzt, etc., beantragt nach der Generierung eines Schlüssels bzw. eines Schlüsselpaares bei der digitalen Zertifizierungsstelle **11** ein Zertifikat bzw. dessen Signierung für diesen Schlüssel.

[0038] Nach der Erfindung ist es im Unterschied zur bisherigen Beantragung möglich, abgesehen von eigenen Informationen auch Informationen Dritter, wie beispielsweise Bestätigungen (endorsements) Dritter des beantragten Zertifikats, Bestätigungen über Teilangaben des Zertifikats, wie beispielsweise von Dritten bestätigte Informationen über Details des Zertifikatsinhabers (beispielsweise seine Adresse, etc.), Bestätigungen, welche durch andere Benutzer, beispielsweise den Arbeitgeber des Zertifikatsinhabers, seinen weiteren Background oder andere Personen und Organisationen, mit welchen der Zertifikatsinhaber in Verbindung steht, mitanzugeben. Selbstverständlich ist es hierbei denkbar, diese bestätigenden Informationen bzw. Bestätigungen einem unterschiedlichen Rang der Bedeutung zuzuordnen, so dass beispielsweise die Bestätigung einer Bank oder einer Regierungsbehörde für einen zukünftigen oder aktuellen Zertifikatsinhaber höher eingeschätzt werden kann als eine Bestätigung eines Bekannten des Zertifikatsinhabers in einem sozialen Netzwerk.

[0039] Derartige Informationen können von dem Zertifikatsinhaber mit der Antragsstellung oder von dieser getrennt an die Zertifizierungsstelle **11** übermittelt werden, wobei die Zertifizierungsstelle **11** hierbei auch mit der Ausstellung eines Zertifikats auf eine zumindest angekündigte Übermittlung warten kann. Die bestätigenden Informationen bzw. Bestätigungen können aber auch auf Veranlassung Dritter, typischerweise auf Anfrage des Zertifikatsinhabers, direkt an die Zertifizierungsstelle übermittelt werden.

[0040] Selbstverständlich ist es auch möglich, dass die Zertifizierungsstelle **11** beispielsweise auf Angabe von entsprechenden Referenzen durch den Zertifikatsinhaber auf eigene Veranlassung von wenigstens Teilen der genannten Referenzen Bestätigungen einholt oder von diesen direkt unaufgefordert mitgeteilt bekommt.

[0041] Bei der Bewertung des Rangs eines Vertrauensstatus werden alle vorgenannten Informationen abhängig von deren Bedeutung mittels eines geeigneten Bewertungsalgorithmus **23** für einen Rang bewertet, wobei im Unterschied zur herkömmlichen Ausstellung eines Zertifikats nicht nur herkömmliche in Zertifizierungsstellen **1** zur Identitätsverifizierung intern vorhandene Parameter verwendet werden, sondern, wie vorstehend erläutert, auch Informationen Dritter hierbei wesentlich eingebunden werden. Zusätzlich ist es denkbar, dass frühere Informationen über den Zertifikatsinhaber, wie beispielsweise die Historie früherer Zertifikate, welche für denselben Zertifikatsinhaber ausgestellt wurden, etc., ebenfalls zur Bewertung der Vertrauensstufe herangezogen werden.

[0042] Eine Entscheidung der Zertifizierungsstelle über den Vertrauensstatus eines Zertifikats kann hierbei beispielsweise auch in Abhängigkeit der Gewichtung der Information und/oder Status des Dritten selbst getroffen werden. Beispielsweise kann die Gewichtung einer Bestätigung durch einen Dritten abhängen von der digitalen Identität des Dritten (dessen Zertifikatsklasse bzw. -stufe, ob und welche Zertifizierungsstelle das Zertifikat des Dritten ausstellte, etc.) und/oder der Historie des Dritten (wie viele von diesem Dritten bestätigte Zertifikate wurden später wegen Missbrauch wiederrufen).

[0043] Auch kann eine Korrelation zwischen Bestätigungen auf der Grundlage von Teil-)Informationen über die Identitäten der (bestätigenden) Dritten ge-

troffen werden.

[0044] Beispielsweise könnte die Zertifizierungsstelle davon ausgehen, dass es sich um ein- und dieselbe Person handelt, falls mehrere (bestätigende) Dritte denselben Vor- und Familiennamen besitzen, während andere Charakteristika abweichen. Demzufolge könnten diese mehreren Bestätigungen (eines einzigen Dritten) geringer gewichtet werden als Bestätigungen unterschiedlicher Dritter.

[0045] Auch ist es denkbar dass Vorname, Name und andere Informationen im Zertifikat des bestätigenden Dritten hinsichtlich ihrer Widerspruchsfreiheit analysiert werden, insbesondere wenn es sich hierbei nur um ein Klasse **1** Zertifikat oder ein von einer weniger bekannten bzw. weniger zuverlässigen Zertifizierungsstelle ausgestelltes höherwertiges Zertifikat handelt. Beispielsweise sagt ein nicht lesbarer Name in der Identität des bestätigenden Dritten nichts über die tatsächliche (dahinterstehende) Person aus. Ebenso sollte einer Bestätigung eines Dritten mit Namen einer berühmten (beispielsweise westlichen) Persönlichkeit, welcher jedoch offensichtlich (aus einer Inkonsistenz hinsichtlich weiterer Informationen erkennbar wie beispielsweise der Ortsinformation „aus dem fernen Osten kommend") missbräuchlich benutzt wird, keinerlei oder eine allenfalls sehr geringe Gewichtung zur Folge haben.

[0046] Weiterhin ist es denkbar eine Korrelation zwischen verschiedenen bzw. unterschiedlichen Bestätigungen von Teilinformationen zu bilden. So können unterschiedliche Dritte ein- und dieselbe Person bestätigen, indem jeder Dritte nur jene (Teil-)Information bestätigt, welche im bekannt ist und welcher er vertraut. Durch die Bildung einer derartige Korrelation kann die Vertauensstufe mittels eines entsprechenden Algorithmus über ein lineares Maß (einfache Addition der Bestätigungen) hinaus erhöht werden.

[0047] Als weitere Möglichkeit einer Korrelation zwischen mehreren Informationen ist es denkbar eine Beziehung zwischen den Identitäten eines Teilnehmers und des bestätigenden Dritten zu berücksichtigen. Beispielweise könnte eine Bestätigung eines Dritten, welcher derselben Firma wie der Zertifikatsinhaber angehört, höher gewichtet werden als die Bestätigung eines Dritten, welcher einem sozialen Netzwerk angehört. Hinsichtlich der postalischen Adresse könnte eine Bestätigung eines Dritten derselben Familie (insbesondere im selben Land lebend) höher gewichtet werden als eine Bestätigung anderer.

[0048] Wie bereits erläutert, werden die ausgestellten Zertifikate zusammen mit der jeweils aktuellen Vertrauensstufe in der Zertifizierungsstelle **11** im Datenbankspeicher **21** gespeichert, so dass Zertifikatsbenutzer **5** diese jederzeit online, beispielsweise via OCSP oder Ähnliches, erhalten können. Die Zertifizierungsstelle **11** übermittelt hierbei dem Zertifikatsbenutzer **5** den Rang bzw. die Vertrauensstufe des Zertifikats.

[0049] Neben der Mitteilung über die Vertrauensstufe des Zertifikats kann die digitale Zertifizierungsstelle **11** zumindest auf Anfrage auch das Zertifikat eines bestimmten Zertifikatsinhabers nach Nennung eines entsprechenden Identifizierungsmerkmals, beispielsweise die Email-Adresse des Zertifikatsinhabers, an einen Zertifikatsbenutzer **5** oder andere zurücksenden. Hierbei ist es denkbar, dass die digitale Zertifizierungsstelle **11** als solches Identifizierungsmerkmal auch Teilmerkmale, wie beispielsweise den Vor- und Nachnamen eines gewünschten Zertifikatsinhabers **5**, akzeptiert, um eine Liste von Zertifikaten zurückzusenden, welche möglicherweise zu dem gewünschten Zertifikatsinhaber **5** gehören bzw. der Anfrage entsprechen. Um Missbrauch insbesondere für Spam-Zwecke zu verhindern, kann die digitale Zertifizierungsstelle **11** geeignete Gegenmaßnahmen vorsehen. So kann beispielsweise die Anzahl der Zertifikate für eine solche Anfrage auf eine vordefinierte Anzahl begrenzt werden.

[0050] Wie bereits vorstehend erläutert, kann die digitale Zertifizierungsstelle **11** auch nach Ausstellung eines Zertifikats weiterhin Informationen über das Zertifikat, wie Bestätigungen und Beschwerden, sammeln, um jeweils eine neue aktuelle Vertrauensstufe des entsprechenden Zertifikats zu ermitteln.

[0051] Falls die Vertrauensstufe eines Zertifikats unter einen vorbestimmten Wert bzw. Rang fällt, kann die digitale Zertifizierungsstelle **11** das Zertifikat widerrufen bzw. als ungültig erklären und dies mittels OCSP oder Sperrliste an andere, insbesondere Zertifikatsbenutzer **5**, mitteilen. Hierdurch werden insbesondere Anwendungen, welche nur Attribute „Zertifikat gültig" oder „Zertifikat nicht gültig" verstehen, aus Kompatibilitätsgründen weiter unterstützt.

[0052] Vorzugsweise werden von der Zertifizierungsstelle **11** jedoch aktiv an entsprechende Teilnehmer Informationen über ein Zertifikat, insbesondere dessen Widerruf, mitgeteilt. Beispielsweise erfolgt eine Mitteilung an Zertifikatsbenutzer **5** über einen Widerruf von Zertifikaten, nach welchen sie bereits früher anfragten mittels eine in der Anwendung voreingestellten automatische Update-Funktion in Form von Sperrlisten oder beliebiger anderer Form.

[0053] Die Zertifikatsbenutzer **5** können den Status des Zertifikats auch über OCSP als Attribut „widerrufen" bzw. „ungültig" erhalten, wenn der Rang bzw. die Vertrauensstufe unter einen vordefinierten Wert bzw. Rang fällt.

[0054] Selbstverständlich ist es auch denkbar, dass die Zertifizierungsstelle **11** auch Zertifikate speichert,

welche bei anderen Zertifizierungsstellen ausgestellt wurden, wobei sich eine Bewertung für diese Zertifikate von der Bewertung der eigenen ausgestellten Zertifikate unterscheiden kann, beispielsweise durch Anwendung eines anderen Parameters des Bewertungsalgorithmus **23** oder durch Anwendung eines anderen entsprechenden Bewertungsalgorithmus.

2. Beispiel

[0055] Nach der Erfindung ist es auch möglich, dass statt des Zertifikatsinhabers auch ein Dritter, beispielsweise der Zertifikatsbenutzer **5**, bei der Zertifizierungsstelle **11** ein Zertifikat für einen anderen Teilnehmer, also den zukünftigen Zertifikatsinhaber **3**, beantragt. In diesem Fall führt die digitale Zertifizierungsstelle **11** einige Überprüfungen unter Zuhilfenahme ihres eigenen Wissens bzw. Informationen und des Wissens bzw. der Informationen von Dritten durch. Beispielsweise kann die Anfrage abgelehnt werden, wenn für den zukünftigen Zertifikatsinhaber bereits ein Zertifikat existiert, welches benutzt werden kann (internes Wissen).

[0056] Weiterhin könnte gefordert werden, dass der Zertifikatstyp zum Antragstellerprofil passen muss; beispielsweise darf ein Email-Benutzer ein Email-Zertifikat für den anderen Email-Teilnehmer (beispielsweise Empfänger) beantragen, dagegen nicht für ein SSL-Zertifikat. Im zulässigen Fall generiert die Zertifizierungsstelle **11** den Schlüssel und registriert das Zertifikat, und der Antragsteller bekommt sein beantragtes Zertifikat zurück.

[0057] Im Weiteren übersendet die Zertifizierungsstelle **11** den generierten Schlüssel und das Zertifikat an den Zertifikatsinhaber auf geschütztem Weg. Beispielsweise können diese zu der zum Zertifikat gehörenden Email-Adresse als PFX-Datei (personal information exchange) übersandt werden, während das Passwort mit einer anderen Mail oder auf anderem digitalen Kanal übermittelt wird. Hierbei kann gefordert sein, dass das neu generierte Zertifikat für dritte Benutzer so lange nicht zur Verfügung stehen, bis es vom Empfänger bestätigt wurde, um Missbrauch zu vermeiden. Sofern der Empfänger das Zertifikat innerhalb einer bestimmten Frist nicht bestätigt, kann die Zertifizierungsstelle **11** das Zertifikat aber auch automatisch widerrufen. Alternativ kann der Empfänger das Zertifikat einmalig verwenden, beispielsweise für das Lesen der an ihn vom Antragsteller gesandten verschlüsselten Email, und später selbst ein eigenes Zertifikat beantragen, so dass das Zertifikat nach einmaliger Benutzung verfällt.

[0058] Hierdurch wird verschiedenen webbasierten Anwendungen bzw. Nutzern allgemein der Zugang zu einer PKI-basierten Sicherheit erleichtert, da beispielsweise ein Internetshop-Besitzer seinen Kunden oder ein Sender an einen Empfänger von den Kunden oder dem Empfänger nicht mehr das Generieren eines Schlüssels und die Beantragung eines Zertifikats als Vorbedingung zur Teilnahme des gesicherten Kommunikation auferlegen muss, sondern diese Schritte für den kundenfreundlich bzw. anwenderfreundlich erledigt werden können. Hierdurch erhöht sich der Komfort für den Kunden und Empfänger wesentlich – zusätzlich zur erhöhten Sicherheit hinsichtlich der Vertrauensstufe des Zertifikats, wie vorstehend erläutert, so dass auch auf diesem Weg einer weiteren und schnelleren Verbreitung von Zertifikaten keine als umständlich empfundenen Bedingungen oder fehlendes Wissen von Benutzern im Wege stehen.

[0059] Wesentlich ist nach der Erfindung, dass statt einem dezentralen gegenseitigen Signieren von Schlüsseln eine Zertifikat bei einer zentralen, digitalen Zertifizierungsstelle beantragt und ausgestellt wird, wobei zur Erhöhung der Zertifikatsqualität der Zertifizierungsstelle zusätzliche Informationen Dritter zugängig gemacht werden. Diese Informationen können daher nicht nur bei der Ausstellung eines Zertifikats berücksichtigt sondern auch zur Bewertung der Zertifikatsqualität bzw. der Vertrauensstatus eines Zertifikats herangezogen werden. Der Vertrauensstatus kann hierbei vorteilhafterweise jedem Zertifikatsbenutzter aktuell zur Verfügung gestellt werden, wodurch sich die Sicherheit bei der Verwendung (Kommunikation, Applikation, etc.) erhöht.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Nicht-Patentliteratur

- X.509 Standard **[0006]**

Patentansprüche

1. Verfahren zur Ausstellung, Überprüfung und Verteilung von digitalen Zertifikaten für die Nutzung in Public-Key-Infrastrukturen, bei dem ein Antragsteller (**3**, **5**) bei einer digitalen Zertifizierungsstelle (**11**) ein digitales Zertifikat beantragt,
dadurch gekennzeichnet, dass
a) zur Bewertung eines Vertrauensstatus für das Zertifikat eines Zertifikatsinhabers (**3**) wenigstens eine Information (**21**) Dritter über den Zertifikatsinhaber (**3**) herangezogen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die wenigstens eine Information (**21**) Dritter von der Zertifizierungsstelle (**11**) von Dritten (**5**, **17**, **19**) über eine digitale Verbindung, insbesondere via Internetverbindung, eingeholt oder von Dritten (**5**, **17**, **19**) oder vom Antragsteller (**3**, **5**) direkt an die Zertifizierungsstelle (**11**) übermittelt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die wenigstens eine Information (**21**) Dritter mittels eines geeigneten Bewertungs-Algorithmus (**23**) zur Bewertung eines Rangs innerhalb einer Rangliste führt.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass eine Information über den Rang des berechneten Vertrauensstatus von der Zertifizierungsstelle (**11**) auf Abfrage online für Zertifikats-Benutzer (**5**) zur Verfügung gestellt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Zertifikat vom Inhaber (**3**) beantragt wird.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass das Zertifikat von einem Dritten (**5**, **17**, **19**) für den Inhaber beantragt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass nach Ausstellung eines Zertifikats kontinuierlich weiter Informationen (**2**) Dritter gesammelt werden und zu einer Neubewertung des Rangs des Vertrauensstatus herangezogen werden, so dass ein aktueller Vertrauensstatus online vom Zertifikatsbenutzer (**5**) jederzeit abgefragt werden kann.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass eine digitale Anwendung auf einer Teilnehmerstation (Frontend) eines Zertifikatsbenutzers (**5**) Informationen über den aktuellen Vertrauensstatus eines Zertifikats von der digitalen Zertifizierungsstelle (CA) vor und/oder während der Ausführung online anfordert und nur bei Bestätigung der Gültigkeit des Zertifikats die Anwendung weiter ausgeführt wird.

9. Digitale Zertifizierungsstelle zur Durchführung eines Verfahrens nach einem der vorhergehenden Ansprüche, welche über ein digitales Netzwerk mit Teilnehmerstationen Informationen austauschen kann, dadurch gekennzeichnet, dass die digitale Zertifizierungsstelle (**11**) Programmmittel aufweist, welche vor und/oder nach der Ausstellung eines Zertifikats eine Übermittlung von Informationen (**21**) Dritter über den Zertifikatsinhaber (**3**) und eine deren Bewertung hinsichtlich eines hiervon abhängigen Rang eines Vertrauensstatus des Zertifikats ermöglichen und diesen Vertrauensstatus online zur Verfügung stellen.

10. Anordnung aus einer digitalen Zertifizierungsstelle nach Anspruch 9 und wenigstens einer hiermit über ein digitales Netzwerk verbundenen Teilnehmerstation eines Zertifikatsbenutzers (**5**), welche Programmmittel aufweist, welche vor und/oder während jeder Ausführung einer Anwendung online den aktuellen Vertrauensstatus des für die Anwendung benötigten Zertifikats bei der Zertifizierungsstelle (**11**) abfragen und nur bei Bestätigung des entsprechenden Rangs die Anwendung weiter ausführen.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

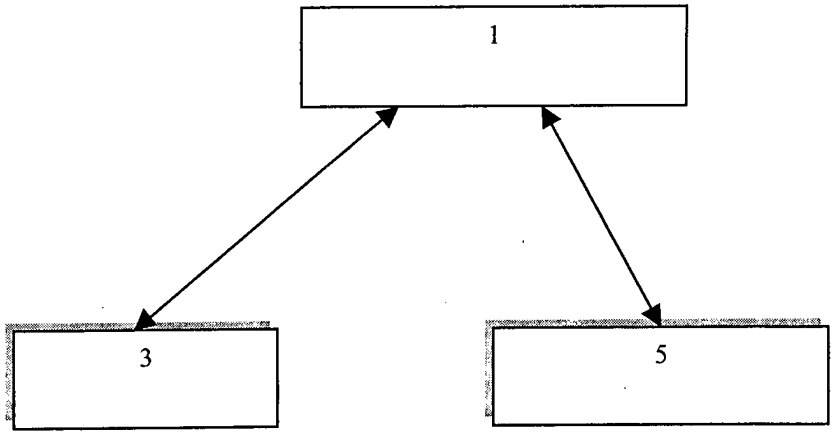


Fig. 1

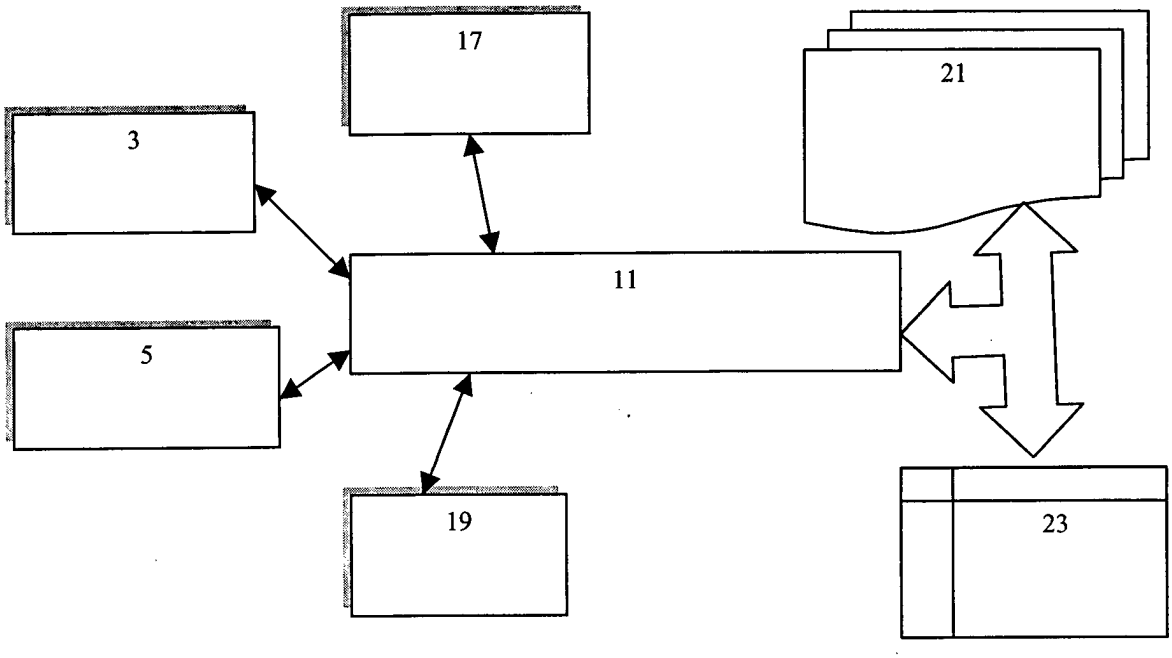


Fig. 2