(19) Deutsches Patent- und Markenamt

(10) **DE 10 2014 224 928 A1** 2016.06.09

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2014 224 928.7**
(22) Anmeldetag: **04.12.2014**
(43) Offenlegungstag: **09.06.2016**

(51) Int Cl.: ***H04L 9/30*** (2006.01)

(71) Anmelder:
Universität Rostock, 18055 Rostock, DE

(74) Vertreter:
Gulde & Partner Patent- und Rechtsanwaltskanzlei mbB, 10179 Berlin, DE

(72) Erfinder:
Salomon, Ralf, Prof., 18119 Rostock, DE

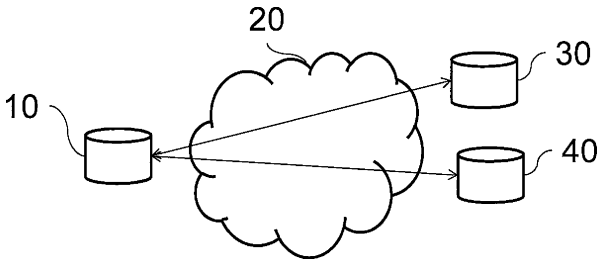
(56) Ermittelter Stand der Technik:
US 2009 / 0 198 997 A1

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren und Server zum Versenden von verschlüsselten Daten an einen Nutzer**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren und einem Server zum Versenden von verschlüsselten Daten an einen Nutzer in einer Domain.
Der Server (10) zum Versenden von verschlüsselten Daten an einen Nutzer in einer Domain umfasst Mittel zum Auslesen mindestens einer zusammen mit der Domain gespeicherten Adresse eines Eingangsservers von einem weiteren Server (30) über ein öffentliches Netzwerk (20), dadurch gekennzeichnet, dass das Mittel zum Auslesen ausgebildet ist, auch eine zusammen mit der Domain gespeicherte Adresse eines Schlüsselservers (40) von dem Server auszulesen, wobei der weitere Server (30) eine Speichereinheit umfasst, auf der in über ein öffentliches Netzwerk adressierbarer Form Mindestens eine Domain zusammen mit mindestens einer Dateneingangsserveradresse und mindestens einer Schlüsselserveradresse gespeichert sind.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren und einem Server zum Versenden von verschlüsselten Daten an einen Nutzer.

[0002] Asymmetrische Kryptographieverfahren zum Verschlüsseln von Daten basieren auf einem Schlüsselpaar mit einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel ermöglicht einem Sender, Daten für einen Datenaustausch in einem öffentlichen Netz mit dem privaten Schlüssel so zu verschlüsseln, dass die Daten nur mittels des privaten Schlüssels veränderbar aber für jeden im Besitz des öffentlichen Schlüssels lesbar sind. Der private Schlüssel entspricht also einer Signatur und garantiert die Echtheit der Daten.

[0003] Weiterhin können Daten mit dem öffentlichen Schlüssel so verschlüsselt werden, dass die Daten nur mittels des privaten Schlüssels lesbar und damit veränderbar sind. Der öffentliche Schlüssel garantiert also die Vertraulichkeit der Daten.

[0004] Ein Sender im Besitz eines öffentlichen Schüssels eines ersten Schlüsselpaars, zu dem ein privater Schlüssel im Besitz eines Empfängers gehört, kann also an den Empfänger zu sendende Daten mit dem öffentlichen Schlüssel verschlüsseln, so dass nur der Empfänger die verschlüsselten Daten lesen kann.

[0005] Ist der Sender hingegen nicht im Besitz des öffentlichen Schlüssels, so muss er den öffentlichen Schlüssel erst selbst empfangen. Insbesondere wenn der Empfänger nicht im Besitz ist eines weiteren öffentlichen Schüssels eines zweiten Schlüsselpaars, zu dem ein weitere privater Schlüssel im Besitz des Senders gehört, muss der öffentliche Schlüssel unverschlüsselt übertragen werden.

[0006] In der Übertragung an den Sender kann der öffentliche Schlüssel gefälscht, also durch einen falschen öffentlichen Schlüssel ersetzt werden, ohne der Sender dies merkt. Dies ist ein sogenannter man-in-the-middle attack.

[0007] Verschlüsselt nun der Sender die Daten mit dem empfangenen öffentlichen Schlüssel, der falsch ist, und überträgt die falsch verschlüsselten Daten, so können die falsch verschlüsselten Daten in der Übertragung abgefangen, mit dem zugehörigen gefälschten privaten Schlüssel entschlüsselt, verändert und mit dem öffentlichen Schlüssel des Empfängers wieder verschlüsselt an den Empfänger übertragen werden, ohne dass der Empfänger dies merkt.

[0008] Solange nicht zumindest einer von Sender und Empfänger zweifelsfrei den richtigen öffentlichen Schlüssel des jeweils anderen besitzt, ist eine fälschungssichere Datenübertragung nicht möglich.

[0009] Ein öffentlicher Schlüssel kann daher beispielsweise auf Internetseiten zur Verfügung gestellt werden. Der Besitzer des zugehörigen privaten Schlüssels kann dann jederzeit und von überall her überprüfen, ob der über die Internetseite abrufbare öffentliche Schlüssel zu seinem privaten Schlüssel gehört.

[0010] Eine andere Möglichkeit ist eine Zertifizierung des Schlüssels. Das Zertifikat bestätigt den Empfänger und/oder weitere Eigenschaften des öffentlichen Schlüssels. Durch das Zertifikat können Sender den öffentlichen Schlüssel dem Empfänger zuordnen und/oder seinen Geltungsbereich bestimmen. Das Zertifikat stellt die korrekte Anwendung des öffentlichen Schlüssels sicher und ermöglicht so Vertraulichkeit, Authentizität und Integrität der verschlüsselten Daten.

Erfindung

[0011] Erfindungsgemäß wird ein Server gemäß Anspruch 1 zur Verfügung gestellt. Der Server umfasst eine Speichereinheit, auf der in über ein öffentliches Netzwerk adressierbarer Form mindestens eine Domain zusammen mit mindestens einer Adresse eines Eingangsservers gespeichert ist. Der Server ist dadurch gekennzeichnet, dass die Domain weiterhin zusammen mit mindestens einer Adresse eines Schlüsselservers gespeichert ist.

[0012] Erfindungsgemäß wird weiterhin ein Server gemäß Anspruch 2 zum Versenden von verschlüsselten Daten an einen Nutzer in einer Domain zur Verfügung gestellt. Der Server umfasst Mittel zum Auslesen mindestens einer zusammen mit der Domain gespeicherten Adresse eines Eingangsservers von einem Server über ein öffentliches Netzwerk. Der Server ist dadurch gekennzeichnet, dass das Mittel zum Auslesen ausgebildet ist, auch eine zusammen mit der Domain gespeicherte Adresse eines Schlüsselservers auszulesen, wenn der Server erfindungsgemäß ausgebildet ist.

[0013] Erfindungsgemäß wird auch ein Verfahren gemäß Anspruch 6 zum Versenden von verschlüsselten Daten an einen Nutzer in einer Domain zur Verfügung gestellt. Das Verfahren umfasst Auslesen mindestens einer zusammen mit der Domain gespeicherten Adresse eines Eingangsservers von einem Server über ein öffentliches Netzwerk. Das Verfahren ist dadurch gekennzeichnet, dass es weiterhin ein Auslesen einer zusammen mit der Domain gespeicherte Adresse eines Schlüsselservers umfasst, wobei der Server erfindungsgemäß ausgebildet ist.

[0014] Die Erfindung ermöglicht eine Automatisierung des sicheren Versendens von Daten, da der dafür notwendige öffentliche Schlüssel in einer Weise abgelegt ist, die ein automatisiertes Auffinden des öffentlichen Schlüssels ermöglicht.

[0015] In einer bevorzugten Ausführungsform kann das Verfahren weiterhin folgende Schritte umfassen: ein Auslesen eines dem Nutzer zugeordneten Schlüssel mittels der Adresse des Schlüsselservers von einem Schlüsselserver, Verschlüsseln der Daten mit dem öffentlichen Schlüssel und Übertragen der verschlüsselten Daten an einen zu der Dateneingangsserveradresse zugehörigen Dateneingangsserver. In einer bevorzugten Ausführungsform kann der Server entsprechend ausgebildete Mittel umfassen.

[0016] Das Verfahren kann weiterhin umfassen: Herunterladen eines Zertifikats des öffentlichen Schlüssels über das öffentliche Netzwerk und Überprüfen der Echtheit des öffentlichen Schlüssels anhand des Zertifikats, wobei das Verschlüsseln nach dem Überprüfen und nur dann erfolgt, wenn der öffentliche Schlüssel echt ist. Der Server kann entsprechend ausgebildete Mittel umfassen.

[0017] Dabei kann das Zertifikat in einer Verschlüsselung des öffentlichen Schlüssels mit einem privaten Schlüssel bestehen und das Überprüfen der Echtheit kann ein Entschlüsseln des verschlüsselten öffentlichen Schlüssels mit einem weiteren, zum privaten Schlüssel zugehörigen öffentlichen Schlüssel umfassen.

[0018] Die verschlüsselten Daten können nach Post Office Protocol (POP), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP) oder Simple Mail Access Protocol (SMAP) übertragen bzw. versandt werden.

[0019] Weitere bevorzugte Ausgestaltungen der Erfindung ergeben sich aus den übrigen, in den Unteransprüchen genannten Merkmalen.

[0020] Die verschiedenen in dieser Anmeldung genannten Ausführungsformen der Erfindung sind, sofern im Einzelfall nicht anders ausgeführt, mit Vorteil miteinander kombinierbar.

[0021] Die Erfindung wird nachfolgend in Ausführungsbeispielen anhand der zugehörigen Zeichnungen erläutert. Es zeigt beispielhaft und schematisch:

[0022] **Fig.** 1 eine Ausführungsform der Erfindung.

[0023] Die Erfindung wird im Folgenden am Beispiel eines Emailaustausches über ein öffentliches Netzwerk beschrieben. Die Erfindung ist jedoch nicht auf Emailaustausch beschränkt, sondern lässt sich für jede Form des Datenaustausches verwenden.

[0024] Ein Nutzer schreibt eine Email an empfänger@domain und gibt einen Befehl zum Versand der Email. Ein Ausgangsserver **10** oder ein Mail Transfer Agenten (MTA) ermittelt zunächst zumindest ein Mail-eXchange-Resource Record (MX-RR oder MXR) der Domain domain. Das MXR ist auf einem über das öffentliche Netzwerk **20** adressierbaren Server **30** gespeichert, dessen Adresse bekannt oder einfach herausfindbar ist. Das MXR listet dabei mindestens eine Maileingangsserveradresse der Domain domain in mittels der Domain adressierbarer Form. Der Ausgangsserver **10** (Datenausgangsserver) liest die Maileingangsserveradresse anhand der Domain domain aus und baut dann eine SMTP-Verbindung mit dem ersten gelisteten Eingangsserver (Dateneingangsserver) der Domain domain auf.

[0025] Erfindungsgemäß listet der MXR zusätzlich eine Adresse eines Schlüsselservers. Es wird daher erfindungsgemäß unter anderem ein Mail-eXchange-Resource and Key Record (MXKR) vorgeschlagen.

[0026] Ehe der Ausgangsserver **10** die SMTP-Verbindung mit dem Eingangsserver anhand der Maileingangsserveradresse aufbaut, baut er eine Verbindung zu dem Schlüsselserver **40** anhand der Adresse des Schlüsselservers auf. Der Schlüsselserver **40** ordnet öffentliche Schlüssel von Nutzern mit Emailadressen in der Domain domain den Emailadressnamen der Nutzer in der Domain zu. Der Ausgangsserver **10** lädt vom Schlüsselserver **40** der öffentlichen Schlüssel, der auf dem Schlüsselserver **40** dem Emailadressnamen empfänger zugeordnet ist.

[0027] Ein Emailprogramm oder der Ausgangsserver **10** verschlüsselt dann die Email mit dem öffentlichen Schlüssel und überträgt die verschlüsselte Email über die SMTP-Verbindung.

[0028] Zusammen mit dem öffentliche Schlüssel können weitere Informationen, beispielsweise bezüglich des zu verwendenden Verschlüsselungsalgorithmus und/oder Parametern der Verschlüsselung, auf dem Schlüsselserver gespeichert sein. Dann können diese Informationen zusammen mit dem öffentlichen Schlüssel vom Schlüsselserver auf den Ausgangsserver heruntergeladen und bei der Verschlüsselung gegebenenfalls berücksichtigt werden.

[0029] Um sicher zu gehen, dass beim Herunterladen des öffentlichen Schlüssels kein man-in-the-middle attack unbemerkt erfolgen kann, kann zusammen mit dem öffentlichen Schlüssel ein Zertifikat hinterlegt sein, mit dem sich die Echtheit des öffentlichen Schlüssels überprüfen lässt. Das Zertifikat kann von einer glaubwürdigen dritten Stelle heraus-

gegeben sein und nachweisen, dass der öffentliche Schlüssel authentisch ist.

[0030] Das Zertifikat kann darin bestehen, dass der öffentlichen Schlüssel in einer mit einem privaten Schlüssel verschlüsselten Form auf dem Schlüsselserver gespeichert ist, wobei der zum privaten Schlüssel zugehörige öffentliche Schlüssel der vertrauenswürdigen dritten Stelle allgemein zugänglich ist und von der Server zum Entschlüsseln des verschlüsselten öffentlichen Schlüssels verwendet wird.

[0031] Dann verschlüsselt das Emailprogramm oder der Ausgangsserver die Email nur dann mit dem öffentlichen Schlüssel und überträgt die verschlüsselte Email über die SMTP-Verbindung, wenn der öffentliche Schlüssel authentisch ist.

[0032] Das Zertifikat bestätigt den Empfänger und/oder weitere Eigenschaften des öffentlichen Schlüssels. Durch das Zertifikat können Sender den öffentlichen Schlüssel dem Empfänger zuordnen und/oder seinen Geltungsbereich bestimmen. Das Zertifikat stellt die korrekte Anwendung des öffentlichen Schlüssels sicher und ermöglicht so Vertraulichkeit, Authentizität und Integrität der verschlüsselten Daten.

[0033] Auch ohne Zertifikat ist es für den Empfänger empfänger möglich, man-in-the-middle attacks zu detektieren. Der Empfänger muss dazu lediglich von einem anderen Computer und mit einer anderen Emailadresse eine email an empfänger@domain schicken und den zur Verschlüsselung der Email erhaltenen öffentlichen Schlüssel dahingehend überprüfen, ob er dem öffentlichen Schlüssel des Empfängers entspricht.

[0034] Diese Detektion kann insbesondere automatisiert erfolgen. Beispielsweise kann der Schlüsselserver oder ein empfängerseitiger Ausgangserver konfiguriert sein, automatisiert von der anderen Emailadresse eine email an empfänger@domain zu schicken und den zur Verschlüsselung der Email erhaltenen öffentlichen Schlüssel mit dem gespeicherten öffentlichen Schlüssel zu vergleichen. Unterscheiden sich die Schlüssel, so kann beispielsweise der Schlüsselserver dem Empfänger eine mit dem gespeicherten öffentlichen Schlüssel verschlüsselte Email schicken, die auf den Unterschied aufmerksam macht.

[0035] Zusätzlich oder alternativ kann das Auslesen des öffentlichen Schlüssels insbesondere über einen anonymisierten Datenpfad durch das Netzwerk, beispielsweise über ein Tor Netzwerk, und mit einem anderen Protokoll erfolgen. Einem man-in-the-middle ist dann unmöglich, festzustellen, wer den öffentlichen Schlüssel ausliest. Der man-in-the-middle kann daher Attacken nicht auf Auslesevorgänge beschränken, bei denen die auslesende Stelle den öffentlichen Schlüssel noch nicht hat.

[0036] Der Schlüsselserver kann insbesondere der Eingangsserver sein, d. h. Schlüsselserver und Eingangsserver sind identisch. In diesem Fall kann der öffentliche Schlüssel an einem Port des Eingangsservers hinterlegt sein und über diesen Port bezogen werden. Der Port kann im Mail-eXchange-Resource and Key Record hinterlegt sein oder voreingestellt sein.

[0037] In einer beispielhaften Ausführungsform umfasst das erfindungsgemäße Verfahren zum Versenden von verschlüsselten Daten an einen Nutzer in einer Domain folgende Schritte: Auslesen mindestens einer zusammen mit der Domain gespeicherten Adresse eines Eingangsservers von einem Server über ein öffentliches Netzwerk und Auslesens eines an einem Port des Eingangsservers hinterlegten öffentlichen Schlüssels des Nutzers. Dabei kann der Port voreingestellt sein oder zusammen mit der Adresse des Eingangsservers auf dem Server gespeichert sein.

[0038] Ein Server zum Versenden von verschlüsselten Daten an einen Nutzer in einer Domain kann Folgendes umfassen: Mittel zum Auslesen mindestens einer zusammen mit der Domain gespeicherten Adresse eines Eingangsservers von einem Server über ein öffentliches Netzwerk und Mittel zum Auslesens eines an einem Port des Eingangsservers hinterlegten öffentlichen Schlüssels des Nutzers. Dabei kann der Port voreingestellt sein oder zusammen mit der Adresse des Eingangsservers auf dem Server gespeichert sein.

Patentansprüche

1. Server (**30**) umfassend:
eine Speichereinheit, auf der in über ein öffentliches Netzwerk adressierbarer Form mindestens eine Domain zusammen mit mindestens einer Adresse eines Eingangsservers gespeichert ist, **dadurch gekennzeichnet,** dass die Domain weiterhin zusammen mit mindestens einer Adresse eines Schlüsselservers gespeichert ist.

2. Server (**10**) zum Versenden von verschlüsselten Daten an einen Nutzer in einer Domain, umfassend:
Mittel zum Auslesen mindestens einer zusammen mit der Domain gespeicherten Adresse eines Eingangsservers von einem Server über ein öffentliches Netzwerk, **dadurch gekennzeichnet,** dass das Mittel zum Auslesen ausgebildet ist, auch eine zusammen mit der Domain gespeicherte Adresse eines Schlüsselservers auszulesen, wenn der Server (**30**) gemäß Anspruch 1 ausgebildet ist.

3. Server (**10**) nach Anspruch 2, wobei das Mittel zum Auslesen ausgebildet ist, mittels der Adresse des Schlüsselservers einen dem Nutzer zugeordneten Schlüssel von einem Schlüsselserver (**40**) auszulesen, und wobei der Server (**10**) weiterhin Mittel zum Verschlüsseln der Daten mit dem öffentlichen Schlüssel und Mittel zum Übertragen der verschlüsselten Daten an einen zu der Dateneingangsserveradresse zugehörigen Dateneingangsserver.

4. Server (**10**) nach Anspruch 2 oder 3, wobei der öffentlichen Schlüssel in einer mit einem privaten Schlüssel verschlüsselten Form auf dem Schlüsselserver (**40**) gespeichert ist und wobei das Mittel zum Überprüfen der Echtheit umfasst:
Mittel zum Entschlüsseln des verschlüsselten öffentlichen Schlüssels mit einem weiteren, zum privaten Schlüssel zugehörigen öffentlichen Schlüssel.

5. Server (**10**) nach einem der Ansprüche 3 und 4, wobei die verschlüsselten Daten nach Post Office Protocol (POP), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP) oder Simple Mail Access Protocol (SMAP) übertragen werden.

6. Verfahren zum Versenden von verschlüsselten Daten an einen Nutzer in einer Domain, umfassend:
Auslesen mindestens einer zusammen mit der Domain gespeicherten Adresse eines Eingangsservers von einem Server über ein öffentliches Netzwerk, wobei das Verfahren dadurch gekennzeichnet ist, dass es weiterhin ein Auslesen einer zusammen mit der Domain gespeicherte Adresse eines Schlüsselservers umfasst, wobei der Server gemäß Anspruch 1 ausgebildet ist.

7. Verfahren nach Anspruch 6, weiterhin umfassend: Auslesen eines dem Nutzer zugeordneten Schlüssel mittels der Adresse des Schlüsselservers von einem Schlüsselserver, Verschlüsseln der Daten mit dem öffentlichen Schlüssel und Übertragen der verschlüsselten Daten an einen zu der Dateneingangsserveradresse zugehörigen Dateneingangsserver.

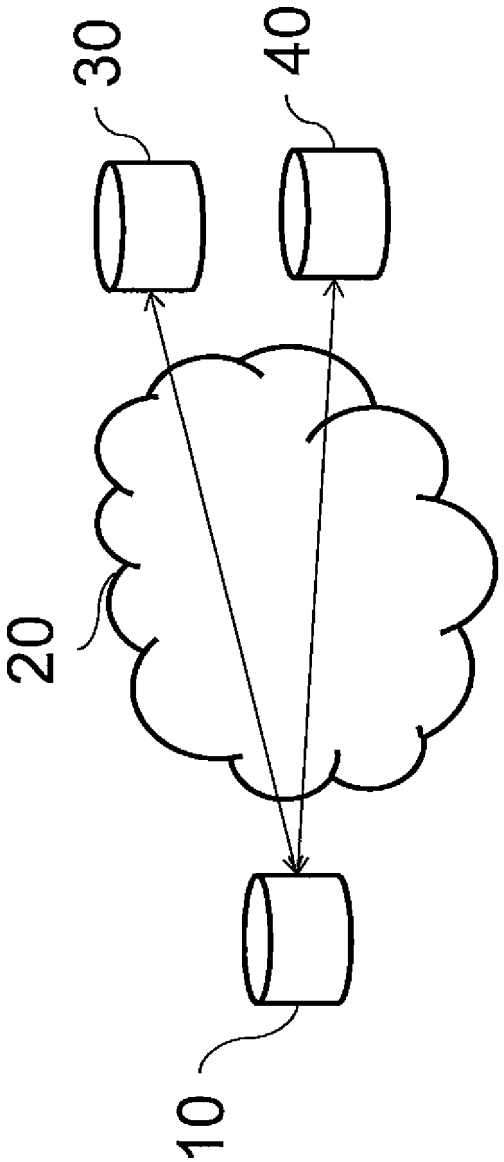
8. Verfahren nach Anspruch 7, weiterhin umfassend:
Herunterladen eines Zertifikats des öffentlichen Schlüssels über das öffentliche Netzwerk und
Überprüfen der Echtheit des öffentlichen Schlüssels anhand des Zertifikats, wobei das Verschlüsseln nach dem Überprüfen und nur dann erfolgt, wenn der öffentliche Schlüssel echt ist.

9. Verfahren nach Anspruch 8, wobei das Zertifikat in einer Verschlüsselung des öffentlichen Schlüssels mit einem privaten Schlüssel besteht und wobei das Überprüfen der Echtheit umfasst:
Entschlüsseln des verschlüsselten öffentlichen Schlüssels mit einem weiteren, zum privaten Schlüssel zugehörigen öffentlichen Schlüssel.

10. Verfahren nach einem der Ansprüche 7 bis 9, wobei die verschlüsselten Daten nach Post Office Protocol (POP), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP) oder Simple Mail Access Protocol (SMAP) übertragen werden.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen



Figur 1