PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :		(11) Internationale Veröffentlichungsnummer: **WO 99/35781**
H04L 9/00	**A2**	(43) Internationales Veröffentlichungsdatum: 15. Juli 1999 (15.07.99)

(21) Internationales Aktenzeichen: PCT/EP98/07984

(22) Internationales Anmeldedatum: 9. Dezember 1998 (09.12.98)

(30) Prioritätsdaten:
198 01 241.1 12. Januar 1998 (12.01.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: MERTES, Paul [DE/DE]; Mertenseifer Grund 9, D–57258 Freudenberg (DE). METTKEN, Werner [DE/DE]; Eichenweg 9, D–59969 Hallenberg (DE).

(74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Technologiezentrum, EK03, D–64307 Darmstadt (DE).

(81) Bestimmungsstaaten: CA, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD FOR GENERATING ASYMMETRICAL CRYPTOGRAPHIC KEYS BY THE USER

(54) Bezeichnung: VERFAHREN ZUR GENERIERUNG ASYMMETRISCHER KRYPTOSCHLÜSSEL BEIM ANWENDER

(57) Abstract

Users need signature and coding keys for generating asymmetrical cryptographic keys. Reliable connections to a trust center are required for personalization and certification. Security problems arise when users wish to generate their own keys, more particularly, cryptographic keys. Said problems are diminished by a method, wherein the user initially receives a generated, personalized and certified pair of keys and components for generating coding pairs from the trust center. At a given moment, the user produces a coding pair of keys, signs the public part of said pair with the secret signature key assigned to him or her and transmits the result to the trust center, where the result is assigned to the user by means of the certified public part of the signature pair of keys. The invention can be particularly applied in all forms of asymmetric cryptographic methods, basically in money cards and bank transactions, access controls to networks and data banks, admission controls to buildings or rooms, digital signatures, digital identification and patient cards.

(57) Zusammenfassung

Bei der Generierung asymmetrischer Kryptoschlüssel in Anwenderhand sind Signatur– und Verschlüsselungsschlüssel und bei der Personalisierung und Zertifizierung zuverlässige Verbindungen zu einem Trust Center erforderlich. Wenn Anwender eigene Schlüssel, insbesondere Kryptoschlüssel, generieren wollen, entstehen Sicherheitsprobleme. Derartige Probleme mindert ein Verfahren, bei dem der Anwender zunächst vom Trust Center ein generiertes, personalisiertes und zertifiziertes Schlüsselpaar sowie Komponenten zur Erzeugung von Verschlüsselungspaaren erhält. Der Anwender erzeugt irgendwann selbst ein Verschlüsselungsschlüsselpaar, signiert den öffentlichen Teil dieses Paares mit dem ihm überlassenen geheimen Signaturschlüssel und übermittelt das Ergebnis zum Trust Center, wo das Ergebnis mittels des zertifizierten öffentlichen Teils des Signaturschlüsselpaares dem Anwender zugeordnet wird. Anwendungsgebiet der Erfindung sind alle Formen asymmetrischer Kryptoverfahren: im wesentlichen Geldkarten/Banktransaktionen, Zugangskontrolle zu Netzwerken/Datenbanken, Zutrittskontrolle zu Gebäuden/Räumen, Digitale Signature, Digitale Ausweise/Patientenkarten.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren zur Generierung asymmetrischer Kryptoschlüssel beim Anwender

Beschreibung:

Die Erfindung bezieht sich auf ein asymmetrisches Kryptoverfahren der im Oberbegriff des Patentanspruchs 1 näher bezeichneten Art. Derartige Verfahren sind vielfach bekannt und z. B. in Menezes: Handbook of applied cryptography 1997 beschrieben.

Ein Kernproblem aller bekannten offenen Kryptoverfahren ist die zuverlässige Zuordnung der eingesetzten Signatur- und Verschlüsselungsschlüssel zum berechtigten Inhaber und die Bestätigung der Zuordnung durch eine unabhängige dritte Instanz. Fachsprachlich ist dies die Frage einer zuverlässigen Personalisierung der Schlüssel mit anschließender Zertifizierung.

Vertrauenswürdige Verfahren, wie z. B. von Kowalski, in Der Fernmeldeingenieur 4/5 1995,: „Security Management System" beschrieben, lösen dies heute, indem solche Schlüssel an zentraler, besonders abgesicherter Stelle (meist sogenannte Trust Center) generiert, personalisiert und zertifiziert werden.

Es ist jedoch nicht auszuschließen, daß die Anwender ihre Kryptoschlüssel, insbesondere jene zur Verschlüsselung, zukünftig zunehmend selbst generieren wollen. Dieser Wunsch darf dabei nicht auf Kosten der Sicherheit und Zuverlässigkeit des jeweiligen Verfahrens realisiert werden, wie dies heute bei nur lose organisierten asymmetrischen Kryptoverfahren des Internet der Fall ist.

Als Aufgabe der Erfindung bedarf es somit eines Verfahrens, welches die Schlüsselgenerierung in den Verantwortungsbereich der Anwender verlagert, ohne auf die organisatorische Sicherheit einer unabhängigen Instanz zu verzichten.

Diese Aufgabe wird mit dem im Kennzeichen des Patentanspruchs 1 aufgeführten Verfahren gelöst.

Vorteilhafte Weiterbildungsmöglichkeiten sind aus dem Kennzeichen des Unteranspruchs 2 ersichtlich.

Die Erfindung wird anhand des nachfolgenden Ausführungsbeispiels näher erläutert:

Der Anwender erhält von zentraler Stelle, nachfolgend allgemein als Trust Center bezeichnet, ein bereits generiertes personalisiertes und zertifiziertes Signaturschlüsselpaar, z. B. ein privater Signaturschlüssel PS und ein öffentlicher Signaturschlüssel ÖS sowie die Komponenten zur Erzeugung eines oder mehrerer Verschlüsselungsschlüsselpaare Generate Encryption Keys GEK.

Der Anwender erzeugt nun irgendwann selbst ein Verschlüsselungsschlüsselpaar, z. B. einen privaten Verschlüsselungsschlüssel PVS, signiert den öffentlichen Teil dieses Paares, den öffentlichen Verschlüsselungsschlüssel ÖVS mit dem zuvor überlassenen geheimen Signaturschlüssel PS, und übermittelt das Ergebnis an das Trust Center. Dort ist das Ergebnis über eine Prüfung mit Hilfe des zertifizierten öffentlichen Teiles des Signaturschlüsselpaares des Anwenders ÖS zweifelsfrei und zuverlässig als dem Anwender gehörend zuzuordnen.

Das Trust Center erzeugt daraufhin ein neues Zertifikat, in dem entweder sowohl der öffentliche Teil des Signaturschlüsselpaares ÖS als auch der des Verschlüsselungsschlüsselpaares ÖVS, oder nur der des Verschschlüsselungsschlüsselpaares des Anwenders ÖVS enthalten sind.

Dieses Zertifikat wird im nächsten Schritt mit dem öffentlichen Teil des Verschlüsselungsschlüsselpaares des Anwenders ÖVS verschlüsselt und dann übermittelt.

Damit ist sichergestellt, daß nur der berechtigte Anwender das Zertifikat entschlüsseln und, bei hardwarebasierten Systemen, in seine korrespondierende Hardware herunterladen kann. Der Anwender mußte zu keinem Zeitpunkt sein Geheimnis, nämlich den geheimen Teil des Verschlüsselungsschlüsselpaares PVS preisgeben.

Will der Anwender zusätzlich auch noch das Signaturschlüsselpaar in seinem Verantwortungsbereich erzeugen, also auch den geheimen Teil eines Signaturschlüsselpaares, einen zweiten privaten Signaturschlüssel PS2, vor dem Zugriff des Trust Center schützen, so wird dieses Verfahren auch dafür analog eingesetzt. Dem Anwender werden nur noch zusätzlich die Komponenten Generate Digital Signature Keys GDSK zur Erzeugung eines oder mehrerer Signaturschlüsselpaare überlassen.

Einmal erzeugt, signiert der Anwender, unter Zuhilfenahme des vom Trust Center überlassenen geheimen Signaturschlüssels PS, neben oder zugleich mit dem öffentlichen Teil des selbst generierten Verschlüsselungspaares ÖVS, auch noch den öffentlichen Teil des selbst generierten Signaturschlüsselpaares ÖS2 und übermittelt das Ergebnis an das

Trust Center, wo danach ebenso wie oben beschrieben, weiter verfahren wird.

Soweit der Anwender AW1 überhaupt keine Kommunikation mehr mit einem Trust Center wünscht, kann er auch dies mit dem beschriebenen Verfahren ohne Verlust an Zuverlässigkeit tun, indem er bei jeder bilateralen Kommunikation mit einem anderen Anwender AW2 dem Kommunikationspartner zunächst den öffentlichen Teil seines selbst generierten Schlüsselpaares ÖVS mit dem geheimen Teil des zuvor vom Trust Center überlassenen, personalisierten und zertifizierten Schlüsselpaares PS signiert und zustellt.

Der empfangende Kommunikationspartner AW2 kann die korrekte Zuordnung dieser Information hinsichtlich des öffentlichen Teils ÖVS des vom sendenden Anwenders AW1 selbst generierten Schlüsselpaares durch eine Verifikation der Signatur zuverlässig prüfen und gegebenenfalls die Echtheit und Gültigkeit des dieser Signatur zugrundeliegenden Zertifikates im Trust Center überprüfen.

Patentansprüche:

1. Verfahren zur Generierung asymmetrischer Kryptoschlüssel beim Anwender, bei dem Schlüssel an einer zentralen, besonders abgesicherten Stelle, (Trust Center), bzw. im Zusammenwirken mit gesicherter Übermittlung zwischen dem Anwender und diesem Trust Center, beim Anwender generiert, personalisiert und zertifiziert werden, d a d u r c h g e k e n n z e i c h n e t , daß

a. dem Anwender zuerst vom Trust Center ein bereits generiertes, personalisiertes und zertifiziertes Signaturschlüsselpaar (PS; ÖS) und dazu Komponenten zur Erzeugung eines bzw. mehrerer Verschlüsselungsschlüsselpaare (GEK) zugestellt wird,

b. vom Anwender danach ein weiteres eigenes Verschlüsselungsschlüsselpaar mit einem öffentlichen (ÖVS) und einem geheimen Teil (PVS) erzeugt, und der öffentliche Teil (ÖVS)mit dem zugestellten geheimen Teil (PS) des Signaturschlüssels signiert und das Ergebnis zum Trust Center übermittelt wird,

c. vom Trust Center danach die zweifelsfreie Zuordnung zum Anwender mittels des zertifizierten öffentlichen Teils (ÖS) des Signaturschlüsselpaares geprüft wird,

d. vom Trust Center, nach erfolgreicher Zuordnungsprüfung, unter Verwendung von wenigstens einem öffentlichen Teil des Signaturschlüsselpaares (ÖS) bzw. des Verschlüsselungsschlüsselpaares (ÖVS) des Anwenders ein neues Zertifikat erzeugt wird, und zuletzt

e. vom Trust Center dieses Zertifikat, mit dem öffentlichen Teil des Verschlüsselungsschlüsselpaares (ÖVS) des Anwenders verschlüsselt, zum Anwender übermittelt wird.

2. Verfahren zur Generierung asymmetrischer Kryptoschlüssel beim Anwender nach Anspruch 1, dadurch gekennzeichnet, daß dem Anwender beim Verfahrensschritt a. zusätzlich Komponenten (GDSK) zur Erzeugung eines bzw. mehrerer Signaturschlüsselpaare zugestellt werden, welche beim Verfahrensschritt b. vom Anwender mit erzeugt werden, und daß vom Anwender auch der öffentliche Teil (ÖS2) dieses selbst generierten Signaturschlüsselpaares zugleich bzw. daneben mittels des geheimen Teils des vom Trust Center erhaltenen Signaturschlüsselpaares (PS) signiert wird.

3. Verfahren zur Generierung asymmetrischer Kryptoschlüssel beim Anwender nach Anspruch 1 und 2, dadurch gekennzeichnet, daß ein Anwender (AW1), der überhaupt keine Kommunikation mit einem Trust Center wünscht, bei jeder bilateralen Kommunikation mit einem anderen Anwender (AW2), diesem zunächst den öffentlichen Teil seines selbst generierten Schlüsselpaares (ÖVS bzw. ÖS2) mit dem geheimen Teil des zuvor vom Trust Center überlassenen, personalisierten und zertifizierten Schlüsselpaares (PS) signiert und zustellt, wonach vom empfangenden Anwender (AW2) die korrekte Zuordnung dieser Information hinsichtlich des öffentlichen Teils (ÖVS bzw. ÖS2) des vom sendenden Anwenders (AW1) selbst generierten Schlüsselpaares durch eine Verifikation der Signatur geprüft wird und die Echtheit und Gültigkeit des dieser Signatur zugrundeliegenden Zertifikates im Trust Center überprüft werden kann.