BUNDESPATENTGERICHT

5 W (pat) 1/06

(Aktenzeichen)

B E S C H L U S S

In der Beschwerdesache

…

wegen der Gebrauchsmusteranmeldung 20 2004 012 201.4

(hier: Eintragungsantrag)

hat der 5. Senat (Gebrauchsmuster-Beschwerdesenat) des Bundespatentgerichts am 18. August 2008 durch den Vorsitzenden Richter Müllner sowie die Richter Baumgärtner und Dipl.-Phys. Dr. Hartung

beschlossen:

Die Beschwerde des Anmelders wird zurückgewiesen.

G r ü n d e

I

Die vorliegende Gebrauchsmusteranmeldung ist am 3. August 2004 eingereicht worden. Sie trägt die Bezeichnung "System zur Absicherung der Erstellung von Public-Key-Zertifikaten". Mit der Anmeldung wurden fünf Schutzansprüche eingereicht.

Die Ansprüche lauten:

1. System zur Absicherung der Erstellung von Public-Key-Zertifikaten,
   dadurch gekennzeichnet,
   - dass die Berechnung der Signatur eines Public-Key-Zertifikats und die Bestätigung des Zertifikatsinhalts, über den sich die Signatur erstreckt, gemeinsam von zwei unabhängigen Parteien, darunter eine zentrale Instanz Z und eine von möglicherweise mehreren, Prüfinstanzen P_i (i = 1, 2, 3…), vorgenommen wird,
   - dass Geheimnisanteile des privaten Schlüssels eines kryptografischen Schlüsselpaars (mit öffentlichem Schlüssel pub und privatem Schlüssel priv), mit dem Public-Key-Zertifikate digital signiert werden, zwischen Z und den P_i (i = 1, 2, 3…) verteilt sind,
   - dass diese Geheimnisanteile derart beschaffen sind, dass nur Z und ein P_i (für ein beliebiges i) gemeinsam in der Lage sind, digitale Zertifikate zu erzeugen, die mit priv signiert sind,

- dass weder Z noch eine beliebige Teilmenge von $\{P_i : i = 1, 2, 3,\ldots\}$ in der Lage ist, alleine digitale Zertifikate zu erzeugen, die mit priv signiert sind,
- dass die digitale Signatur des Zertifikats mit Hilfe von pub überprüft werden kann.

2. System nach Anspruch 1, **dadurch gekennzeichnet**,
   - dass das Schlüsselpaar (priv, pub) in einer Weise generiert wird, dass weder Z noch eine Teilmenge von $\{P_i : i = 1, 2, 3,\ldots\}$ Kenntnis von priv erlangt.

3. System nach Anspruch 1, **dadurch gekennzeichnet**,
   - dass zunächst nur Z und P_1 Geheimnisanteile des privaten Schlüssels priv besitzen und diese beiden Parteien Geheimnisanteile für weitere Prüfinstanzen P_i (i = 2, 3, 4, …) erzeugen und an diese verteilen.

4. System nach Anspruch 1, **dadurch gekennzeichnet**,
   - dass das Schlüsselpaar (priv, pub) in einer Weise generiert wird, dass weder Z noch eine beliebige Teilmenge von $\{P_i : i = 1, 2, 3,\ldots\}$ Kenntnis von priv erlangt,
   - dass zunächst nur Z und P_1 Geheimnisanteile des privaten Schlüssels priv besitzen und diese beiden Parteien Geheimnisanteile für weitere Prüfinstanzen P_i (i = 2, 3, 4, …) erzeugen und an diese verteilen.

5. System nach Anspruch 1, 2, 3 oder 4, **dadurch gekennzeichnet**,
   - dass es sich derart in bestehende Abläufe eines Trustcenters integriert, dass die Zertifizierungsinstanz des Trustcenters (CA) in der Rolle von Z agiert,
   - dass die Registrierungsstellen (zur Unterscheidung bezeichnet mit RA_i (i = 1, 2, 3,…)) um eine Komponenten zum Gegenzeichnen (GA_i (i = 1, 2, 3,…)) erweitert werden, um ihnen die Funktionalität einer Prüfinstanz P_i zu geben,
   - dass RA_i (i = 1, 2, 3,…) jeweils ein Geheimnisanteil K'_i von priv zugeordnet ist,
   - dass - nachdem sie einen Certification Request von RA_i erhalten hat - die CA statt mit priv mit einem geeigneten Teilschlüssel K_i signiert, der von der RA abhängt, die den Antrag geprüft hat (ausgedrückt durch den Index i),
   - dass das mit K_i teilsignierte Zertifikat zwischengespeichert wird und dann durch Gegenzeichnen mit dem zu K_i passenden Geheimnisanteil K'_i (der zusammen mit K_i den privaten Schlüssel priv ergibt) eine gültige Signatur erhält, die mit pub überprüft werden kann.

Die Anmeldung wurde mit Beschluss vom 6. Oktober 2005 von der Gebrauchsmusterstelle des Deutschen Patent- und Markenamts mit der Begründung zurückgewiesen, dass sie auf einen Gegenstand gerichtet sei, der dem Gebrauchsmusterschutz nicht zugänglich sei, weil es sich hierbei um keine Erfindung auf dem Gebiet der Technik handle.

Gegen diesen Beschluss wendet sich die Beschwerde des Anmelders vom 12. Dezember 2005. In der Begründung der Beschwerde vom 15. April 2007 führt der Anmelder an, dass die Anmeldung das konkrete - und technische - Problem löse, zum Zwecke der Risikominimierung gewisse Sicherheitsziele in einer Public-Key-Infrastruktur (PKI) durchzusetzen. Die Erfindung löse das vorgenannte Problem mit einer nachweislich höheren Sicherheit, die mathematisch beweisbar ist und damit nicht auf Erfahrungswerten, Annahmen (der praktisch nicht zu erzielenden) Fehlerfreiheit von Software oder dergleichen beruht, und außerdem effektiver, da mit niedrigeren Kosten eine angestrebte Sicherheit erlangt werden kann. Zur Gewährleistung dieser Sicherheitsziele würden nach dem Stand der Technik insbesondere – technische - Mittel eingesetzt, wie spezielle Hardware, vom Netzwerk getrennte Rechner, bauliche Schutzvorrichtungen etc., des Weiteren werde ein hoher Aufwand betrieben, um den vorgeschriebenen Prozessablauf durchzusetzen sowohl mit technischen (z. B. feste Vorgabe durch Trustcenter-Software) als auch mit organisatorischen Mitteln (z. B. Rollentrennung zwischen beteiligten Mitarbeitern). Die mit der Anmeldung beschriebene Erfindung erlaube die verteilte Speicherung und Verwendung eines Zertifizierungsschlüssels und das Erzwingen des Zusammenwirkens von beteiligten Mitarbeitern bei der Teilnehmerregistrierung und Zertifikatsausstellung auf eine Standard-konforme, für Anwender (Zertifikatsinhaber sowie prüfende Parteien) völlig transparente und damit konkret einsetzbare Weise. Bei einem Einsatz der Erfindung bei einem Zertifizierungsdiensteanbieter (ZDA) gelte insbesondere, dass - bei einer verteilten Speicherung der Teile des Zertifizierungsschlüssels - ein Angreifer an zwei geographisch auseinander liegenden Standorten erfolgreich sein müsste (wogegen Maßnahmen in einer niedrigeren Schutzklasse an einem einzelnen Standort ausreichend wären), ein Angreifer allein könnte es nicht schaffen, sich über das erfindungsgemäße Vier-Augen-Prinzip hinwegzusetzen, dies beruhe auf beweisbaren mathematischen Eigenschaften.

Bzgl. des Einsatzes beherrschbarer Naturkräfte verweist der Anmelder auf die Anmeldeunterlagen. Dort werde insbesondere beschrieben, wie die in den Schutzansprüchen erwähnten Parteien den Komponenten einer konkreten Public Key-Infrastruktur zugeordnet werden können und wie sich die Erfindung konkret in Abläufe eines bestehenden Zertifizierungsdiensteanbieters integrieren lässt. Auch können - nach dem Stand der Technik und Wissenschaft - bekannte Methoden zur Schlüssel- und Signatur-Erzeugung sowie der Geheimnisverteilung verwendet werden, und es werde aufgezeigt, wie ein Computersystem modifiziert werden muss, um die Erfindung praktisch umzusetzen.

Der Anmelder beantragt sinngemäß,

> den Beschluss des Deutschen Patent- und Markenamtes vom 6. Oktober 2005 aufzuheben und die Eintragung des Gebrauchsmusters 20 2004 012 201 zu verfügen.

II

Die zulässige Beschwerde ist nicht begründet. Dem Antrag auf Eintragung eines Gebrauchsmusters nach § 8 Abs. 1 GebrMG war nicht zu folgen, da der mit der Anmeldung beanspruchte Gegenstand keine Erfindung im Sinne des § 1 Abs. 1 GebrMG ist.

1. In der Beschreibungseinleitung der Anmeldung sind die Komponenten einer Public-Key-Infrastruktur beschrieben, umfassend im Wesentlichen eine Zertifizierungsstelle (certification authority, CA), eine oder mehrere Registrierungsstellen (registration authority, RA) und einen Verzeichnisdienst (directory, DIR), vgl. Anmeldeunterlagen Seite 3. Es folgt die Beschreibung eines typischen Prozesses der Erstellung von Public-Key-Zertifikaten unter Beteiligung der vorgenannten Komponenten, Seite 4. Im Anschluss an die Schilderung bestehender Sicherheitsrisiken (Seite 5) wird schließlich das nötige Zusammenwirken von Registrierungsstellen

und Zertifizierungsstelle bei der Erstellung eines Zertifikats beschrieben mit dem Ziel, die Erstellung von Public-Key-Zertifikaten abzusichern (Seite 6, Abschnitt 1.4), letzteres soll durch die Erfindung nach Schutzanspruch 1 sichergestellt werden.

Demgemäß ist Schutzanspruch 1 auf ein System zur Absicherung der Erstellung von Public-Key-Zertifikaten gerichtet. Die Berechnung der Signatur eines Public-Key-Zertifikats und die Bestätigung des Zertifikatsinhalts, über den sich die Signatur erstreckt, soll gemeinsam von zwei unabhängigen Parteien, darunter eine zentrale Instanz *Z* und eine von möglicherweise mehreren Prüfinstanzen P_i (i = 1, 2, 3...) vorgenommen werden. Die Geheimnisanteile des privaten Schlüssels eines kryptografischen Schlüsselpaars (mit öffentlichem Schlüssel pub und privatem Schlüssel priv), mit dem die Public-Key-Zertifikate digital signiert werden, sind zwischen *Z* und den P_i (i = 1, 2, 3...) verteilt und sind derart beschaffen, dass nur *Z* und ein P_i (für ein beliebiges i) gemeinsam in der Lage sind, digitale Zertifikate zu erzeugen, die mit priv signiert sind. Weder Z noch eine beliebige Teilmenge von $\{P_i : i = 1, 2, 3,\ldots\}$ ist in der Lage, alleine digitale Zertifikate zu erzeugen, die mit dem privaten Schlüssel priv signiert sind. Schließlich soll die digitale Signatur des Zertifikats mit Hilfe des öffentlichen Schlüssels pub überprüft werden können.

Der Fachmann, hier ein Informatiker mit Hochschulausbildung mit besonderer Erfahrung auf dem Gebiet der Kryptologie und den damit verbundenen mathematischen Methoden und deren Umsetzung mittels Computern, entnimmt im Lichte der Beschreibung (vgl. insbesondere die Seiten 6 bis 10 der Anmeldeunterlagen) dem Schutzanspruch 1, dass die Erstellung von Public-Key-Zertifikaten dadurch abgesichert werden kann, dass die Berechnung der Signatur eines Public-Key-Zertifikats und die Bestätigung des Zertifikatsinhalts, über den sich die Signatur erstreckt, gemeinsam von zwei unabhängigen Parteien vorgenommen wird. Dabei werden die Public-Key-Zertifikate digital signiert mit auf den Parteien verteilten Geheimnisanteilen des privaten Schlüssels eines kryptografischen Schlüsselpaars. Diese Geheimnisanteile sind derart beschaffen, dass nur entsprechend ausge-

wählte Parteien die digitalen Zertifikate erzeugen, signieren und überprüfen können (Vier-Augen-Prinzip). Das im Schutzanspruch 1 angegebene System und die davon umfassten Parteien und Prüfinstanzen versteht der Fachmann als Datenverarbeitungssystem, das Rechner (Server, Clients) und Netzwerke umfasst und mit der erforderlichen Software ausgestattet ist, um die vorgenannten Berechnungs- und Verarbeitungsvorgänge auszuführen. Mit dem solcherart beanspruchten System soll das beabsichtigte Vier-Augen-Prinzip bei der Erstellung eines Zertifikats sichergestellt werden (Seite 6, dritter Absatz).

2. Die mit dem Schutzanspruch 1 beanspruchte Lehre liegt nicht auf technischem Gebiet.

Dem Gebrauchsmusterschutz sind ebenso wie dem Patentschutz nur Erfindungen zugänglich, die auf technischem Gebiet liegen, vgl. § 1 Abs. 1 i. V. m. Abs. 2 und 3 GebrMG. In der Entscheidung "Suche fehlerhafter Zeichenketten" hat der Bundesgerichtshof zu computerbezogenen (Patent-) Anmeldungen hervorgehoben, dass in Hinblick auf die für eine Erfindung erforderliche Technizität eine Gesamtbetrachtung darüber zu fordern ist, was nach der beanspruchten Lehre im Vordergrund steht (Mitt. 2001, 553, 555 m. w. N.; ergänzend: BPatG 5 W (pat) 6/03, 28. Juli 2004, BlPMZ 2005, 227-230 - Internet-Befragung).

a) Im Vordergrund der hier vorliegenden Anmeldung steht, wie auch durchgängig in der Beschreibung abgehandelt (vgl. vorstehend unter Abschnitt **1.**), das Problem der Absicherung der Erstellung von Public-Key-Zertifikaten. Diese Problemstellung liegt nicht auf technischem Gebiet. Eine konkrete technische Problemstellung, wie sie nach der Rechtsprechung des Bundesgerichtshofs für eine auf technischem Gebiet liegende Lehre vorauszusetzen ist (vgl. "Suche fehlerhafter Zeichenketten" a. a. O., Leitsatz 1), ergibt sich weder aus der Beschreibung noch aus den Schutzansprüchen.

Der mit dem Schutzanspruch 1 beanspruchte Gegenstand (vgl. ebenfalls unter Abschnitt **1.**) ist nicht von technischen Problemstellungen geprägt, sondern durch Überlegungen, wie die Erstellung von Public-Key-Zertifikaten abgesichert werden kann, indem insbesondere die Berechnung der Signatur eines Public-Key-Zertifikats und die Bestätigung des Zertifikatsinhalts und weiter die Beschaffenheit der Geheimnisanteile kryptografischer Schlüssel festgelegt werden. Derartige Überlegungen sind nicht dem Gebiet der Technik zuzuordnen, sondern betreffen die dem Gebiet der Kryptologie zugrunde liegenden mathematischen Methoden als solche, wie die Berechnung von – digitalen – Signaturen und Schlüsseln und die zugehörigen Verschlüsselungsverfahren.

b) Dabei wird nicht verkannt, dass zur Ausführung und Auswertung der nicht auf technischem Gebiet liegenden Lehre technische Mittel zum Einsatz kommen. Zweifellos wird der vorgenannte Fachmann bei der Absicherung der Erstellung von Public-Key-Zertifikaten gemäß der Lehre des Schutzanspruchs 1 auch technische Mittel in Anschlag bringen, insbesondere zur Berechnung der Signaturen und Schlüssel und zu deren Verteilung, Signierung und Überprüfung. Das mit Schutzanspruch 1 beanspruchte System umfasst Rechner (Server, Clients) und Netzwerke und ist mit der erforderlichen Software ausgestattet, um die in Schutzanspruch 1 genannten Berechnungs- und Verarbeitungsvorgänge auszuführen.

Der Umstand, dass technische Mittel zur Ausführung einer nichttechnischen Lehre zum Einsatz kommen, führt aber nicht zwangsläufig dazu, dass diese Lehre als dem Gebrauchsmusterschutz zugänglich anzusehen ist. Gemäß den vom Gebrauchsmusterschutz ausgenommenen Gegenständen nach § 1 Abs. 2 und 3 GebrMG - entsprechend nach § 1 Abs. 2 und 3 PatG – insbesondere gemäß den Schutzverboten für mathematische Methoden als solche oder auch für Computerprogramme als solche, verbietet es sich, bereits jedwede in computergerechte Anweisungen gekleidete Lehre als schutzfähig zu erachten. Nur wenn die prägenden Anweisungen der beanspruchten Lehre der Lösung eines konkreten technischen Problems dienen, kann eine solche Schutzfähigkeit gegeben sein (vgl. einmal

mehr BGH "Suche fehlerhafter Zeichenketten" a. a. O., insbesondere Leitsatz 1). Letzteres ist jedoch, wie vorstehend aufgezeigt, hier nicht der Fall. Der Schutzanspruch 1 lässt auch unter Berücksichtigung des nicht näher spezifizierten Systems und – möglicherweise - davon umfasster Parteien und Prüfinstanzen keine auf technischem Gebiet liegende Besonderheit bei der Implementierung der - nicht technischen - Lehre zur Absicherung der Erstellung von Public-Key-Zertifikaten erkennen.

c) Der Anmelder macht hiergegen vergeblich geltend, dass die Erfindung es gestatte, Sicherheitsziele in einer Public-Key-Infrastruktur mit einer nachweislich höheren, mathematisch beweisbaren Sicherheit durchzusetzen. Dem mag zwar im Ergebnis beizupflichten sein, jedoch sind die der Erfindung zugrunde liegenden Überlegungen, wie vorstehend dargelegt, nicht dem Gebiet der Technik zuzuordnen, sondern betreffen die dem Gebiet der Kryptologie zugrunde liegenden mathematischen Methoden. Auch der Einsatz von technischen Mitteln, wie Rechnern, Netzwerken, baulicher Schutzvorrichtungen, kann vorliegend das Vorliegen einer technischen Erfindung nicht begründen, nachdem die prägenden Anweisungen der beanspruchten Lehre nicht dem Gebiet der Technik zuzuordnen sind und auch keine auf technischem Gebiet liegende Besonderheit bei der Implementierung der nicht technischen Lehre zur Absicherung der Erstellung von Public-Key-Zertifikaten ersichtlich ist. Auch die verteilte Speicherung und erfindungsgemäße Verwendung eines Zertifizierungsschlüssels lassen solche Besonderheiten nicht erkennen. Gleiches gilt auch bzgl. eines vorgeschriebenen organisatorischen und software-basierten Prozessablaufs, insbesondere, wenn es darum geht, die Erfindung in Abläufe eines bestehenden Zertifizierungsdiensteanbieters oder Trustcenters zu integrieren.

3. Auch die mit den untergeordneten Ansprüchen 2 bis 5 beanspruchten Ausprägungen des Systems zur Absicherung der Erstellung von Public-Key-Zertifikaten nach dem Schutzanspruch 1 liegen nicht auf technischem Gebiet. Denn diese Ansprüche betreffen Ausbildungen der Lehre nach dem Anspruch 1, die ebenfalls

nicht als technische Erfindung i. S. d. § 1 Abs. 1 GebrMG anerkannt werden können. Auch ist aus den beanspruchten Sachverhalten keine besondere Ausbildung des Systems gemäß den Schutzansprüchen 2 bis 5 in technischer Hinsicht erkennbar.

Die Ansprüche 2 bis 4 befassen sich insbesondere damit, wie Schlüsselpaare (priv, pub) aus privaten und öffentlichen Schlüsseln generiert werden und welche Parteien Geheimnisanteile des privaten Schlüssels besitzen und für weitere Prüfinstanzen erzeugen und an diese verteilen. Derartige Überlegungen sind ebenfalls nicht dem Gebiet der Technik zuzuordnen, sondern betreffen ebenfalls die dem Gebiet der Kryptologie zugrunde liegenden mathematischen Methoden, wie die Generierung von Schlüsseln und deren Geheimnisanteilen und deren Behandlung durch die zugehörigen Instanzen.

Schutzanspruch 5 befasst sich mit der Integration des Systems nach den Schutzansprüchen 1, 2, 3 oder 4 in die bestehenden Abläufe eines Trustcenters, dahingehend dass die Zertifizierungsinstanz des Trustcenters (CA) in der Rolle der zentralen Instanz Z agiert. Das soll insbesondere dadurch geschehen, dass Funktionalitäten, wie Signierung, Prüfung und Speicherung, der (Teil-) Signaturen, des in Rede stehenden Systems an die beteiligten Instanzen verteilt werden. Zwar mag der Fachmann zur Durchführung dieser Funktionalitäten auch technische Mittel, wie bspw. Rechner mit Speichern und Netzwerke einsetzen, jedoch ist auch der mit dem Schutzanspruch 5 beanspruchte Gegenstand nicht von technischen Problemstellungen geprägt, sondern durch Überlegungen, wie die Erstellung von Public-Key-Zertifikaten abgesichert werden kann, indem insbesondere die Berechnung der Signatur eines Public-Key-Zertifikats und die Bestätigung des Zertifikatsinhalts und die Überprüfung der Geheimnisanteile kryptografischer Schlüssel in die Abläufe eines Trustcenters integriert werden können. Derartige Überlegungen sind nicht dem Gebiet der Technik zuzuordnen, sondern betreffen einmal mehr die der Kryptologie zugrunde liegenden mathematischen (Rechen- und Verschlüsselungs-) Methoden.

Auch in den untergeordneten Ansprüchen 2 bis 5 kann somit keine auf technischem Gebiet liegende Lehre erkannt werden, die über die Lehre zur Absicherung der Erstellung von Public-Key-Zertifikaten gemäß Schutzanspruch 1 hinausginge. Noch weniger kann erkannt werden, dass die prägenden Anweisungen eines dieser Ansprüche auf die Lösung eines konkreten technischen Problems gerichtet sind. Eine durch technische Gesichtspunkte bestimmte Problemlösung ist auch unter Berücksichtigung der Beschreibung nicht ersichtlich.

4. In Anbetracht der Sachlage kann die Frage dahinstehen, ob mit dem System nach dem Schutzanspruch 1 ein Verfahren beansprucht wird und demnach ein Schutzausschluss nach § 2 Nr. 3 GebrMG vorliegt.

Müllner Baumgärtner Dr. Hartung

Pü