

Interner Verteilerschlüssel:

- (A) [-] Veröffentlichung im ABl.
- (B) [-] An Vorsitzende und Mitglieder
- (C) [-] An Vorsitzende
- (D) [X] Keine Verteilung

**Datenblatt zur Entscheidung
vom 15. November 2013**

Beschwerde-Aktenzeichen: T 1284/10 - 3.5.03

Anmeldenummer: 02742989.3

Veröffentlichungsnummer: 1393526

IPC: H04L29/06, G07F7/10

Verfahrenssprache: DE

Bezeichnung der Erfindung:

Verfahren zur Schlüsselgenerierung für Signaturkarten

Anmelder:

Giesecke & Devrient GmbH

Stichwort:

parallele Schlüsselgenerierung/GIESECKE

Relevante Rechtsnormen:

EPÜ Art. 56

Schlagwort:

Erfinderische Tätigkeit - (nein)

Zitierte Entscheidungen:

Orientierungssatz:



**Beschwerdekammern
Boards of Appeal
Chambres de recours**

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Beschwerde-Aktenzeichen: T 1284/10 - 3.5.03

**E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.03
vom 15. November 2013**

Beschwerdeführerin: Giesecke & Devrient GmbH
(Anmelderin) Prinzregentenstrasse 159
81677 München (DE)

Angefochtene Entscheidung: Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 21. Januar 2010 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 02742989.3 aufgrund des Artikels 97 (2) EPÜ zurückgewiesen worden ist.

Zusammensetzung der Kammer:

Vorsitzender: F. van der Voort
Mitglieder: B. Noll
R. Menapace

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung der Prüfungsabteilung über die Zurückweisung der europäischen Patentanmeldung Nr. 02742989.3, die als internationale Anmeldung eingereicht und unter dem Aktenzeichen WO 02/093868 A1 veröffentlicht wurde. Die angefochtene Entscheidung stützte sich darauf, dass der Gegenstand eines unabhängigen Anspruchs 1 nicht auf einer erfinderischen Tätigkeit beruhte (Artikel 52 (1), 56 und 97 (2) EPÜ).

II. In der Beschwerdeschrift beantragte die Beschwerdeführerin, die angefochtene Entscheidung aufzuheben und ein Patent "im beantragten Umfang" zu erteilen. Hilfsweise wurde die Anberaumung einer mündlichen Verhandlung beantragt.

In der Beschwerdebegründung beantragte die Beschwerdeführerin, ein Patent auf der Grundlage der gültigen Unterlagen zu erteilen.

III. In einer Mitteilung, die zusammen mit der Ladung zur mündlichen Verhandlung erging, wies die Kammer auf die in der mündlichen Verhandlung zu erörternden Punkte hin, insbesondere die erfinderische Tätigkeit des Verfahrens gemäß Anspruch 1. Es wurde auf die folgenden Druckschriften verwiesen:

D1: WO 99/19846 A2

D3: W. Rankl et al.: "Handbuch der Chipkarten",
3. Auflage (1999), Seiten 582 bis 584.

IV. Die mündliche Verhandlung vor der Kammer fand am 15. November 2013 statt.

Die Beschwerdeführerin beantragte, die angefochtene Entscheidung aufzuheben und ein Patent auf Grundlage der der angefochtenen Entscheidung zugrundeliegenden Ansprüche zu erteilen.

V. Nach Schließen der Debatte und interner Beratung der Kammer wurde die Entscheidung verkündet.

VI. Anspruch 1 lautet:

"Verfahren zur Erzeugung eines Signaturschlüssels für eine Signaturkarte (11), mit folgenden Verfahrensschritten:

- Erzeugen eines geheimen Schlüssels in einer Schlüsselgenerierungseinheit (21),
 - Erzeugen eines Sitzungsschlüssels durch die Schlüsselgenerierungseinheit (21) und die Signaturkarte,
 - verschlüsselte Übertragung des erzeugten Schlüssels an die Signaturkarte
- dadurch gekennzeichnet, dass mehrere Schlüsselgenerierungseinheiten (21) parallel betrieben werden, wobei die Koordination einer zugeordneten Personalisierungsvorrichtung (1) zu den Schlüsselgenerierungseinheiten (21) durch einen Steuerrechner 3 erfolgt."

Entscheidungsgründe

1. *Anspruch 1 - erfinderische Tätigkeit (Artikel 56 EPÜ)*

1.1 Die Druckschrift D1 offenbart ein Verfahren zur Personalisierung von Signaturkarten, bei dem geheime Schlüssel erzeugt und auf sichere Art an die Signaturkarte übertragen werden. Das System zur Schlüsselerzeugung und Personalisierung, durch welches

das Verfahren durchgeführt wird, ist in der Figur 1 von D1 schematisch dargestellt; in seinem Konzept entspricht es den Ausführungen auf Seite 1, Zeile 26 bis Seite 2, Zeile 3 der Anmeldung, wonach Schlüssel erzeugt, in Form einer Ausgangsdatei an eine Personalisierungseinrichtung weitergereicht und durch diese in eine Signaturkarte eingeschrieben werden. Im Einzelnen werden bei dem aus D1 bekannten Verfahren ein geheimer Schlüssel durch ein Sicherheitsmodul ("Hardware security module" (HSM) 130) erzeugt (Seite 9, Zeilen 25 bis 30). Die Schlüsselgenerierungseinheit 130 dient auch zur Erzeugung von Sitzungsschlüsseln ("Hardware security module (HSM) 130 ... generates session keys", vgl. Seite 9, Zeilen 16 bis 18). Der geheime Schlüssel erreicht als Bestandteil der geheimen Daten in der Ausgangsdatei 160 (vgl. Seite 19, Zeilen 21 bis 23, "It should be appreciated that ... keys for an application may be stored within field 636 ..." sowie Fig. 5A-5D) das Sicherheitsmodul (HSM 152) und wird von diesem Modul unter Verwendung eines der Signaturkarte bekannten Sitzungsschlüssels verschlüsselt an die Signaturkarte übertragen. Die beiden Module 130 und 152 in D1 stellen somit eine Schlüsselgenerierungseinheit im Sinn des Anspruchs 1 dar. Somit sind die Merkmale des Oberbegriffs des Anspruchs 1 aus D1 bekannt. Dies wurde von der Beschwerdeführerin auch nicht in Frage gestellt.

- 1.2 Das beanspruchte Verfahren unterscheidet sich von dem aus D1 bekannten Verfahren dadurch, dass mehrere Schlüsselgenerierungseinheiten parallel betrieben werden, wobei die Koordination einer zugeordneten Personalisierungsvorrichtung zu den Schlüsselgenerierungseinheiten durch einen Steuerrechner erfolgt.

Durch eine Parallelisierung der Schlüsselerzeugung wird zunächst die Produktionskapazität bei der Schlüsselerzeugung selbst erhöht. Ist, wie in D1 bereits angedeutet (vgl. Seite 2, Zeile 25 bis Seite 3, Zeile 7), beim Personalisierungsprozess die Erzeugung der geheimen Schlüssel das produktionsbegrenzende Element, so kann aufgrund einer parallelen Erzeugung von Schlüsseln die Produktionskapazität bei der Personalisierung insgesamt gesteigert werden. Ausgehend von D1 und unter Berücksichtigung der unterscheidenden Merkmale stellt sich dem Fachmann somit die technische Aufgabe, die Produktionskapazität der Personalisierung von Signaturkarten zu steigern.

- 1.3 Auf dem Gebiet der Produktion von Signaturkarten ist es fachüblich, zur Steigerung der Produktionskapazität bestimmte Produktionsschritte zu parallelisieren. Insbesondere offenbart D3 hierzu (vgl. auf Seite 583 das Bild 10.34 sowie den nachfolgenden Text), die Initialisierung, also den der Personalisierung vorausgehenden Produktionsschritt, zu parallelisieren, indem einerseits mehrere Initialisierungsmaschinen parallel betrieben werden und andererseits innerhalb einer Maschine mehrere Karten parallel initialisiert werden. Der Fachmann würde auch eine Parallelisierung der Schlüsselproduktion bei der Personalisierung in Betracht ziehen, falls die Schlüsselproduktion der Produktionsengpass bei der Personalisierung wäre, und würde hierzu in naheliegender Weise mehrere Schlüsselgenerierungseinheiten parallel betreiben. Weiterhin ist die reine Idee, innerhalb eines Produktionsprozesses mit parallel arbeitenden Maschinen diese Maschinen untereinander oder mit anderen am Produktionsprozess beteiligten Maschinen zu koordinieren, eine übliche Vorgabe, die keiner erfinderischen Überlegungen bedarf. Eine solche

Koordination zwischen parallel arbeitenden Schlüsselgenerierungseinheiten und einer zugeordneten Personalisierungsvorrichtung durch einen Steuerrechner zu implementieren ist für den Fachmann naheliegend, insbesondere da die Schlüsselgenerierungseinheiten selbst als auch die Personalisierungsvorrichtung jeweils eigene Rechner sind bzw. durch einen Rechner gesteuert werden. Somit gelangt der Fachmann ausgehend von D1 und unter Beachtung des durch D3 belegten Fachwissens in naheliegender Weise zu dem beanspruchten Verfahren.

- 1.4 Die Beschwerdeführerin trug in der mündlichen Verhandlung vor, D1 beziehe sich lediglich auf die Schlüsselerzeugung für symmetrische Verschlüsselung, für die ein Schlüssel auf einfache Art und Weise und vor allem in kurzer Zeit aus einem Masterschlüssel abgeleitet werden könne und die daher keine aufwendigen, spezialisierten Maschinen benötige. Somit stelle sich dem von D1 ausgehenden Fachmann nicht das Problem einer aufgrund der Schlüsselerzeugung beschränkten Produktionskapazität. Der Fachmann werde auch unter Beachtung von D3 nicht zu der beanspruchten Lösung geführt. Es werde zwar in D3 vorgeschlagen, die Initialisierung von Signaturkarten zu parallelisieren, jedoch würde der Fachmann auch unter Berücksichtigung dieses Wissens eine Parallelisierung der Schlüsselerzeugung bei der Personalisierung nicht in Betracht ziehen, da die Personalisierung besonderen Sicherheitsanforderungen unterliegt. Deswegen fehle im Stand der Technik auch jeglicher Hinweis auf eine mögliche Parallelisierung von Arbeitsschritten bei der Personalisierung. Folglich sei dem Fachmann durch den Stand der Technik nicht nahegelegt, mehrere Schlüsselgenerierungseinheiten parallel zu betreiben und eine zugeordnete Personalisierungsvorrichtung durch

einen Steuerrechner zu diesen Einheiten zu koordinieren.

- 1.5 Diese Argumente überzeugen die Kammer nicht. Zum einen sind im Anspruch 1 weder die Art der Verschlüsselung, für die der geheime Schlüssel erzeugt wird, noch ein zur Schlüsselerzeugung erforderlicher Aufwand irgendwie spezifiziert und daher bei der Beurteilung der erfinderischen Tätigkeit nicht zu berücksichtigen. Zum anderen ist in dem Verfahren gemäß D1 vorgesehen, dass sowohl symmetrische (vgl. Seite 16, Zeilen 8 bis 15 sowie Figur 3) als auch asymmetrische (vgl. Seite 16, Zeilen 26 bis 29 sowie Figur 4) Schlüssel erzeugt werden. Weiterhin stellt sich dem von D1 ausgehenden Fachmann das Problem, wonach die Erzeugung von Schlüsselpaaren zum Zeitpunkt der Personalisierung die Produktion begrenzen kann, sehr wohl (vgl. Punkt 1.2 oben). Folglich kann sich das beanspruchte Verfahren auch bei expliziter Angabe der Art der Verschlüsselung oder des Aufwands zur Schlüsselerzeugung nicht weiter von D1 unterscheiden. Hinsichtlich des Arguments, auch durch das mit D3 belegte Fachwissen sei für den Fachmann eine Parallelisierung der Schlüsselerzeugung bei der Personalisierung nicht naheliegend, ist es im vorliegenden Fall unerheblich, dass der Fachmann durch den Stand der Technik nicht explizit auf die Möglichkeit, die Schlüsselgenerierung zu parallelisieren, hingewiesen wird. Entscheidend ist vielmehr das Fehlen jeglichen gegenteiligen Hinweises im Stand der Technik, durch den der Fachmann überhaupt davon abgehalten worden wäre, eine Parallelisierung auch der Schlüsselgenerierung zumindest in Erwägung zu ziehen. Daher kann die Kammer nicht nachvollziehen, weshalb der Fachmann dieses allgemein bekannte Prinzip, nämlich einen Produktionsengpass durch eine Parallelisierung des begrenzenden Produktionsschritts

zu vermeiden, bei der Schlüsselerzeugung ausnahmsweise nicht berücksichtigt hätte und demzufolge eine Parallelisierung der Schlüsselerzeugung eine erfinderische Tätigkeit erfordern würde.

- 1.6 Folglich beruht das Verfahren gemäß Anspruch 1 nicht auf einer erfinderischen Tätigkeit (Artikel 56 EPÜ).
2. Da der Anspruch 1 des einzigen Antrags nicht gewärbar ist, muss die Beschwerde zurückgewiesen werden.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

Die Beschwerde wird zurückgewiesen.

Die Geschäftsstellenbeamtin:

Der Vorsitzende:



G. Rauh

F. van der Voort

Entscheidung elektronisch als authentisch bestätigt