BUNDESPATENTGERICHT

20 W (pat) 31/12

_____

(Aktenzeichen)

Verkündet am
3. August 2015
…

B E S C H L U S S

In der Beschwerdesache

betreffend die Patentanmeldung 10 2008 018 001.7-31

…

hat der 20. Senat (Technischer Beschwerdesenat) auf die mündliche Verhandlung vom 3. August 2015 durch den Vorsitzenden Richter Dipl.-Phys. Dr. Mayer, den Richter Dipl.-Ing. Gottstein, die Richterin Kopacek und den Richter Dipl.-Geophys. Dr. Wollny

beschlossen:

Die Beschwerde wird zurückgewiesen.

G r ü n d e

I.

Das Deutsche Patent- und Markenamt - Prüfungsstelle für Klasse H 04 L - hat die am 9. April 2008 eingegangene Patentanmeldung 10 2008 018 001.7 mit der Bezeichnung

„Verfahren und Vorrichtung zur Übertragung von Nachrichten in Echtzeit“

durch Beschluss vom 24. Mai 2012 zurückgewiesen.

Der Zurückweisung lagen die ursprünglich eingereichten Patentansprüche 1 bis 38 zu Grunde.

Die Prüfungsstelle führte in ihrem Zurückweisungsbeschluss insbesondere aus, dass der Gegenstand des Patentanspruchs 1 zwar neu sei, jedoch nicht auf einer erfinderischen Tätigkeit beruhe, denn dem zuständigen Fachmann hätte es unter Zuhilfenahme seines allgemeinen Fachwissens - belegt durch das einschlägige Fachbuch **D5** - bereits vor dem Anmeldetag der vorliegenden Patentanmeldung nahe gelegen, das in der Druckschrift **D4** beschriebene Verfahren wie beansprucht auszugestalten, wobei die genannten zwei Druckschriften im Einzelnen wie folgt lauten:

D4 EP 0 639 907 A1

D5 MENEZES, A. et. al.: Handbook of Applied Cryptography, CRC Press, 1997, Kapitel 1 „Overview of Cryptography“, Seiten 1-48, und Kapitel 11 „Digital Signatures“, Seiten 425-488.

Im Rahmen des Prüfungsverfahrens wurden noch folgende Druckschriften als Stand der Technik genannt:

D1 DE 101 41 737 C1

D2 US 2004 / 0 260 778 A1

D3 KLINGST, H.: Auf dem Weg zum Netz des Vertrauens – Grundlagen und Besonderheiten der Public Key-Verfahren. In: Networking, Datacom 5/00, Seiten 44-46.

Wegen weiterer Einzelheiten wird auf den Beschluss der Prüfungsstelle verwiesen.

Gegen diesen Beschluss richtet sich die am 15. Juni 2012 beim Deutschen Patent- und Markenamt eingegangene Beschwerde.

Die Anmelderin beantragt in der mündlichen Verhandlung vom 9. März 2015:

den Beschluss der Prüfungsstelle für Klasse H 04 L des Deutschen Patent- und Markenamts vom 24. Mai 2012 aufzuheben und das nachgesuchte Patent auf der Grundlage folgender Unterlagen zu erteilen:

Patentansprüche:

Patentansprüche 1 bis 38 vom Anmeldetag, 9. April 2008 (Hauptantrag)

Beschreibung:

Beschreibungsseiten 1 bis 15 vom Anmeldetag, 9. April 2008

Zeichnungen:

Figuren 1 bis 3 vom 15. April 2008

Hilfsantrag:

Patentanspruch 1, überreicht in der mündlichen Verhandlung am 3. August 2015 (Hilfsantrag), restliche Ansprüche und übrige Unterlagen wie Hauptantrag.

Der Patentanspruch 1 gemäß **Hauptantrag** lautet:

" Verfahren zur Übertragung einer Nachricht in Echtzeit zwischen Teilnehmern in einem geschlossenen Netz eines Fahrzeugs (1) mit folgenden Schritten:

(a) Verschlüsseln (S1) von sicherheitsrelevanten Echtzeit-Daten (D) einer Nachricht (N) einschließlich einer Sender-ID (A-ID) eines Senders (3) innerhalb des geschlossenen Netzes mit einem privaten Schlüssel (K_{privA}) des Senders (3) zur Erzeugung einer verschlüsselten Nachricht (N');

(b) Übertragen (S2) der verschlüsselten Nachricht (N') zusammen mit der unverschlüsselten Sender-ID (A-ID) des Senders (3) von dem Sender (3) über einen Fahrzeugbus (2) zu einem Empfänger (4) innerhalb des geschlossenen Netzes;

(c) Entschlüsseln der verschlüsselten Nachricht (N') durch den Empfänger (4) mittels eines öffentlichen Schlüssels ($K_{publicA}$) des durch die empfangene unverschlüsselte Sender-ID A-ID bezeichneten Senders (3) zur Wiedergewinnung der unverschlüsselten Nachricht (N);

(d) Vergleichen der empfangenen Sender-ID (A-ID) mit der in der wiedergewonnenen Nachricht (N)enthaltenen Sender-ID (A-ID') zur Feststellung ob die Übertragung der Nachricht (N) korrekt erfolgt ist. "

Der Patentanspruch 1 gemäß **Hilfsantrag** lautet (unterstrichen die im Vergleich zum Patentanspruch gemäß Hauptantrag neu hinzugetretenen Merkmale):

" Verfahren zur Übertragung einer Nachricht in Echtzeit zwischen Teilnehmern in einem geschlossenen Netz eines Fahrzeugs (1) mit folgenden Schritten:

(a) Verschlüsseln (S1) von sicherheitsrelevanten Echtzeit-Daten (D) einer Nachricht (N) einschließlich einer Sender-ID (A-ID) eines Senders (3) innerhalb des geschlossenen Netzes mit einem privaten Schlüssel (K_{privA}) des Senders (3) zur Erzeugung einer verschlüsselten Nachricht (N'), wobei der private Schlüssel (K_{privA}) von einer Speicherzelle innerhalb eines Speichers (3A) im Sender (3) ausgelesen wird, indem die Sender-ID (A-ID) der zu übertragenden Nachricht N die Speicherzelle adressiert.

(b) Übertragen (S2) der verschlüsselten Nachricht (N') zusammen mit der unverschlüsselten Sender-ID (A-ID) des Senders (3) von dem Sender (3) über einen Fahrzeugbus (2) zu einem Empfänger (4) innerhalb des geschlossenen Netzes;

(c) Entschlüsseln der verschlüsselten Nachricht (N') durch den Empfänger (4) mittels eines öffentlichen Schlüssels ($K_{publicA}$) des durch die empfangene unverschlüsselte Sender-ID A-ID bezeichneten Senders (3) zur Wiedergewinnung der unverschlüsselten Nachricht (N);

(d) Vergleichen der empfangenen Sender-ID (A-ID) mit der in der wiedergewonnenen Nachricht (N) enthaltenen Sender-ID (A-ID') zur Feststellung ob die Übertragung der Nachricht (N) korrekt erfolgt ist. "

Wegen weiterer Einzelheiten wird auf den Akteninhalt verwiesen.

II.

Die zulässige Beschwerde hat keinen Erfolg, da das Verfahren nach Patentanspruch 1 sowohl gemäß Hauptantrag als auch gemäß Hilfsantrag mangels des Zugrundeliegens einer erfinderischen Tätigkeit nicht patentfähig ist (§ 1 Abs. 1 i. V. m. § 4 PatG):

1. Die Patentanmeldung betrifft laut Ursprungsunterlagen, Seite 1, Absatz 2, ein Verfahren und eine Vorrichtung zur Übertragung zwischen Teilnehmern in einem geschlossenen Netz eines Fahrzeugs.

Bei der Datenübertragung in geschlossenen Netzen müsse eine Verzögerung, eine Vertauschung, eine Auslassung von Daten und eine Datenverfälschung vermieden und eine korrekte Übertragung von Daten an den richtigen Empfänger gewährt werden. Fahrzeuge, insbesondere auch schienengebundene Fahrzeuge, verfügten über eine Vielzahl von Komponenten, wie etwa Bremssteuerung, Antriebssteuerung, Sanitäranlagensteuerung oder Klimaanlagensteuerung, die über einen Fahrzeugbus mit einem Server bzw. einer zentralen Steuerung verbunden seien. Jede dieser Komponenten sende und empfange Daten und sei z. B. über einen Ethernet-Bus mit anderen verbunden. Bei sicherheitskritischen Anwendungen in Echtzeit, etwa bei einer Ansteuerung der Bremsen eines Zuges, dürften die Daten, die über den Fahrzeugbus übertragen werden, nicht verfälscht sein, da dies zu einem Zugunglück führen könne (Ursprungsunterlagen, S. 1, Abs. 3).

Herkömmliche Systeme zur Übertragung von Nachrichten in Echtzeit zwischen Teilnehmern in einem geschlossenen Netz eines Fahrzeugs böten lediglich applikative Sicherungsmechanismen, wie beispielsweise CRC (Cyclic Redundancy Check) oder andere Checksummen für die übertragenen Telegramme bzw. Nachrichten. Dies sei problematisch, wenn mehrere und weniger vertrauenswürdige Kommunikationspartner in dem Kommunikationspfad lägen bzw. Netzzugang hätten. Es könne bei herkömmlichen Systemen bei einer Datenverfälschung nicht

nachgewiesen werden, ob diese durch einen internen Fehler oder durch einen systematischen Fehler hervorgerufen worden sei, wobei die empfangene Nachricht von anderen Kommunikationspartnern abgesendet und gegebenenfalls verfälscht worden sei. Insbesondere gegen mutwillige Hackerangriffe böten herkömmliche Systeme keinen ausreichenden Schutz (Ursprungsunterlagen, S. 1, Abs. 4 bis S. 2, Abs. 1).

Der Erfindung liege daher die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zur Übertragung einer Nachricht in Echtzeit zwischen Teilnehmern in einem geschlossenen Netz eines Fahrzeugs zu schaffen, bei der eine Verfälschung der Nachrichten verhindert werde (Ursprungsunterlagen, S. 2, Abs. 2).

2. Die Anmeldung richtet sich ihrem technischen Sachgehalt nach an einen Diplom-Ingenieur der Nachrichtentechnik oder einen Diplom-Informatiker (Univ.), die langjährige Erfahrungen auf dem Gebiet der Kryptographie besitzen. Ihre Fachkenntnisse ergeben sich insbesondere aus dem Lehrbuch MENZES, 1997 (**D5**).

3. Zu den Anträgen

Patentanspruch 1 gemäß Hilfsantrag umfasst Patentanspruch 1 gemäß Hauptantrag, d. h. so wie er mit den Ursprungsunterlagen eingereicht wurde, und ergänzt diesen um ein weiteres Merkmal.

Im Einzelnen lässt sich Patentanspruch 1 gemäß Hilfsantrag wie folgt gliedern (im Vergleich zum ursprünglichen Patentanspruch 1 neue Merkmalsteile mittels Fettdruck hervorgehoben):

1.0 Verfahren zur Übertragung einer Nachricht in Echtzeit zwischen Teilnehmern in einem geschlossenen Netz eines Fahrzeugs (1) mit folgenden Schritten:

1.1 (a) Verschlüsseln (S1) von sicherheitsrelevanten Echtzeit-Daten (D) einer Nachricht (N) einschließlich einer Sender-ID (A-ID) eines Senders (3) innerhalb des geschlossenen Netzes mit einem privaten Schlüssel (K_{privA}) des Senders (3) zur Erzeugung einer verschlüsselten Nachricht (N');

1.1H wobei der private Schlüssel (K_{privA}) von einer Speicherzelle innerhalb eines Speichers (3A) im Sender (3) ausgelesen wird, indem die Sender-ID (A-ID) der zu übertragenden Nachricht N die Speicherzelle adressiert;

1.2 (b) Übertragen (S2) der verschlüsselten Nachricht (N') zusammen mit der unverschlüsselten Sender-ID (A-ID) des Senders (3) von dem Sender (3) über einen Fahrzeugbus (2) zu einem Empfänger (4) innerhalb des geschlossenen Netzes;

1.3 (c) Entschlüsseln der verschlüsselten Nachricht (N') durch den Empfänger (4) mittels eines öffentlichen Schlüssels ($K_{publicA}$) des durch die empfangene unverschlüsselte Sender-ID A-ID bezeichneten Senders (3) zur Wiedergewinnung der unverschlüsselten Nachricht (N);

1.4 (d) Vergleichen der empfangenen Sender-ID (A-ID) mit der in der wiedergewonnenen Nachricht (N) enthaltenen Sender-ID (A-ID') zur Feststellung ob die Übertragung der Nachricht (N) korrekt erfolgt ist.

Die in diesem Anspruch verwendeten Begrifflichkeiten sind – wie auch von der Anmelderin nicht in Abrede gestellt - durch den Fachmann wie folgt auszulegen:

Zwar wird explizit ein Verfahren zur Übertragung einer Nachricht in Echtzeit zwischen Teilnehmern in einem geschlossenen Netz eines Fahrzeugs beansprucht, jedoch kommt es auf die Begriffe „Fahrzeug“ und „geschlossen“ nicht weiter an, da weder der Einsatzort noch das Netz im Anspruch erfindungsrelevant ausgestaltet werden. Folglich ist letzteres allgemein als ein auf seinen Einsatzbereich beschränktes Kommunikationsnetz anzusehen, über das mehrere Sender und Empfänger miteinander digitale Daten (Nachrichten) austauschen können. Der für diesen Datenverkehr eingesetzte Bus (sog. Fahrzeugbus) steht wie beansprucht synonym für das genannte Netz, d. h. das wie auch immer geartete digitale Kommunikationsnetz nutzt zum Datenaustausch ein Bussystem. In diesem Zusammenhang kann die bloße Angabe eines Datentransfers in Echtzeit im Anspruch nur der Hintergrundinformation dienen, Daten im Netz schnellstmöglich zu übermitteln, was letztlich nur den Nutzerwunsch nach entsprechend praxistauglichen Komponenten (Sender, Empfänger, Netze) wiederspiegelt. All diese Angaben zeigen folglich nur Grundvoraussetzungen, die ein Fachmann im Rahmen eines digitalen Kommunikationsnetzes vorzufinden erwartet.

Im Hinblick auf die sicherheitsrelevanten Daten werden die Daten verschlüsselt übertragen, d. h. der Sender verschlüsselt und der Empfänger entschlüsselt die Daten. Die Begriffe privater und öffentlicher Schlüssel bedeuten, dass ein sogenanntes asymmetrisches Verschlüsselungsverfahren mit zwei unterschiedlichen Schlüsseln verwendet werden soll (vgl. Beschreibung S. 14, Z. 4 bis 6): einer zum Verschlüsseln und einer zum Entschlüsseln.

Da das anspruchsgemäße System aus mehreren Teilnehmern besteht, die untereinander kommunizieren sollen, muss jeder Teilnehmer als Sender einen individuellen Schlüssel zum „Verschlüsseln“ (anspruchsgemäß „privater Schlüssel“ genannt) nutzen. Will dieser Sender als Empfänger von einem anderen Teilnehmer im geschlossenen Netz des Fahrzeugs verschlüsselte Nachrichten empfangen und verarbeiten können, muss er von diesem Sender dessen Schlüssel zum „Entschlüsseln“ (anspruchsgemäß „öffentlicher Schlüssel“ genannt) kennen. In der Beschreibung Seite 14 Zeilen 9 bis 11 ist daher ausgeführt: „Jeder an dem Fahrzeugbus 2 angeschlossene Kommunikationsteilnehmer erhält hierzu einen öffentlichen und einen privaten geheimen Schlüssel.“ Gemeint ist hierbei: jedem Teilnehmer ist ein Schlüsselpaar zugeordnet.

Ein asymmetrisches Verschlüsselungsverfahren zwischen zwei Kommunikationsteilnehmern ist dem Fachmann aus dem Lehrbuch MENZES, 1997 (**D5**) Abschnitt 1.8 „Public-Key cryptography“ bekannt. Insbesondere wird dort auch das Prinzip der asymmetrischen Verschlüsselung von digitalen Daten (hier als „public-key technique“ bezeichnet) in einem Kommunikationsnetz beschrieben (vgl. **D5**, S. 26, Figur 1.11 und S. 27, Figur 1.12 mit zugehörigen Figurenbeschreibungen).

Im Einzelnen wird dort auf eine einem ersten Netzwerkteilnehmer („Alice“) als Sender zuzuordnende zu verschlüsselnde - und somit offenbar sicherheitsrelevante – Nachricht („plaintext source“, „m“) eine Verschlüsselungsfunktion („$E_e(m)$“, „public key e“ (hier als „öffentlicher Schlüssel“ bezeichnet)) angewandt („encryption“ i. V. m. **D5**, S. 26, Abs. 2, Z. 1: „... encryption key e need not be kept secret, it may be made public.”). Als Folge hiervon wird die Nachricht in verschlüsselter Form („c“) erhalten („$E_e(m) = c$“), d. h. sicherheitsrelevante Daten einer Nachricht werden mit einem Schlüssel des Senders zur Erzeugung einer verschlüsselten Nachricht verschlüsselt (Merkmal **1.1_{teilw}**).

Anschließend wird die verschlüsselte Nachricht („c“) an einen zweiten Netzwerkteilnehmer („Bob“) als Empfänger über einen Kanal („UNSECURED CHANNEL“) gesendet, d. h. die verschlüsselte Nachricht wird vom Sender über ein Netz zu einem Empfänger übertragen (Merkmal **1.2$_{teilw}$**).

Gemäß Figur 1.11 der Druckschrift **D5** wird die vom Sender („Alice“) zum Empfänger („Bob“) gelangte Nachricht beim Empfänger durch eine sich von der Verschlüsselungsfunktion unterscheidende nur dem Empfänger bekannte Funktion ($D_d(c) = m$“; „private key d“) entschlüsselt („decryption“), um wieder zur Ursprungsnachricht des ersten Teilnehmers („m“) zu gelangen (**D5**, S. 26, Abs. 4, Z. 1 f.: „Public-key encryption, as described here, assumes that knowledge of the public key e does not allow computation of the private key d.“), d. h. die verschlüsselte Nachricht wird durch den Empfänger mittels eines Schlüssels zur Wiedergewinnung der unverschlüsselten Nachricht entschlüsselt, wobei dieser Schlüssel zum Entschlüsseln zu dem Schlüssel des Senders zum Verschlüsseln passen muss (= zusammengehöriges Schlüsselpaar) (Merkmal **1.3$_{teilw}$**).

Steht der Fachmann vor der Aufgabe, das asymmetrische Verschlüsselungsverfahren auf ein System anzuwenden, das aus einer Mehrzahl von Sendern und Empfängern besteht, bei dem aus Sicherheitserwägungen jeder Sender einen eigenen Schlüssel zum Verschlüsseln verwendet, d. h. dass jedem Sender ein Schlüsselpaar zugeordnet ist, ergibt es sich für den Fachmann von selbst, dass einerseits jeder Empfänger die Entschlüsselungsfunktionen zu allen ihm zugeordneten Sendern kennen muss, und dass andererseits der Empfänger zusammen mit der verschlüsselten Nachricht unverschlüsselt die zugehörige Sender-ID erhalten muss, um den richtigen Schlüssel zum Entschlüsseln verwenden zu können (Merkmale **1.2$_{Rest}$** und **1.3$_{Rest}$**). Dies ist dem Fachmann auch aus seinem Alltag beim Umgang mit asymmetrisch verschlüsselten E-Mails bekannt, bei denen er aus der E-Mail-Senderadresse den zugehörigen Schlüssel zum Entschlüsseln aus einer gespeicherten Liste von individuellen Schlüsseln ermittelt.

Im Hinblick auf die Sicherheitserwägungen im Zusammenhang mit der Nachrichtenübertragung und dem Einsatzort ist es dem Fachmann bekannt, wie auch in der Beschreibung ausgeführt, Überprüfungen durchzuführen, ob eine Nachricht unverfälscht angekommen ist. Bei einer verschlüsselten E-Mail erfolgt diese Überprüfung dadurch, ob ein sprachlich verständlicher Kontext nach der Entschlüsselung entstanden ist.

Da der sendende Teilnehmer eine Sender-ID unverschlüsselt zusammen mit der verschlüsselten Nachricht versendet, damit der Empfänger die verschlüsselte Nachricht entschlüsseln kann, wird er diese in natürlicher Weise auch für eine Plausibilitätsprüfung einsetzen, da ihm so kein zusätzlicher Aufwand für die Erstellung neuer Überprüfungsdaten entsteht. Es ist somit für den Fachmann nahe liegend, die Sender-ID zusätzlich in den verschlüsselten Datensatz aufzunehmen (Merkmal **1.1$_{Rest}$**) und durch Vergleichen der empfangenen unverschlüsselten Sender-ID mit der in der wiedergewonnenen entschlüsselten Nachricht enthaltenen Sender-ID die Korrektheit der Übertragenen Nachricht festzustellen (Merkmal **1.4**). Diese Verwendung einer Sender-ID innerhalb der verschlüsselten Nachricht bietet sich dem Fachmann auch aus dem folgenden Grund an: Handelt es sich bei der Nachricht, wie in der Beschreibung ausgeführt, um Messergebnisse von Sensoren, die als Sender fungieren, muss für die Weiterverarbeitung der Messergebnisse der zugehörige Sensor, also die Sender-ID, bekannt sein und ist somit bereits funktionsnotwendig Teil der zu senden Nachricht. Eine erfinderische Tätigkeit ist in dieser Plausibilitätskontrolle nicht erkennbar, da diese auf Grund des allgemeinen Fachwissens des Fachmanns für eine Vielzahl von Anwendungsfällen in Betracht kommt, für den Fachmann sinnvoll und zweckmäßig ist sowie Hinderungsgründe für dieses Vorgehen nicht ersichtlich sind (vgl. BGH, Urteil vom 11. März 2014 – X ZR 139/10 - Farbversorgungssystem).

Dass zum Zwecke der Verschlüsselung der jeweils notwendige Schlüssel bei den jeweiligen Teilnehmern in geeigneter – z. B. in einem Speicher in individualisierbarer – Form vorgehalten wird, wie es im Einzelnen im Merkmal **1.1H** angegeben ist, und entsprechend aufruf- und in Folge ausführbar sein muss, stellt eine Funktionsnotwendigkeit jedes Daten verarbeitenden Verfahrens dar und wird vom Fachmann im Rahmen der Realisierung des anspruchsgemäßen Verfahrens ohne Weiteres entsprechend den gegebenen Randbedingungen realisiert.

Somit sind alle Merkmale des mit dem Hilfsantrag beanspruchten Verfahrens gemäß Patentanspruch 1 dem Fachmann durch seine Fachkenntnisse auf der Grundlage des Lehrbuches MENEZES, 1997 (**D5**) nahe gelegt. Patentanspruch 1 gemäß Hilfsantrag ist daher nicht gewährbar.
Nachdem letzterer - wie die vorstehenden Ausführungen zum Hilfsantrag zeigen - nicht auf einer erfinderischen Tätigkeit beruht, erweist sich auch der weiter gefasste Gegenstand des Patentanspruchs 1 nach Hauptantrag als nicht patentfähig.

4. Mit Patentanspruch 1 gemäß Hauptantrag und Hilfsantrag fallen auch alle anderen Ansprüche der jeweiligen Anspruchsfassungen da ein Patent nur so erteilt werden kann, wie es beantragt ist (BGH, Beschluss vom 26. September 1996 – X ZB 18/95, GRUR 1997, 120 - elektrisches Speicherheizgerät, mit weiteren Nachweisen).

5. Bei der gegebenen Sach- und Rechtslage kann vorliegend ferner dahingestellt bleiben, ob der elektronisch erstellte und signierte Beschluss des DPMA möglicherweise an Wirksamkeitsmängeln leidet (vgl. 20 W (pat) 28/12 vom 12. Mai 2014 u. a. im Hinblick auf das Erfordernis einer signierten Urschrift in der elektronischen Akte).

6. Im Ergebnis konnte somit dem Antrag der Anmelderin, nämlich den Zurückweisungsbeschluss der Prüfungsstelle vom 24. Mai 2012 aufzuheben und in Folge ein Patent auf Basis eines der von ihr gestellten Anträge zu erteilen, nicht stattgegeben werden.

Die Beschwerde war daher zurückzuweisen.

Rechtsbehelfsbelehrung

Gegen diesen Beschluss des Beschwerdesenats steht den am Beschwerdeverfahren Beteiligten die Rechtsbeschwerde zu (§ 99 Absatz 2, § 100 Absatz 1, § 101 Absatz 1 des Patentgesetzes).

Da der Senat die Rechtsbeschwerde nicht zugelassen hat, ist sie nur statthaft, wenn gerügt wird, dass

1. das beschließende Gericht nicht vorschriftsmäßig besetzt war,
2. bei dem Beschluss ein Richter mitgewirkt hat, der von der Ausübung des Richteramtes kraft Gesetzes ausgeschlossen oder wegen Besorgnis der Befangenheit mit Erfolg abgelehnt war,
3. einem Beteiligten das rechtliche Gehör versagt war,
4. ein Beteiligter im Verfahren nicht nach Vorschrift des Gesetzes vertreten war, sofern er nicht der Führung des Verfahrens ausdrücklich oder stillschweigend zugestimmt hat,
5. der Beschluss aufgrund einer mündlichen Verhandlung ergangen ist, bei der die Vorschriften über die Öffentlichkeit des Verfahrens verletzt worden sind, oder
6. der Beschluss nicht mit Gründen versehen ist

(§ 100 Absatz 3 des Patentgesetzes).

Die Rechtsbeschwerde ist beim Bundesgerichtshof einzulegen (§ 100 Absatz 1 des Patentgesetzes). Sitz des Bundesgerichtshofes ist Karlsruhe (§ 123 GVG).

Die Rechtsbeschwerde ist innerhalb eines Monats nach Zustellung des Beschlusses beim Bundesgerichtshof schriftlich einzulegen (§ 102 Absatz 1 des Patentgesetzes). Die Postanschrift lautet: Bundesgerichtshof, Herrenstraße 45 a, 76133 Karlsruhe.

Sie kann auch als elektronisches Dokument eingereicht werden (§ 125a Absatz 2 des Patentgesetzes in Verbindung mit der Verordnung über den elektronischen Rechtsverkehr beim Bundesgerichtshof und Bundespatentgericht (BGH/BPatGERVV) vom 24. August 2007 (BGBl. I S. 2130)). In diesem Fall muss die Einreichung durch die Übertragung des elektronischen Dokuments in die elektronische Poststelle des Bundesgerichtshofes erfolgen (§ 2 Absatz 2 BGH/BPatGERVV).

Die Rechtsbeschwerde kann nur darauf gestützt werden, dass der Beschluss auf einer Verletzung des Rechts beruht (§ 101 Absatz 2 des Patentgesetzes). Die Rechtsbeschwerde ist zu begründen. Die Frist für die Begründung beträgt einen Monat; sie beginnt mit der Einlegung der Rechtsbeschwerde und kann auf Antrag von dem Vorsitzenden verlängert werden (§ 102 Absatz 3 des Patentgesetzes). Die Begründung muss enthalten:

1. die Erklärung, inwieweit der Beschluss angefochten und seine Abänderung oder Aufhebung beantragt wird;
2. die Bezeichnung der verletzten Rechtsnorm;
3. insoweit die Rechtsbeschwerde darauf gestützt wird, dass das Gesetz in Bezug auf das Verfahren verletzt sei, die Bezeichnung der Tatsachen, die den Mangel ergeben

(§ 102 Absatz 4 des Patentgesetzes).

Vor dem Bundesgerichtshof müssen sich die Beteiligten durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten vertreten lassen (§ 102 Absatz 5 des Patentgesetzes).

Dr. Mayer Gottstein Kopacek Dr. Wollny

Pü