BUNDESPATENTGERICHT

17 W (pat) 3/07

_____

(Aktenzeichen)

Verkündet am
27. März 2012
…

B E S C H L U S S

In der Beschwerdesache

betreffend die Patentanmeldung 103 53 966.2-53

…

hat der 17. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 27. März 2012 unter Mitwirkung des Vorsitzenden Richters Dipl.-Phys. Dr. Fritsch, der Richterin Eder sowie des Richters Dipl.-Ing. Baumgardt und der Richterin Dipl.-Ing. Wickborn

beschlossen:

Die Beschwerde wird zurückgewiesen.

G r ü n d e

I.

Die vorliegende Patentanmeldung wurde am 19. November 2003 beim Deutschen Patent- und Markenamt eingereicht. Sie trägt die Bezeichnung:

„Verfahren zum Zugriff auf eine Datenverarbeitungsanlage“.

Die Anmeldung wurde durch Beschluss der Prüfungsstelle für Klasse G 06 F des Deutschen Patent- und Markenamts mit der Begründung zurückgewiesen, dass das Verfahren nach dem Patentanspruch 1 des Hauptantrags und der drei damals geltenden Hilfsanträge nicht entscheidend technisch geprägt sei.

Gegen diesen Beschluss ist die Beschwerde der Anmelderin gerichtet.

Sie erläutert die technischen Aspekte der Anmeldung und benennt konkrete Lösungsmerkmale, die ihrer Auffassung nach technische Merkmale seien.

Mit Ladungszusatz wurde darauf hingewiesen, dass diesen Einwänden zwar gefolgt werden könne, dann jedoch der jeweilige Hauptanspruch des dem Zurückweisungsbeschluss zugrundeliegenden Hauptantrags und der Hilfsanträge voraussichtlich mangels erfinderischer Tätigkeit nicht gewährbar sei.

Die Anmelderin hat daraufhin einen neuen Hauptanspruch eingereicht und stellt den Antrag,

> den angegriffenen Beschluss aufzuheben und das nachgesuchte Patent mit folgenden Unterlagen zu erteilen:

Patentanspruch 1 vom 22. März 2012,
eingegangen am 26. März 2012,
Patentansprüche 2-13 vom Anmeldetag,
Beschreibung Seiten 1-12 vom 26. Juli 2004,
eingegangen am 29. Juli 2004,
2 Blatt Zeichnungen mit 2 Figuren vom Anmeldetag.

Im Beschwerdeschriftsatz regt sie ferner die Rückerstattung der Beschwerdegebühr an, ohne dies näher zu begründen.

Der geltende Patentanspruch 1, hier mit einer möglichen Gliederung versehen, lautet:

"**1.** Verfahren zum Zugriff auf eine Datenverarbeitungsanlage (D1), welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten (1, 2, 3) gebildet ist,
mit folgenden Schritten:

(a) Authentifizierung des Systemadministrators (4) an einer ersten Datenverarbeitungseinheit (1) durch Übergabe eines ersten Authentifizierungsmittels (9) an ein Authentifizierungsprogramm (5),

(b) Authentifizierung des Systemtechnikers (8) an einer von der ersten Datenverarbeitungseinheit (1) entfernt angeordneten zweiten Datenverarbeitungseinheit (7) durch Übergabe eines zweiten Authentifizierungsmittels (10) an das Authentifizierungsprogramm (5)

(b1) und dadurch bedingtes automatisches Erzeugen einer den Träger des zweiten Authentifizierungsmittels (10) identifizierenden Identifikationsinformation,

(c) Anzeigen der Identifikationsinformation an der ersten Datenverarbeitungseinheit (1) des Systemadministrators (4),

(d) automatisches Freischalten einer Zugangsberechtigung für den Systemtechniker (8),

(d1) wenn der Systemadministrator (4) und der Systemtechniker (8) gleichzeitig authentifiziert sind, und

(e) automatisches Auslösen einer Funktion zum Erzeugen und Speichern einer die Tätigkeit des Systemtechnikers (8) an der Datenverarbeitungsanlage (D1) protokollierenden Protokolldatei."

Bezüglich der Unteransprüche 2 bis 13 wird auf die Akte verwiesen.

Der Anmeldung soll die **Aufgabe** zugrundeliegen, ein Verfahren anzugeben, welches einen eine Datenhoheit eines Systemadministrators sicherstellenden Zugriff auf eine Datenverarbeitungsanlage lediglich nach dem Grundsatz des 4-Augen-Prinzips ermöglicht (siehe geltende Beschreibung Seite 2 Absatz 2).

II.

Die Beschwerde wurde frist- und formgerecht eingelegt und ist auch sonst zulässig. Sie hat jedoch keinen Erfolg, weil das beanspruchte Verfahren zum Zugriff auf eine Datenverarbeitungsanlage nicht auf einer erfinderischen Tätigkeit beruht (§ 4 PatG).

1. Die vorliegende Patentanmeldung betrifft den Zugriffsschutz bei einer Datenverarbeitungsanlage, welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten gebildet ist. Sie geht von der besonderen Bedingung aus, dass aus datenschutzrechtlichen Gründen ein Zugriff auf bestimmte derartige Datenverarbeitungsanlagen nur nach dem 4-Augen-Prinzip (d h. nur durch zwei befugte Personen gleichzeitig) erfolgen dürfe.

Als Beispiel nennt die Anmeldung Krankenhäuser, in denen u. a. Diagnose- und Analysegeräte Bestandteile solcher Datenverarbeitungsanlagen seien. Die Wartung oder Reparatur der Geräte erfordere in der Regel den Zugriff eines Systemtechnikers auf die Datenverarbeitungsanlage. Problematisch sei, dass der Systemtechniker dabei auch Zugriff auf personenbezogene Patientendaten erhalten könne, vgl. Offenlegungsschrift Absatz [0003]. Deshalb bestehe dort das genannte „4-Augen-Prinzip“. Dieses sei aber in der Praxis kaum realisierbar, weil bei einer Funktionsstörung einer Datenverarbeitungsanlage in der Regel eine sofortige Abhilfe erforderlich sei und zwei befugte und zur Behebung der Funktionsstörung ausreichend qualifizierte Systemtechniker nicht immer gleichzeitig verfügbar seien.

Mit der Anmeldung wird daher ein Verfahren beansprucht, welches das Problem des „4-Augen-Prinzips“ dahingehend vereinfacht, dass ein einzelner Systemtechniker allein an der Datenverarbeitungsanlage arbeiten kann, er aber dennoch ständig überwacht wird und es möglich ist, einen unbefugten Zugriff auf schutzbedürftige Daten, wie z. B. Patientendaten, zu unterbinden.

Dies gelingt nach den Ausführungen der Anmeldung insbesondere dadurch, dass die Aufsichtsfunktion der „zweiten Person“ auf den authentifizierten Systemadministrator (Merkmal **(a)**) übertragen wird: Dieser erhält nach erfolgreicher Anmeldung und Authentifizierung des Systemtechnikers an einer entfernt angeordneten Datenverarbeitungseinheit (Merkmal **(b)**) eine besondere Anzeige an der Datenverarbeitungsanlage vor Ort (Merkmal **(c)**), welche ihn auf die Anwesenheit der zu überwachenden Person im System und deren Identität (Merkmal **(b1)**) hinweist. Der Systemtechniker erhält nur dann automatisch eine Freischaltung seiner Zugangsberechtigung, wenn der Systemadministrator gleichzeitig mit ihm im System anwesend (authentifiziert) ist (Merkmale **(d)**, **(d1)**). Mit der Freischaltung wird automatisch eine Protokollierung der Tätigkeiten des Systemtechnikers an der Datenverarbeitungsanlage ausgelöst (Merkmal **(e)**), so dass diese Tätigkeiten gewissermaßen unter der Kontrolle des Systemadministrators stehen, welcher einen unbefugten Zugriff jederzeit unterbinden könnte.

Unter dem Begriff „Authentifizierungsmittel“ versteht die Anmeldung einen – an sich üblichen – Zugangscode wie ein Passwort, der auch z. B. auf einer Speicherkarte abgelegt sein kann (siehe Offenlegungsschrift Absatz [0011]). Entsprechend stellen die Verfahrensschritte **(a)** und **(b)** sowie der dadurch ausgelöste Schritt **(d)** des automatischen Freischaltens einer Zugangsberechtigung lediglich die allgemein bekannte, übliche Authentifizierung bei der Anmeldung an einer DV-Anlage oder -Einheit dar.

Als **Fachmann**, der mit der Aufgabe betraut wird, ein Verfahren zum Zugriffsschutz für Datenverarbeitungsanlagen auf einen besonderen Anwendungsfall hin auszulegen, sieht der Senat einen System-Ingenieur an, der im Bereich der Konzeptionierung von Zugriffsauthentisierungsverfahren mehrjährige Berufserfahrung besitzt.

2. Allerdings kann der Argumentation der Prüfungsstelle nicht gefolgt werden.

Die Prüfungsstelle hat als Grund für die Zurückweisung der Anmeldung geltend gemacht, dass das beanspruchte Verfahren nicht entscheidend technisch geprägt sei; denn es sei ein Tätigwerden des menschlichen Geistes des Systemadministrators erforderlich, ohne welches das jeweils beanspruchte Verfahren nicht zum Erfolg führen könne.

Diese Argumentation ist in mehrfacher Hinsicht nicht tragfähig:

2.1 Grundsätzlich kommt es nach der neueren Rechtsprechung des BGH nicht speziell darauf an, ob die „prägenden Anweisungen der beanspruchten Lehre ... der Lösung eines konkreten technischen Problems dienen“ (BGH BlPMZ 2002, 114 – Suche fehlerhafter Zeichenketten). Vielmehr ist es für das Technizitätserfordernis unerheblich, ob der Gegenstand einer Anmeldung neben technischen Merkmalen auch nichttechnische aufweist: „... entscheidet über die Patentierung

nicht das Ergebnis einer Gewichtung technischer und nichttechnischer Elemente“ (BGH BlPMZ 2009, 183 – Steuerungseinrichtung für Untersuchungsmodalitäten).

2.2 Darüber hinaus kann ein konkreter Verfahrensschritt, der ein „Tätigwerden des menschlichen Geistes“ beansprucht, zwar nicht patentbegründend sein; patenthindernd ist er aber ebensowenig, vgl. z. B. BGH BlPMZ 2000, 276 – Sprachanalyseeinrichtung: „Dem technischen Charakter der Vorrichtung steht es nicht entgegen, dass ein Eingreifen des Menschen in den Ablauf des auf dem Rechner durchzuführenden Programms in Betracht kommt“; oder BGH Mitt. 2002, 176 – Gegensprechanlage: „Dass ein Arbeitsgang durch einen Menschen eingeleitet oder ausgelöst wird, nimmt der Erfindung nicht die erforderliche Technizität ...“.

2.3 Und schließlich ist auch in der dem Zurückweisungsbeschluss zugrundeliegenden Anspruchsfassung (damals Hauptantrag, Anspruch 1: „Freischalten einer Zugangsberechtigung für den Systemtechniker“) von einem Tätigwerden des menschlichen Geistes gar keine Rede; dies war nur eine Option eines Unteranspruchs.

Die geltende Anspruchsfassung ist nunmehr ausdrücklich auf ein „automatisches Freischalten einer Zugangsberechtigung für den Systemtechniker“ (Merkmal **(d)**) gerichtet, so dass die Option eines Tätigwerdens des menschlichen Geistes nicht weiter besteht.

3. Das Verfahren zum Zugriff auf eine Datenverarbeitungsanlage gemäß dem geltenden Patentanspruch 1 ergab sich für den Durchschnittsfachmann in naheliegender Weise aus dem Stand der Technik.

Von besonderer Bedeutung dafür sind die von der Prüfungsstelle entgegengehalten Druckschriften:

E1 DE 101 21 819 A1,

E2 EP 1 028 568 A1.

3.1 Wie bereits dargestellt, war die Authentifizierung eines berechtigten Nutzers an einer Datenverarbeitungseinheit durch Übergabe eines Authentifizierungsmittels (Passwort) an ein Authentifizierungsprogramm, mit anschließender automatischer Freischaltung einer Zugangsberechtigung, im Sinne der Merkmale **(a)**, **(b)** und **(d)** bereits lange vor den Anmeldetag allgemein üblich. Dies gilt auch für den Fall, dass bei miteinander vernetzten Datenverarbeitungseinheiten sich ein Nutzer von einer entfernt angeordneten Verarbeitungseinheit aus anmeldet und authentifiziert. Beispielhaft hierzu kann auf die in Druckschrift **E2** geschilderte „normale“ Anmeldung verwiesen werden (siehe **E2** Absatz [0021] in Verbindung mit Figur 1, oberer Hälfte).

Dass grundsätzlich bei der erstmaligen Schaffung einer Zugangsberechtigung zu einem DV-System neben Benutzerkennung und Authentifizierungsmittel (Passwort) auch eine Identifikationsinformation (insbesondere der reale Name des Benutzers) gespeichert wird, die bei Bedarf abrufbar ist (Merkmal **(b1)**), war dem Fachmann ebenfalls vertraut.

3.2 Wenn z. B. gesetzliche Vorgaben einen höheren Zugriffsschutz erforderten, wurde das beschriebene übliche Verfahren um weitere Maßnahmen ergänzt.

So lehrt etwa Druckschrift **E1** ein Verfahren zum Zugriff auf Patientendaten. Dem behandelnden Arzt soll nur dann Zugriff auf verschlüsselte personenbezogene gesundheitsrelevante Daten ermöglicht werden, wenn der Patient tatsächlich in der Praxis anwesend ist und durch Freigabe seiner Chipkarte sein Einverständnis erklärt (siehe Zusammenfassung). Dazu ist im einzelnen vorgesehen, dass Arzt und

Patient sich beide beispielsweise durch eine Chipkarte an der Datenverarbeitungseinheit identifizieren, wobei die Freischaltung erfordert, dass beide gleichzeitig authentifiziert sind; mittels des beschriebenen „Freigabeantrags“ (Anspruch 3) erfolgt die Freigabe automatisch, wenn die Anforderungen erfüllt sind (siehe insbesondere Absatz [0118] bis [0120] – i. w. Merkmale **(a)**, **(b)**, **(d)**, **(d1)**, zu den Unterschieden s. u. Gliederungspunkt **3.4**). Merkmal **(b1)** ist implizit entnehmbar, vgl. **3.1** und im Speziellen Figur 3 „This Certificate belongs to:“. Alle Vorgänge, insbesondere die weiteren Datenzugriffe des Arztes, können dann z. B. zur Beweissicherung mitprotokolliert werden (siehe Absatz [0102] – Merkmal **(e)**).

3.3 Die Anmelderin wendet hier ein, dass Systemtechniker und Systemadministrator von ihrer Funktion her nicht mit dem Arzt und dem Patienten aus **E1** vergleichbar seien. Ferner falle bei einem derartigen Merkmalsvergleich das grundlegende erfinderische Konzept, im Sinne des „Vier-Augen-Prinzips“ die Aufsicht über den Systemtechniker auf den Systemadministrator zu übertragen, völlig unter den Tisch.

Hinsichtlich der technischen Auslegung eines Zugriffsschutzverfahrens kommt jedoch der innerbetrieblichen Funktion der Beteiligten keine Bedeutung zu.

Grundsätzlich sind nach der Rechtsprechung des Bundesgerichtshofs „bei der Prüfung der Erfindung auf erfinderische Tätigkeit … nur diejenigen Anweisungen zu berücksichtigen, die die Lösung des technischen Problems mit technischen Mitteln bestimmen oder zumindest beeinflussen“; nichttechnische Vorgaben für den technischen Fachmann bleiben dabei außer Betracht (BGH GRUR 2011, 125 – Wiedergabe topografischer Informationen).

Das zugrundeliegende objektive technische Problem sieht der Senat im vorliegenden Fall darin, einem berechtigten Nutzer (Systemtechniker) Zugriff zu gewähren, ohne dass die Datensicherheit besonders sensibler Daten beeinträchtigt wird. Die Lösung besteht in der beanspruchten konkreten Auslegung der Verfahrensschritte,

wobei aus technischer Sicht unerheblich ist, ob die den Zugriff freigebende Person Systemadministrator oder Patient ist. Ferner liegen der hier in Rede stehenden Abwandlung des Vier-Augen-Prinzips keine „auf technischen Überlegungen beruhenden Erkenntnisse“ zugrunde, sondern vielmehr wirtschaftliche oder betriebsorganisatorische Überlegungen – d. h. es handelt sich um nicht-technische Vorgaben. Somit kann der Aspekt, dass die Überwachung des Systemtechnikers auf den Systemadministrator hin verschoben wird, bei der Beurteilung der erfinderischen Tätigkeit nicht berücksichtigt werden.

3.4 Der wesentliche Unterschied der Lehre der **E1** gegenüber der Anmeldung besteht – wie die Anmelderin geltend macht – darin, dass gemäß **E1** Arzt und Patient gleichzeitig in der Praxis anwesend sein sollen, während sich anmeldungsgemäß der Systemtechniker von einer entfernt angeordneten zweiten Datenverarbeitungseinheit anmeldet (Teil von Merkmal **(b)**) und daraufhin dem Systemadministrator eine Identifikationsinformation des Systemtechnikers an seiner lokalen (ersten) Datenverarbeitungseinheit angezeigt wird (Merkmal **(c)**).

Allein mit diesem Unterschied lässt sich das Vorliegen einer erfinderischen Tätigkeit nicht begründen.

Denn es lag für den Fachmann nahe, das in **E1** beschriebene Authentifizierungsverfahren weiterzuentwickeln für den Fall, dass der Patient etwa von zuhause aus den Zugriff des Arztes auf seine geschützten Patientendaten freigeben könnte – so wie sich ja ein berechtigter Nutzer beispielsweise gemäß **E2** auch von einer entfernt angeordneten Datenverarbeitungseinheit in einem vernetzten DV-System anmelden kann. Die grundsätzliche Idee, eine Datenfreigabe auch dann zu ermöglichen, wenn der Patient selbst nicht anwesend ist, ergibt sich aus der Praxis (vgl. auch **E1** Absatz [0167] „Vertretung von Personen“). **E1** enthält hierzu bereits in Absatz [0077] den Hinweis, die verschiedenen Schritte im Authentifizierungsprozess „räumlich und datentechnisch“ weitgehend zu entkoppeln. Die Vernetzung der beteiligten Datenverarbeitungseinheiten über ein Netzwerk wie das Internet ist

in **E1** ebenfalls beschrieben, vergleiche Figur 1 und z. B. Absatz [0112] bis [0114]. Der Fachmann erkennt ohne Weiteres, dass bei dem System gemäß **E1** die technischen Bedingungen (Vernetzung der DV-Einheiten, Verschlüsselungstechnik, verteilte Datenhaltung, netzweite Authentifizierung mit Zertifikaten u. a.) vorliegen, die erfüllt sein müssen, wenn der Patient die Freigabe eines Arzt-Zugriffs auf seine Patientendaten von einer räumlich entfernt angeordneten Datenverarbeitungseinheit freigeben wollte.

Für den Fachmann war allerdings offensichtlich, dass der Patient sich über die Identität des Arztes sicher sein musste, wenn er von einer entfernt angeordneten Datenverarbeitungseinheit aus eine Zugangsberechtigung für diesen einräumen sollte. Weil aber das in **E1** dargestellte Applet (Figur 2) mit Zertifikaten arbeitet, welche – wie in Figur 3 dargestellt – eine Identifikationsinformation des Inhabers enthalten, war es unmittelbar naheliegend, eine solche Identifikationsinformation zur Sicherstellung der Identität des Arztes dem Patienten anzuzeigen (Merkmal **(c)**).

Somit ergeben sich alle Merkmale des geltenden Patentanspruchs 1 aus Druckschrift **E1** und der einfachen, in **E1** bereits angeregten Überlegung, dem Patienten eine Freigabe seiner Patientendaten für den Arzt auch von einer entfernt angeordneten Datenverarbeitungseinheit aus zu ermöglichen.

4. Mit dem Patentanspruch 1 fallen auch die Unteransprüche, weil über einen Antrag nur einheitlich entschieden werden kann.

III.

Die beantragte Rückzahlung der Beschwerdegebühr ist nicht geboten.

Nach § 80 Abs. 3 PatG ist die Rückzahlung anzuordnen, wenn sie der Billigkeit entspricht. Dem genügt allein eine fehlerhafte Begründung der Entscheidung oder

eine sachliche Fehlbeurteilung noch nicht. Vielmehr müssten noch besondere Umstände hinzukommen, die das Einbehalten der Gebühr als ungerecht erscheinen ließen (vgl. Schulte, PatG, 8. Auflage (2008), § 73 Rdnr. 130; Busse, PatG, 6. Auflage (2003), § 80 Rdnr. 124, Rdnr. 140).

Derartige besondere Umstände wurden von der Anmelderin jedoch weder vorgetragen, noch sind sie für den Senat ersichtlich.

Dr. Fritsch Eder Baumgardt Wickborn

Me