



BUNDESPATENTGERICHT

17 W (pat) 26/15

Verkündet am
21. Februar 2017

(Aktenzeichen)

...

BESCHLUSS

In der Beschwerdesache

betreffend die Patentanmeldung 10 2013 015 382.4-53

...

hat der 17. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 21. Februar 2017 unter Mitwirkung des Vorsitzenden Richters Dipl.-Phys. Dr. Morawek, der Richterin Eder, der Richterin Dipl.-Phys. Dr. Thum-Rung und des Richters Dipl.-Ing. Hoffmann

beschlossen:

Die Beschwerde wird zurückgewiesen.

Gründe

I.

Die vorliegende Patentanmeldung wurde am 17. September 2013 beim Deutschen Patent- und Markenamt eingereicht. Sie trägt die Bezeichnung:

„Verfahren zum Anzeigen einer Information“.

Die Anmeldung wurde durch Beschluss der Prüfungsstelle für Klasse G06Q in der Anhörung vom 23. April 2015 zurückgewiesen. Die Prüfungsstelle führt zur Begründung der Zurückweisung aus, dass der Gegenstand des Patentanspruchs 1 in naheliegender Weise mit dem aus dem Stand der Technik Vorbekanntem erreicht sei und somit mangels erfinderischer Tätigkeit nicht gewährbar sei.

Gegen diesen Beschluss ist die Beschwerde der Anmelderin gerichtet.

Der Vertreter der Beschwerdeführerin stellte den Antrag,

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

Patentansprüche 1–10 vom 12. August 2014,
Beschreibung Seiten 1–11 und
2 Blatt Zeichnungen mit Figuren 1–3, jeweils vom Anmeldetag.

Der geltende **Patentanspruch 1** (hier mit einer denkbaren Gliederung versehen) lautet:

1. **(A)** Verfahren zum Anzeigen einer vertraulichen Information, aufweisend die folgenden Schritte:
 - (a)** postalisches Bereitstellen einer Authentisierungsinformation (10) an einen Nutzer;
 - (b)** Einlesen der Authentisierungsinformation (10) mit einer Aufnahmeeinheit (12) einer am Kopf angeordneten Anzeigeeinrichtung (14, 16) oder einer Aufnahmeeinheit (12) eines Mobilfunkgerätes;
 - (c)** Übermitteln einer der Anzeigeeinrichtung (14, 16) oder dem Mobilfunkgerät zugeordneten Identifizierungsinformation und der eingelesenen Authentisierungsinformation (10) an eine Serviceeinrichtung über eine Luftschnittstelle,
 - (d)** wobei die Identifizierungsinformation der Serviceeinrichtung vor dem Bereitstellen der Authentisierungsinformation (10) bekannt ist;
 - (e)** Übermitteln der vertraulichen Information an die an den Kopf des Nutzers angeordnete Anzeigeeinrichtung (16) über die Luftschnittstelle,
 - (f)** wenn die Identifizierungsinformation und die Authentisierungsinformation mit der bei der Serviceeinrichtung gespeicherten Identifizierungsinformation und der Authentisierungsinformation übereinstimmen und
 - (g)** Anzeigen der vertraulichen Information auf der an dem Kopf des Nutzers angeordneten Anzeigeeinrichtung (16), wobei es sich bei der vertraulichen Information um ein Zugangspasswort und/oder eine Geheimzahl handelt.

Zu den übrigen Ansprüchen wird auf die Akte verwiesen.

Im Verfahren sind folgende Druckschriften genannt worden:

- D1:** Markus Mandau: „Die beste Online-Bank“, CHIP Online vom 04.09.2013,
Online: http://www.chip.de/artikel/Online-Banking-Test_63471557.html;
- D2:** US 8 511 547 B2;
- D3:** US 2012 / 218 188 A1.

Zu den Einzelheiten wird auf die Akte verwiesen.

II.

Die Beschwerde wurde frist- und formgerecht eingelegt und ist auch sonst zulässig. Sie hat jedoch keinen Erfolg, da das beanspruchte Verfahren nach Patentanspruch 1 nicht auf einer erfinderischen Tätigkeit beruht (§ 4 PatG).

1. Die vorliegende Patentanmeldung betrifft ein Verfahren zum Anzeigen einer vertraulichen Information mit einer an einem Kopf angeordneten Anzeigevorrichtung (vgl. Offenlegungsschrift, Absatz [0001]).

Gemäß der vorliegenden Anmeldung sei es bekannt, bei Beantragung einer neuen Kreditkarte oder einer neuen Geldkarte die zugehörige Geheimzahl / PIN in einem separaten Brief zu übermitteln. Dieses Verfahren weise den Nachteil auf, dass zusätzlich zu der Kreditkarte ein weiterer Brief verschickt werden müsse. Dadurch entstünden zusätzlich Kosten und es bestehe das Risiko, dass der Brief mit der PIN von einem unbefugten Dritten abgefangen werden könnte.

Ferner sei das sogenannte ePIN-Verfahren bekannt, bei welchem einem Kartenbesitzer die PIN per Kurznachricht (SMS) mitgeteilt werde. Dieses Verfahren weise den Nachteil auf, dass auch der Versand von Kurznachrichten Kosten verursache und zusätzlich die Gefahr bestehe, dass eine auf der Anzeigevorrichtung

eines Mobilfunkgerätes dargestellte PIN von einem in der Nähe stehenden Dritten mitgelesen werde, um die PIN anschließend missbräuchlich einzusetzen (Offenlegungsschrift, Absätze [0002] und [0003]).

Der Anmeldung soll die **Aufgabe** zugrundeliegen, die genannten Nachteile bei der Übertragung von PINs zu lösen und ferner ein Verfahren zum Anzeigen einer vertraulichen Information zur Verfügung zu stellen, das es ermöglicht, vertrauliche Informationen sicher und geschützt vor dem Zugriff durch Dritte zu übertragen und darzustellen (Offenlegungsschrift, Absatz [0004]).

Zur Lösung dieser Aufgabe schlägt der **Patentanspruch 1** ein Verfahren zum Anzeigen einer vertraulichen Information vor (Merkmal **(A)**). Bei dem Verfahren wird einem Nutzer eine Authentisierungsinformation postalisch bereitgestellt (Merkmal **(a)**) und mit einer Aufnahmeeinheit, welche sich an einer am Kopf angeordneten Anzeigeeinrichtung oder an einem Mobilfunkgerät befindet, eingelesen (Merkmal **(b)**).

Anschließend wird eine der Anzeigeeinrichtung oder dem Mobilfunkgerät zugeordnete Identifizierungsinformation gemeinsam mit der eingelesenen Authentisierungsinformation an eine Serviceeinrichtung über eine Luftschnittstelle übermittelt (Merkmal **(c)**), wobei die Identifizierungsinformation der Serviceeinrichtung vor dem Bereitstellen der Authentisierungsinformation bekannt ist (Merkmal **(d)**). Bei der Identifizierungsinformation kann es sich um eine beliebige mit der Serviceeinrichtung ausgehandelte Information handeln (vgl. Offenlegungsschrift, Absätze [0012], [0026]).

Schließlich wird, wenn die Identifizierungsinformation und die Authentisierungsinformation mit der bei der Serviceeinrichtung gespeicherten Identifizierungsinformation und der Authentisierungsinformation übereinstimmen (Merkmal **(f)**), eine vertrauliche Information an die an den Kopf des Nutzers angeordnete Anzeigeeinrichtung über die Luftschnittstelle übermittelt (Merkmal **(e)**) und auf der an dem Kopf des Nutzers angeordneten Anzeigeeinrichtung angezeigt, wobei es sich bei der

vertraulichen Information um ein Zugangspasswort und/oder eine Geheimzahl handelt (Merkmal **(g)**).

Als **Fachmann**, der mit der Aufgabe betraut wird, ein Verfahren zum Anzeigen von vertraulichen Informationen im Finanzbereich zu entwickeln, ist ein Elektroingenieur oder Programmierer mit Kenntnissen in der Entwicklung von mobilen elektronischen Bankanwendungen anzusehen.

2. Der Gegenstand des Patentanspruchs 1 beruht nicht auf einer erfinderschen Tätigkeit.

Als im Stand der Technik besonders relevant sieht der Senat die Druckschrift **D2** an.

Aus der **D2** (Titel, Abstract) sind unterschiedliche Authentisierungsverfahren zu entnehmen, die auf zwei Schritten basieren. Zur Ausführung der Verfahren wird eine kontaktlose Chip-Karte oder ein kontaktloses Zahlungsgerät und ein kontaktloses Lesegerät wie bspw. ein Mobiltelefon verwendet.

Zum Verfahrensablauf ist in der **D2** die Eingabe einer ersten Eingabeinformation an ein mobiles Gerät, z. B. ein Mobiltelefon, durch einen Benutzer beschrieben, wobei der erste Eingabewert bspw. eine PIN sein kann, die nur dem Benutzer bekannt ist (Sp. 4 Z. 4–20). Diese Eingabeinformation wird an eine dem Benutzer vorliegende Chipkarte gesendet (Sp. 4 Z. 22–24).

Die Chipkarte generiert zumindest anhand der Eingabeinformation und eines auf der Chipkarte gespeicherten geheimen Wertes (Authentisierungsinformation im Sinne der vorliegenden Anmeldung) einen „dynamischen Wert“. Dieser dynamische Wert kann von dem mobilen Gerät über eine NFC-Verbindung eingelesen werden (Merkmal **(b)**) und anschließend generiert das mobile Gerät hieraus so-

nannte „authentication data“, die aus dem dynamischen Wert selbst bestehen können (Fig. 3, Sp. 6 Z. 8–14, Sp. 4 Z. 60 – Sp. 5 Z. 19).

Ebenso kann das mobile Gerät einen zweiten Eingabewert generieren, der auf im mobilen Gerät gespeicherten Daten (Identifizierungsinformationen im Sinne der Anmeldung) basieren kann. Dieser zweite Eingabewert wird entweder in den „dynamischen Wert“ integriert oder den „authentication data“ hinzugefügt (Sp. 5 Z. 20–30, Sp. 5 Z. 66–67). Die „authentication data“, welche somit sowohl eine Authentisierungsinformation als auch eine Identifizierungsinformation enthalten, werden von dem mobilen Gerät an eine entfernte Serviceeinrichtung („issuer“) über eine Luftschnittstelle, bspw. in Form von Mobilfunkdaten, übermittelt (Fig. 2, Sp. 6 Z. 15–23 – Merkmal **(c)**).

Für die Überprüfung der Echtheit der Daten wird in der Zentrale (Serviceeinrichtung / „issuer“) ein weiterer Wert (Fig. 2 „second authentication data 260“) ermittelt. Hierfür benutzt die Zentrale Daten aus einer Datenbank, die eine Überprüfung ermöglichen (Sp. 3 Z. 61–65, Sp. 6 Z. 30–50). Somit liegen der Zentrale die von dem mobilen Gerät gelieferten Informationen in Klartext oder in verschlüsselter Form bereits vor (Merkmal **(d)**).

Bei der Überprüfung werden die übermittelten Informationen mit den gespeicherten Informationen auf Übereinstimmung verglichen (Fig. 2, Sp. 6 Z. 30–50 – teilweise Merkmal **(f)**) und anschließend wird eine von der Zentrale generierte Antwort (eine weitere Information) an das mobile Gerät bzw. das Head-Mounted-Display zur Anzeige gesendet (Fig. 2, Sp. 6 Z. 30–50, Sp. 6 Z. 1–5 – Merkmal **(e)**, und restlicher Teil von Merkmal **(f)**).

Die an den Benutzer gesendete Antwort, welche aus einer positiven bzw. negativen Rückmeldung besteht (Fig. 2, Sp. 6 Z. 42–50), kann auf dem Display des mobilen Geräts oder auf dem Head-Mounted-Display angezeigt werden (Fig. 2, Sp. 6 Z. 1–5). Da die Kommunikation und damit auch die Datenübertragung zwischen einem Benutzer und bspw. einem Finanzinstitut erfolgt (Sp. 6 Z. 16–19),

ergibt es sich von selbst, dass es sich bei den übertragenen Daten um private, d. h. vertrauliche Daten handelt. Damit ist das Anzeigen einer Information auf einer am Kopf des Benutzers angeordneten Anzeigeeinrichtung (teilweise Merkmal **(g)**) und somit auch ein Verfahren zum Anzeigen einer vertraulichen Information (Merkmal **(A)**) gezeigt.

Die Art der vertraulichen Information (restlicher Teil von Merkmal **(g)**), wie bspw. ein Zugangspasswort oder eine Geheimzahl, trägt nicht zur Lösung eines technischen Problems bei und ist daher bei der Prüfung auf erfinderische Tätigkeit nicht zu berücksichtigen.

Der Vertreter der Beschwerdeführerin wendet ein, dass aus der **D2** keine postalische Übermittlung der Authentisierungsinformation (Merkmal **(a)**) zu entnehmen sei.

Aus der **D2** ist zu entnehmen, dass der Benutzer im Besitz einer Chipkarte ist (Fig. 3, Sp. 6 Z. 8–13), die, wie oben erläutert, Authentisierungsinformationen enthält. Dem Fachmann ist das Versenden von Chipkarten bzw. Bank- oder Kreditkarten als übliche Vorgehensweise bekannt. Die Einbeziehung der postalischen Übermittlungsart (Merkmal **(a)**) war somit für den Fachmann naheliegend.

Damit gelangte der Fachmann ausgehend von **D2** in naheliegender Weise zum Gegenstand des Hauptanspruchs.

3. Nachdem der Anspruch 1 nicht gewährbar ist, fallen auch die übrigen Ansprüche 2–10, da über einen Antrag nur einheitlich entschieden werden kann (BGH GRUR 1997, 120 – *Elektrisches Speicherheizgerät*).

Rechtsmittelbelehrung

Gegen diesen Beschluss steht den am Beschwerdeverfahren Beteiligten das Rechtsmittel der Rechtsbeschwerde zu. 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.

Die Rechtsbeschwerde ist innerhalb eines Monats nach Zustellung des Beschlusses beim Bundesgerichtshof, Herrenstr. 45 a, 76133 Karlsruhe, durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten schriftlich einzulegen.

Dr. Morawek

Eder

Dr. Thum-Rung

Hoffmann

Fa