BUNDESPATENTGERICHT

Verkündet am
10. August 2017
…

23 W (pat) 22/17

_____

(Aktenzeichen)

B E S C H L U S S

In der Beschwerdesache

…

Verfahrensbevollmächtigte: Tergau & Walkenhorst,
Patentanwälte – Rechtsanwälte, Partnerschaftsgesellschaft mbB,
Eschersheimer Landstraße 105-107, 60322 Frankfurt/Main

betreffend die Patentanmeldung 10 2011 112 855.0

hat der 23. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 10. August 2017 unter Mitwirkung des Vorsitzenden Richters Dr. Strößner sowie der Richter Brandt, Dr. Friedrich und Dr. Himmelmann

beschlossen:

Die Beschwerde wird zurückgewiesen.

G r ü n d e

I.

Die vorliegende Anmeldung mit dem Aktenzeichen 10 2011 112 855.0 und der Bezeichnung „Verfahren zur elektronischen Durchführung einer Zahlungstransaktion“ wurde am 12. September 2011 beim Deutschen Patent- und Markenamt eingereicht. Die Prüfungsstelle für Klasse H04L hat im Prüfungsverfahren u. a. auf den Stand der Technik gemäß den Druckschriften

D1 US 2009/0104888 A1
D2 WO 2009/149723 A1
D3 DE 10 2007 006 659 A1

verwiesen und im einzigen Prüfungsbescheid vom 7. Mai 2012 das beanspruchte Verfahren als nicht neu bezüglich der Druckschrift D1 angesehen. Mit Eingabe vom 26. Juni 2012 hat die Anmelderin einen neuen Anspruch 1 vorgelegt, zu dem die Prüfungsstelle im Ladungszusatz vom 13. März 2014 ausgeführt hat, dass Bedenken hinsichtlich dessen Zulässigkeit bestünden und darüber hinaus dessen Gegenstand durch die Druckschrift D1 dem Fachmann nahegelegt sei.

In der daraufhin am 29. April 2014 durchgeführten Anhörung, in der die Anmelderin die Patenterteilung mit Anspruchssätzen nach Hauptantrag und Hilfsanträgen 1 bis 3 beantragt hat, ist die Anmeldung durch die Prüfungsstelle mit der Begründung fehlender erfinderischer Tätigkeit zurückgewiesen worden. Ihre Entscheidung hat die Prüfungsstelle mit einem auf den 29. April 2014 datierten Beschluss begründet.

Gegen diesen der Anmelderin am 12. Mai 2014 zugestellten Beschluss richtet sich die am 10. Juni 2014 beim Deutschen Patent- und Markenamt eingegangene Beschwerde mit den nachgereichten Eingaben vom 12. Juni 2014 und 1. August 2017.

In der mündlichen Verhandlung am 10. August 2017 beantragt die Anmelderin:

1.
den Beschluss der Prüfungsstelle für Klasse H04L des Deutschen Patent- und Markenamts vom 29. April 2014 aufzuheben.

2.a) Hauptantrag
Ein Patent zu erteilen mit der Bezeichnung „Verfahren zur elektronischen Durchführung einer Zahlungstransaktion“, dem Anmeldetag 12. September 2011 auf der Grundlage folgender Unterlagen:

- Patentansprüche 1 bis 10 gemäß Hauptantrag, eingegangen am 1. August 2017;
- 8 Beschreibungsseiten (Seiten 3 bis 10)
- 1 Seite Bezugszeichenliste (Seite 11), jeweils eingegangen im Deutschen Patent- und Markenamt am 18. Juni 2014;
- 1 Blatt Zeichnungen mit einer Figur, eingegangen im Deutschen Patent- und Markenamt am Anmeldetag.

2.b) Hilfsantrag 1
Hilfsweise für die unter 2.a) genannte technische Neuerung ein Patent zu erteilen auf der Grundlage folgender Unterlagen:

- Patentansprüche 1 bis 10 gemäß Hilfsantrag 1, eingegangen am 1. August 2017;
- die unter 2.a) genannten Beschreibungsseiten, Bezugszeichenliste und Zeichnungen.

2.c) Hilfsantrag 2

Weiter hilfsweise für die unter 2.a) genannte technische Neuerung ein Patent zu erteilen auf der Grundlage folgender Unterlagen:

- Patentansprüche 1 bis 9 gemäß Hilfsantrag 2, überreicht in der mündlichen Verhandlung am 10. August 2017;
- die unter 2.a) genannten Beschreibungsseiten, Bezugszeichenliste und Zeichnungen.

2.d) Hilfsantrag 3

Weiter hilfsweise für die unter 2.a) genannte technische Neuerung ein Patent zu erteilen auf der Grundlage folgender Unterlagen:

- Patentansprüche 1 bis 9 gemäß Hilfsantrag 3, eingegangen am 1. August 2017;
- die unter 2.a) genannten Beschreibungsseiten, Bezugszeichenliste und Zeichnungen.

2.d) Hilfsantrag 4

Weiter hilfsweise für die unter 2.a) genannte technische Neuerung ein Patent zu erteilen auf der Grundlage folgender Unterlagen:

- Patentansprüche 1 bis 8 gemäß Hilfsantrag 4, eingegangen am 1. August 2017;
- die unter 2.a) genannten Beschreibungsseiten, Bezugszeichenliste und Zeichnungen.

2.d) Hilfsantrag 5

Weiter hilfsweise für die unter 2.a) genannte technische Neuerung ein Patent zu erteilen auf der Grundlage folgender Unterlagen:

- Patentansprüche 1 bis 8 gemäß Hilfsantrag 5, eingegangen am 1. August 2017;
- die unter 2.a) genannten Beschreibungsseiten, Bezugszeichenliste und Zeichnungen.

2.d) Hilfsantrag 6

Weiter hilfsweise für die unter 2.a) genannte technische Neuerung ein Patent zu erteilen auf der Grundlage folgender Unterlagen:

- Patentansprüche 1 bis 9 gemäß Hilfsantrag 6, als Hauptantrag eingegangen im Deutschen Patent- und Markenamt am 18. Juni 2014;
- die unter 2.a) genannten Beschreibungsseiten, Bezugszeichenliste und Zeichnungen.

2.d) Hilfsantrag 7

Weiter hilfsweise für die unter 2.a) genannte technische Neuerung ein Patent zu erteilen auf der Grundlage folgender Unterlagen:

- Patentansprüche 1 bis 8 gemäß Hilfsantrag 7, eingegangen am 1. August 2017;
- die unter 2.a) genannten Beschreibungsseiten, Bezugszeichenliste und Zeichnungen.

2.d) Hilfsantrag 8

Weiter hilfsweise für die unter 2.a) genannte technische Neuerung ein Patent zu erteilen auf der Grundlage folgender Unterlagen:

- Patentansprüche 1 bis 8 gemäß Hilfsantrag 8, überreicht in der mündlichen Verhandlung am 10. August 2017;
- die unter 2.a) genannten Beschreibungsseiten, Bezugszeichenliste und Zeichnungen.

Anspruch 1 des Hauptantrags hat folgenden Wortlaut (Gliederung hinzugefügt):

Verfahren zur elektronischen Durchführung einer Zahlungstransaktion, bei dem

(a) eine erste Datenverbindung (2) von einer mobilen Einheit (1) zu einem Zahlungsendgerät (4) aufgebaut wird und Authentifizierungsdaten zur Autorisierung einer Zahlung von der mobilen Einheit (1) über die erste Datenverbindung (2) an das Zahlungsendgerät (4) übertragen werden,

(b) wobei vor der Übertragung der Authentifizierungsdaten von der mobilen Einheit (1) eine zweite Datenverbindung (6) zu einem Authentifizierungsdatenserver (5) aufgebaut wird, der ein Authentifizierungselement enthält;

(c) das Authentifizierungselement über die zweite Datenverbindung (6) an der mobilen Einheit (1) empfangen wird;

(d) das Authentifizierungselement als Bestandteil der Authentifizierungsdaten verwendet wird;

dadurch gekennzeichnet, dass

(e) das Authentifizierungselement Informationen umfasst, die den von einer ec- oder Kreditkarte beim Bezahlvorgang verwendeten oder preisgegebenen Informationen entsprechen.

Anspruch 1 des Hilfsantrags 1 ergibt sich aus Anspruch 1 des Hauptantrags, indem dessen kennzeichnendes Merkmal (e) durch das folgende Merkmal (e1) ersetzt wird:

(e1) das Authentifizierungselement zumindest eines der Folgenden umfasst:

- dem Inhalt eines Magnetstreifens einer ec- oder Kreditkarte entsprechende Daten,
- eine Kartennummer einer ec- oder Kreditkarte mit CVC-Code,
- dem Inhalt und dem Kommunikations-Protokoll eines EMV-Chips entsprechende Daten.

Anspruch 1 des Hilfsantrags 2 ergibt sich aus Anspruch 1 des Hilfsantrags 1 durch das Anfügen folgender Zusatzmerkmale:

(f) wobei eine PIN als weiteres gegenüber dem Zahlungsendgerät (4) benutztes Authentifizierungselement von einem Benutzer eingegeben wird,
(g) die zweite Datenverbindung (6) eine Authentifizierung erfordert und
(h) die PIN auch zur Authentifizierung der zweiten Datenverbindung (6) verwendet wird.

Anspruch 1 des Hilfsantrags 3 hat folgenden Wortlaut (Gliederung hinzugefügt):

Verfahren zur elektronischen Durchführung einer Zahlungstransaktion, bei dem

a. eine erste Datenverbindung (2) von einer mobilen Einheit (1) zu einem Zahlungsendgerät (4) aufgebaut wird und Authentifizierungsdaten zur Autorisierung einer Zahlung von der mobilen Einheit (1) über die erste Datenverbindung (2) an das Zahlungsendgerät (4) übertragen werden,
b. vor der Übertragung der Authentifizierungsdaten von der mobilen Einheit (1) eine zweite Datenverbindung (6) zu einem Authentifizierungsdatenserver (5) aufgebaut wird, der ein Authentifizierungselement enthält;
c. das Authentifizierungselement über die zweite Datenverbindung (6) an die mobile Einheit (1) übertragen wird;
d. das Authentifizierungselement als Bestandteil der Authentifizierungsdaten verwendet wird;
dadurch gekennzeichnet, dass
e. die Authentifizierungsdaten vom Authentifizierungsdatenserver (5) zum Zahlungsendgerät (4) in einem verschlüsselten Tunnel durch die mobile Einheit (1) getunnelt werden.

Anspruch 1 des Hilfsantrags 4 ergibt sich aus Anspruch 1 des Hilfsantrags 3, indem vor das Merkmal e. das folgende Zusatzmerkmal f. eingefügt wird:

f. die erste Datenverbindung (2) eine NFC-Verbindung ist; und.

Anspruch 1 des Hilfsantrags 5 ergibt sich aus Anspruch 1 des Hilfsantrags 3, indem nach dem Merkmal e. das folgende Zusatzmerkmal f1. angefügt wird:

f1. und die zweite Datenverbindung (6) eine Authentifizierung erfordert.

Anspruch 1 des Hilfsantrags 6 ergibt sich aus Anspruch 1 des Hilfsantrags 3, indem vor das Merkmal e. das folgende Zusatzmerkmal f2. eingefügt wird:

f2. das Authentifizierungselement vom Authentifizierungsdatenserver (5) die gesamten Authentifizierungsdaten bildet; und

Anspruch 1 des Hilfsantrags 7 ergibt sich aus Anspruch 1 des Hilfsantrags 6, indem in dessen Merkmal f2. das Wort „und“ gestrichen und nach dem Merkmal e. das folgende Zusatzmerkmal g. angefügt wird:

g. und das Authentifizierungselement direkt vom Authentifizierungsdatenserver (5) an das Zahlungsendgerät (4) ohne Zwischenspeicherung auf der mobilen Einheit (1) übertragen wird.

Anspruch 1 des Hilfsantrags 8 ergibt sich aus Anspruch 1 des Hilfsantrags 6, indem in dessen Merkmal f2. das Wort „und“ gestrichen, am Anfang von dessen Merkmal e. das Wort „wobei“ eingefügt und nach dem Merkmal e. das folgende Zusatzmerkmal h. angefügt wird:

h. und wobei die zweite Datenverbindung (6) eine Authentifizierung durch die Eingabe eines Passworts oder einer PIN durch den Benutzer der mobilen Einheit (1) erfordert.

Hinsichtlich der abhängigen und selbständigen Ansprüche des Hauptantrags und der Hilfsanträge 1 bis 8 sowie bezüglich der weiteren Einzelheiten wird auf den Akteninhalt verwiesen.

II.

1. Die form- und fristgerecht eingelegte Beschwerde der Anmelderin ist zulässig. Sie erweist sich aber nach dem Ergebnis der mündlichen Verhandlung als nicht begründet, da dem Fachmann die jeweiligen Verfahren nach den Ansprüchen 1 des Hauptantrags und der Hilfsanträge 1 und 2 durch den Stand der Technik gemäß Druckschrift D1 und die Verfahren nach den Ansprüchen 1 der Hilfsanträge 3 bis 8 durch den Stand der Technik gemäß den Druckschriften D1 und D3 nahegelegt werden, so dass sie gemäß § 4 PatG wegen fehlender erfinderischer Tätigkeit nicht patentfähig sind.

Bei dieser Sachlage kann die Zulässigkeit der geltenden Patentansprüche dahingestellt bleiben *(vgl. BGH GRUR 1991, 120-122, insbesondere 121, II.1 - Elastische Bandage).*

Der zuständige Fachmann ist hier als ein berufserfahrener Ingenieur der Nachrichtentechnik mit Hochschulabschluss und Detailkenntnissen elektronischer Zahlungssysteme zu definieren.

2. Die Anmeldung betrifft ein Verfahren zur elektronischen Durchführung einer Zahlungstransaktion, bei dem eine erste Datenverbindung von einer mobilen Einheit zu einem Zahlungsendgerät aufgebaut wird und Authentifizierungsdaten zur Autorisierung einer Zahlung von der mobilen Einheit über die erste Datenverbindung an das Zahlungsendgerät übertragen werden.

Nach den Ausführungen in der Beschreibungseinleitung steigt mit der zunehmenden Verbreitung von Smartphones auch das Anwendungsgebiet des „Bezahlens

per Mobiltelefon“. Hierbei soll dem Benutzer des Mobiltelefons als mobile Einheit die Möglichkeit gegeben werden, eine Zahlungstransaktion auf elektronischem Wege durchzuführen, ohne eine ec- oder Kreditkarte manuell in ein Zahlungsendgerät wie z. B. ein ec-Terminal einführen zu müssen. Die Zahlungstransaktion soll vielmehr durch einfaches Auflegen oder vollständig berührungslos erfolgen. Grundlage ist hierbei die NFC-Technik (**N**ear **F**ield **C**ommunication-Technik), die einen Übertragungsstandard zum kontaktlosen Austausch von Daten über kurze Strecken darstellt und auf der Kombination aus Smartcard- und kontaktlosen Verbindungstechniken basiert. Sie arbeitet in einem Frequenzbereich von 13,56 MHz und bietet eine Datenübertragungsrate von maximal 424 kBit/s bei einer Reichweite von nur 10 Zentimetern, was deshalb gewünscht ist, da dann die Kontaktaufnahme als Zustimmung zu einer Transaktion gewertet werden kann.

Zur Durchführung eines elektronischen Zahlungsverkehrs sind NFC-fähige Smartphones mit einem NFC-Chip ausgestattet, der die drahtlose Kommunikation des Smartphones gegenüber anderen NFC-fähigen Geräten erlaubt. Dabei kann der NFC-Chip sowohl eine „passive“ Rolle einnehmen (z. B. sich gegenüber einem NFC-Bezahlterminal als NFC-fähige Kreditkarte ausgeben) oder eine „aktive“ Rolle, in dem er z. B. als Zahlungsendgerät oder Bezahlterminal gegenüber einer anderen NFC-fähigen (passiven) Kreditkarte agiert.

Im vorliegenden Fall steht die passive Betriebsart des NFC-Chips im Vordergrund. Dabei wird eine erste Datenverbindung von einer mobilen Einheit wie z. B. einem Smartphone zu einem Zahlungsendgerät wie z. B. einem Bezahlterminal aufgebaut und Authentifizierungsdaten zur Autorisierung einer Zahlung werden von der mobilen Einheit über die erste Datenverbindung an das Zahlungsendgerät übertragen.

Nach den weiteren Ausführungen in der Beschreibungseinleitung verwaltet das Smartphone bei bekannten Bezahlverfahren die Authentifizierungsdaten vollstän-

dig, d. h. alle für die Bezahlung notwendigen Informationen werden vom Smartphone verwaltet.

Dabei sind diese Authentifizierungsdaten entweder in der SIM-Karte des Mobilfunkanbieters oder in einem separaten Chip des Smartphones abgelegt. In beiden Fällen befinden sich die Authentifizierungsdaten daher innerhalb des Mobiltelefons und unter der Kontrolle des Mobilfunk- bzw. des Smartphoneplattform-Anbieters. Die Authentifizierungsdaten sind hierbei vergleichbar mit denjenigen Informationen, die eine herkömmliche ec- oder Kreditkarte beim Bezahlvorgang verwendet. Zu den Authentifizierungselementen, die die Authentifizierungsdaten bilden, kann bspw. der Inhalt des Magnetstreifens bzw. der Inhalt und das Kommunikations-Protokoll des EMV Chips (**E**uropay International, **M**asterCard und **V**ISA) zählen, die vom Benutzer eingegebene PIN oder die Kartennummer mit CVC-Code (nicht eingeprägter, sondern gedruckter Sicherheitscode auf der Rückseite der Kreditkarte).

Durch eine derartige Ausgestaltung ergeben sich aber sicherheitstechnische Risiken. Zum einen sind die Authentifizierungsdaten, insbesondere die Authentifizierungselemente wie der Inhalt des Magnetstreifens, Kartennummer o. ä. aus dem Einflussbereich der klassischen, etablierten Betreiber von Bezahl-Infrastrukturen wie z.B. Banken oder Kreditkartenanbietern entfernt. Zum anderen wird so der Verlust des Smartphones praktisch gleichbedeutend mit dem Verlust einer ec- oder Kreditkarte, *vgl. Beschreibungsseiten 3 bis 5, zweiter Absatz.*

Vor diesem Hintergrund liegt der Anmeldung als technisches Problem die Aufgabe zugrunde, ein Verfahren zur elektronischen Durchführung einer Zahlungstransaktion anzugeben, das die Sicherheit des elektronischen Zahlungsverkehrs erhöht, *vgl. Beschreibungsseite 5, dritter Absatz.*

Diese Aufgabe wird durch die Verfahren der Ansprüche 1 nach dem Hauptantrag und nach den Hilfsanträgen 1 bis 8 sowie durch die Computerprogrammprodukte,

mobilen Einheiten und Telekommunikationssysteme der selbständigen Ansprüche der jeweiligen Anspruchssätze gelöst.

Das Verfahren nach Anspruch 1 wird in der Beschreibung auf Seite 10 anhand der einzigen Figur erläutert. Der Verfahrensablauf ist demnach folgender:

(1) Die mobile Einheit, typischerweise ein Smartphone, stellt zur Durchführung einer elektronischen Zahlungstransaktion eine erste drahtlose Verbindung zu einem Zahlungsendgerät her, und danach wird der Benutzer ggf. zur Eingabe eines Passworts oder einer PIN aufgefordert.
(2) Anschließend wird eine authentifizierte Verbindung zu einem Authentifizierungsdatenserver hergestellt. Diese findet über eine zweite drahtlose Verbindung statt, die bspw. als GSM-, EDGE- oder UMTS-Verbindung ausgestaltet sein kann und zunächst zu einem Mobilfunkempfänger und dann zum Authentifizierungsdatenserver führt.
(3) Vom Authentifizierungsdatenserver wird ein Authentifizierungselement über die zweite drahtlose Verbindung zunächst an die mobile Einheit und von dort über die erste drahtlose Verbindung an das Zahlungsendgerät weiter übertragen, wobei dies bei ggf. vorhandener PIN-Abfrage die Autorisierung durch das korrekte Passwort bzw. die korrekte PIN erfordert.

Hinsichtlich des Oberbegriffs der Ansprüche 1 nach Hauptantrag und nach den Hilfsanträgen 1 bis 8 bedeutet dies, dass zunächst der die erste Datenverbindung betreffende Teil des Merkmals a ausgeführt wird, danach die Verfahrensschritte der Merkmale b, c und d und schließlich der die zweite Datenverbindung betreffende Teil des Merkmals a.

Mit den kennzeichnenden Merkmalen der Ansprüche 1 der jeweiligen Anspruchssätze werden das Authentifizierungselement bzw. die Authentifizierungsdaten sowie die Datenverbindungen und die zugehörigen Autorisierungen spezifiziert.

3. Das Verfahren des Anspruchs 1 nach Hauptantrag wird dem Fachmann durch die Druckschrift D1, die ebenfalls ein Verfahren zur elektronischen Durchführung einer Zahlungstransaktion beschreibt, vgl. bspw. deren Abs. [0001], nahegelegt.

Gemäß deren Fig. 1 mit Beschreibung in den Abs. [0045] bis [0052] kommuniziert während einer solchen Zahlungstransaktion die mobile Einheit *(wireless bzw. mobile device 124)* über eine erste Datenverbindung mit dem Zahlungsendgerät *(POS (point-of-sale) Device 110)* und über eine zweite Datenverbindung *(relay station 125, Service Provider System 130)* mit einem Zahlungsabwicklungssystem *(Acquirer System 112, Financial Network 113, Financial Institution 116, 117, 118).* Dazu ist nach Fig. 2A und der Beschreibung in den Abs. [0053] bis [0063] auf der mobilen Einheit *(Mobile Device 124)* eine Finanztransaktionssoftware *(Wallet 208)* installiert, die mittels NFC *(NFC 206, 207)* mit dem Zahlungsendgerät *(POS 110)* kommuniziert und über die zweite Datenverbindung *(Service Provider/Carrier 130)* Authentifizierungsdaten von einem Authentifizierungsdatenserver *(Mobile wallet server 210, PIN generator 240)* erhält, der wiederum mit dem Zahlungsabwicklungssystem *(Acquirer System 112)* kommuniziert. Ein beispielhaftes Bezahlverfahren ist in Abs. [0063] folgendermaßen beschrieben: „*The PIN generator 240 may also generate a password upon request from a mobile device 124 through the service provider 130. When a user of the mobile device 124 presents an account from the mobile wallet 208 through the NFC transponder 207 to POS 110 to settle a transaction, the user may request a onetime password from the mobile wallet server 210 through the service provider 130. The mobile device 124 may then send the onetime password to the POS 110 for authentication through the acquirer system 112*."

Demnach offenbart Druckschrift D1 in Übereinstimmung mit dem Oberbegriff des Anspruchs 1 nach Hauptantrag ein

Verfahren zur elektronischen Durchführung einer Zahlungstransaktion *(vgl. Abs. [0001]: „More specifically, embodiments of the present invention relate to*

payment systems supporting use of mobile electronic devices using onetime user passwords in various types of financial transactions.”), bei dem

(a) eine erste Datenverbindung *(NFC 206, 207)* von einer mobilen Einheit *(Mobile Device 124)* zu einem Zahlungsendgerät *(POS 110)* aufgebaut wird und Authentifizierungsdaten *(password, vgl. Abs. [0063])* zur Autorisierung einer Zahlung von der mobilen Einheit *(124)* über die erste Datenverbindung *(NFC)* an das Zahlungsendgerät *(110)* übertragen werden,

(b) wobei vor der Übertragung der Authentifizierungsdaten von der mobilen Einheit *(124)* eine zweite Datenverbindung *(communication network, Service Provider 130)* zu einem Authentifizierungsdatenserver *(mobile wallet server 210)* aufgebaut wird, der ein Authentifizierungselement *(password)* enthält;

(c) das Authentifizierungselement *(password)* über die zweite Datenverbindung *(130)* an der mobilen Einheit *(124)* empfangen wird;

(d) das Authentifizierungselement *(password)* als Bestandteil der Authentifizierungsdaten verwendet wird.

Aus Druckschrift D1 ist folglich ein Verfahren mit sämtlichen Merkmalen des Oberbegriffs des Anspruchs 1 nach Hauptantrag bekannt.

Nach dessen kennzeichnendem Merkmal soll dabei das Authentifizierungselement Informationen umfassen, die den von einer ec- oder Kreditkarte beim Bezahlvorgang verwendeten oder preisgegebenen Informationen entsprechen. Diese Informationen müssen folglich nicht identisch mit den von einer ec- oder Kreditkarte beim Bezahlvorgang verwendeten oder preisgegebenen Informationen sein, sondern diesen Informationen lediglich entsprechen, d. h. zugeordnet werden können.

Dieses Merkmal ergibt sich für den Fachmann jedoch in naheliegender Weise aus Abs. [0059] von Druckschrift D1, denn dort ist ausgeführt, dass auf dem Authentifizierungsdatenserver *(mobile wallet server 210)* eine Datenbank unterhalten wird, die die einzelnen Bankkonten, mobilen Einheiten und Authentifizierungselemente einander zuordnet *(„The mobile wallet server 210 and/or the acquirer system 112*

may maintain a database associating, at least, financial accounts, onetime passwords, and mobile devices.“). Da die das Bankkonto betreffenden Daten zwangsläufig beim Bezahlvorgang mit einer ec- oder Kreditkarte verwendet werden und diese Daten nach obiger Fundstelle dem Authentifizierungselement *(onetime password)* zugeordnet sind, umfasst auch bei dem in Druckschrift D1 beschriebenen Verfahren das Authentifizierungselement Informationen, die den von einer ec- oder Kreditkarte beim Bezahlvorgang verwendeten Informationen entsprechen.

Das Verfahren des Anspruchs 1 nach Hauptantrag ergibt sich somit in naheliegender Weise aus Druckschrift D1 und ist daher wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

4. Das Verfahren des Anspruchs 1 nach Hilfsantrag 1 wird dem Fachmann durch die Druckschrift D1 nahegelegt.

Der Oberbegriff des Anspruchs 1 nach Hilfsantrag 1 stimmt mit Anspruch 1 des Hauptantrags 1 überein, dessen Merkmale, wie bereits dargelegt, aus Druckschrift D1 bekannt sind.

Das kennzeichnende Merkmal umfasst mehrere Alternativmerkmale, wobei eine dieser Alternativen darin besteht, dass das Authentifizierungselement dem Inhalt eines Magnetstreifens einer ec- oder Kreditkarte entsprechende Daten umfasst. Für diese Variante des kennzeichnenden Merkmals gelten somit die gleichen Ausführungen wie zum Kennzeichen des Anspruchs 1 nach Hauptantrag, da nach Abs. [0059] der Druckschrift D1 das Authentifizierungselement den das Bankkonto betreffenden Daten, die zwangsläufig ein Bestandteil des Dateninhalts eines Magnetstreifens einer ec- oder Kreditkarte sind, zugeordnet werden kann und somit Daten umfasst, die dem Inhalt eines Magnetstreifens einer ec- oder Kreditkarte entsprechen.

Das Verfahren des Anspruchs 1 nach Hilfsantrag 1 ergibt sich somit in naheliegender Weise aus Druckschrift D1 und ist daher wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

5. Das Verfahren des Anspruchs 1 nach Hilfsantrag 2 wird dem Fachmann durch die Druckschrift D1 nahegelegt.

Anspruch 1 des Hilfsantrags 2 umfasst hinsichtlich des Anspruchs 1 nach Hilfsantrag 1 die Zusatzmerkmale

(f) wobei eine PIN als weiteres gegenüber dem Zahlungsendgerät (4) benutztes Authentifizierungselement von einem Benutzer eingegeben wird,
(g) die zweite Datenverbindung (6) eine Authentifizierung erfordert und
(h) die PIN auch zur Authentifizierung der zweiten Datenverbindung (6) verwendet wird.

Auch diese weiteren Merkmale entnimmt der Fachmann in naheliegender Weise der Druckschrift D1.

So wird in den Abs. [0067] und [0068] von Druckschrift D1 hervorgehoben, dass die mobile Einheit *(124)* mit einem Bildschirm *(380)* und einer Eingabevorrichtung *(382)*, bspw. einer Tastatur oder einem berührungsempfindlichen Bildschirm, ausgestattet sein kann, um Authentifizierungselemente wie Passwörter und PINs dem Zahlungsendgerät zuzuleiten *(vgl. den letzten Satz von Abs. [0068]: „The display device 380 and the input device 382 may be used to request and receive a password, PIN, biometric feature, etc, in order to gain access to information within the mobile wallet 376 and/or in order to transmit account information and/or passwords to a POS device 110.“)*. Dies gibt dem Fachmann somit den Hinweis, dass in Übereinstimmung mit obigem Merkmal (f) eine PIN als weiteres gegenüber dem Zahlungsendgerät benutztes Authentifizierungselement von einem Benutzer eingegeben wird.

Zudem ist in Abs. [0037] der Druckschrift D1 beschrieben, dass ein Zahlvorgang, der den Zugriff auf das Netzwerk und Datensystem eines Finanzdienstleisters beinhaltet, üblicherweise die Eingabe einer PIN erfordert *(vgl. Abs. [0037], vierter Satz: „Access to a network by a consumer can be achieved through entry of a secret code, such as a personal identification number ("PIN"), in combination with data extracted from the mobile device.").* Da bei dem in Druckschrift D1 beschriebenen Bezahlverfahren der Zugang zum Netzwerk und Datensystem des Finanzdienstleisters über den Authentifizierungsdatenserver erfolgt und von der mobilen Einheit mittels der zweiten Datenverbindung hergestellt wird, gibt diese Textstelle dem Fachmann den Hinweis, auch für die zweite Datenverbindung das Erfordernis einer Authentifizierung bspw. in Form einer PIN einzurichten. Somit entnimmt der Fachmann auch das Merkmal (g), wonach die zweite Datenverbindung eine Authentifizierung erfordert, in naheliegender Weise der Druckschrift D1.

Das verbleibende Merkmal (h), dass die gegenüber dem Zahlungsendgerät benutzte PIN auch zur Authentifizierung der zweiten Datenverbindung verwendet wird, stellt eine naheliegende, fachmännische Maßnahme dar. Denn ein Ziel des in Druckschrift D1 beschriebenen elektronischen Bezahlverfahrens besteht in der Bereitstellung eines für den Nutzer sicheren und komfortablen elektronischen Bezahlsystems. Die zweifache Eingabe von PINs für einen einzigen Bezahlvorgang steht im Gegensatz zu diesem Erfordernis, da es den Bezahlvorgang für den Nutzer unnötig verkomplizieren und verzögern würde, müsste er gleiche oder unterschiedliche PINs zweimal für einen einzigen Bezahlvorgang eingeben. Aus diesem Grund wird der Fachmann bei dem in Druckschrift D1 beschriebenen Bezahlverfahren die gegenüber dem Zahlungsendgerät benutzte PIN in naheliegender Weise auch zur Authentifizierung der zweiten Datenverbindung verwenden, ohne dazu erfinderisch tätig werden zu müssen.

Das Verfahren des Anspruchs 1 nach Hilfsantrag 2 ergibt sich somit in naheliegender Weise aus Druckschrift D1 und ist daher wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

5. Das Verfahren des Anspruchs 1 nach Hilfsantrag 3 wird dem Fachmann durch die Druckschrift D1 in Verbindung mit Druckschrift D3 nahegelegt.

Der Oberbegriff des Anspruchs 1 von Hilfsantrag 3 unterscheidet sich inhaltlich lediglich dadurch vom Oberbegriff des Anspruchs 1 nach Hauptantrag, dass in Merkmal c das Authentifizierungselement über die zweite Datenverbindung an die mobile Einheit übertragen wird. Dieses Merkmal ist jedoch aus den bereits zitierten Fundstellen der Druckschrift D1, insbesondere aus deren Abs. [0063] bekannt, so dass Druckschrift D1 sämtliche Merkmale des Oberbegriffs von Anspruch 1 des Hilfsantrags 3 offenbart.

Ausgehend von Druckschrift D1 ergibt sich für den Fachmann das kennzeichnende Merkmal des Anspruchs 1, wonach die Authentifizierungsdaten vom Authentifizierungsdatenserver zum Zahlungsendgerät in einem verschlüsselten Tunnel durch die mobile Einheit getunnelt werden, in naheliegender Weise aus der Druckschrift D3. Denn gemäß Abs. [0007] der Druckschrift D1 steht dort die Erhöhung der Sicherheit bei Zahlungstransaktionen mit mobilen Einheiten im Vordergrund. Der Fachmann ist folglich bestrebt, auch für die Übertragung des Passworts vom Authentifizierungsdatenserver *(mobile wallet server 210)* über die mobile Einheit *(Mobile Device 124)* zum Zahlungsendgerät *(POS 110)* eine möglichst hohe Sicherheit gewährleisten zu können. In diesem Zusammenhang entnimmt er der Druckschrift D3 mit dem Titel „Mobiles Echtzeit Bezahlverfahren“ bspw. in Anspruch 16 die Lehre, sicherheitsrelevante Daten zwischen dem Mobilfunk-Finanzdienstleistungs-System (MFS), dem Mobilfunk-Endgerät (MS) und dem Bezahlpunkt (POS) mittels einer durch das Mobilfunk-Endgerät (MS) hindurchgehenden Tunnelverbindung zwischen dem Mobilfunk-Finanzdienstleistungs-System (MFS) und dem Bezahlpunkt (POS) durchzuführen. Diese Lehre wird der Fachmann zur Erhöhung der Sicherheit in naheliegender Weise auch bei dem Verfahren der Druckschrift D1 anwenden, indem die Authentifizierungsdaten *(password)* vom Authentifizierungsdatenserver *(mobile wallet server 210)* zum Zahlungsendgerät

(POS 110) in einem verschlüsselten Tunnel durch die mobile Einheit *(Mobile Device 124)* getunnelt werden.

Das Verfahren des Anspruchs 1 nach Hilfsantrag 3 ergibt sich somit in naheliegender Weise aus Druckschrift D1 in Verbindung mit Druckschrift D3 und ist daher wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

6. Das Zusatzmerkmal f des Anspruchs 1 nach Hilfsantrag 4, wonach die erste Datenverbindung eine NFC-Verbindung ist, ist aus Druckschrift D1 bekannt, vgl. deren Fig. 2A *(NFC 206, 207)*, und das Zusatzmerkmal f1 des Anspruchs 1 nach Hilfsantrag 5, wonach die zweite Datenverbindung eine Authentifizierung erfordert, entnimmt der Fachmann in naheliegender Weise der Druckschrift D1, wie bereits zum Hilfsantrag 2 ausgeführt wurde.

Die Verfahren der Ansprüche 1 nach den Hilfsanträgen 4 und 5 ergeben sich somit in naheliegender Weise aus Druckschrift D1 in Verbindung mit Druckschrift D3 und sind wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

7. Das Zusatzmerkmal f2 des Anspruchs 1 nach Hilfsantrag 6, dass das Authentifizierungselement vom Authentifizierungsdatenserver die gesamten Authentifizierungsdaten bildet, entnimmt der Fachmann ebenfalls in naheliegender Weise der Druckschrift D1, denn deren Abs. [0063] ist zu entnehmen, dass mit dem Passwort als Authentifizierungselement die Authentifizierung erfolgt. Da in dieser Fundstelle keine weiteren zur Authentifizierung notwendigen Daten angeführt sind, folgt daraus auch, dass das Authentifizierungselement vom Authentifizierungsdatenserver die gesamten Authentifizierungsdaten bildet.

Das Verfahren des Anspruchs 1 nach Hilfsantrag 6 ergibt sich somit in naheliegender Weise aus Druckschrift D1 in Verbindung mit Druckschrift D3 und ist daher wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

8. Das Zusatzmerkmal g des Anspruchs 1 von Hilfsantrag 7, wonach das Authentifizierungselement direkt vom Authentifizierungsdatenserver an das Zahlungsendgerät ohne Zwischenspeicherung auf der mobilen Einheit übertragen wird, versteht der Fachmann dahingehend, dass keine permanente Speicherung des Authentifizierungselements der mobilen Einheit erfolgt.

Dieses Merkmal ist jedoch zwangsweise erfüllt, wenn die Authentifizierungsdaten entsprechend Merkmal e vom Authentifizierungsdatenserver zum Zahlungsendgerät in einem verschlüsselten Tunnel durch die mobile Einheit getunnelt werden.

Das Verfahren des Anspruchs 1 nach Hilfsantrag 7 ergibt sich somit in naheliegender Weise aus Druckschrift D1 in Verbindung mit Druckschrift D3 und ist daher wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

9. Wie bereits im Zusammenhang mit Hilfsantrag 2 erläutert, entnimmt der Fachmann auch das Zusatzmerkmal h des Anspruchs 1 von Hilfsantrag 8, wonach die zweite Datenverbindung eine Authentifizierung durch die Eingabe eines Passworts oder einer PIN durch den Benutzer der mobilen Einheit erfordert, der Druckschrift D1, vgl. die dort angeführten Fundstellen.

10. Für die auf ein Computerprogrammprodukt, eine mobile Einheit und ein Telekommunikationssystem gerichteten selbständigen Ansprüche nach Hauptantrag und nach den Hilfsanträgen 1 bis 8 gelten obige Ausführungen in gleicher Weise.

11. Es kann dahingestellt bleiben, ob die Gegenstände der abhängigen oder selbständigen Ansprüche des Hauptantrags und der Hilfsanträge 1 bis 8 patentfähig sind, denn wegen der Antragsbindung im Patenterteilungsverfahren fallen mit dem Patentanspruch 1 auch die mittelbar oder unmittelbar auf die selbständigen Patentansprüche rückbezogenen Unteransprüche *(vgl. BGH GRUR 2007, 862, 863 Tz. 18 – Informationsübermittlungsverfahren II m. w. N.)*.

12. Bei dieser Sachlage war die Beschwerde der Anmelderin zurückzuweisen.

R e c h t s m i t t e l b e l e h r u n g

Gegen diesen Beschluss steht der Anmelderin – vorbehaltlich des Vorliegens der weiteren Rechtsmittelvoraussetzungen, insbesondere des Vorliegens einer Beschwer – das Rechtsmittel der **Rechtsbeschwerde** zu. Da der Senat die Rechtsbeschwerde nicht zugelassen hat, ist sie nur statthaft, wenn einer der nachfolgenden Verfahrensmängel gerügt wird, nämlich

1. dass das beschließende Gericht nicht vorschriftsmäßig besetzt war,
2. dass 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. dass einem Beteiligten das rechtliche Gehör versagt war,
4. dass ein Beteiligter im Verfahren nicht nach Vorschrift des Gesetzes vertreten war, sofern er nicht der Führung des Verfahrens ausdrücklich oder stillschweigend zugestimmt hat,
5. dass der Beschluss aufgrund einer mündlichen Verhandlung ergangen ist, bei der die Vorschriften über die Öffentlichkeit des Verfahrens verletzt worden sind, oder
6. dass der Beschluss nicht mit Gründen versehen ist.

Die Rechtsbeschwerde ist **innerhalb eines Monats** nach Zustellung des Beschlusses

schriftlich durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten beim Bundesgerichtshof, Herrenstr. 45 a, 76133 Karlsruhe, einzureichen oder

durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten in elektronischer Form bei der elektronischen Poststelle des BGH,

www.bundesgerichtshof.de/erv.html. Das elektronische Dokument ist mit einer prüfbaren qualifizierten elektronischen Signatur nach dem Signaturgesetz oder mit einer prüfbaren fortgeschrittenen elektronischen Signatur zu versehen. Die Eignungsvoraussetzungen für eine Prüfung und für die Formate des elektronischen Dokuments werden auf der Internetseite des Bundesgerichtshofs www.bundesgerichtshof.de/erv.html bekannt gegeben.

Dr. Strößner Brandt Dr. Friedrich Dr. Himmelmann

prö