BUNDESPATENTGERICHT

18 W (pat) 182/14

(Aktenzeichen)

B E S C H L U S S

In der Beschwerdesache

betreffend die Patentanmeldung 10 2004 026 933.5-53

…

hat der 18. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts am 27. September 2017 durch die Vorsitzende Richterin Dipl.-Ing. Wickborn sowie die Richter Kruppa, Dipl.-Ing. Altvater und Dr.-Ing. Flaschke

beschlossen:

Auf die Beschwerde des Anmelders wird der Beschluss der Prüfungsstelle für Klasse G 06 F des Deutschen Patent- und Markenamts aufgehoben und das Patent auf der Grundlage der folgenden Unterlagen erteilt:

- Patentansprüche 1 bis 8 nach Hauptantrag, eingegangen am 23. August 2017,

- Beschreibung, Seiten 1 und 1a, eingegangen am 28. Juli 2017, Seiten 2, 3, 5, 7 und 7a, eingegangen am 10. April 2013, Seiten 4 und 6, eingegangen am 23. August 2017 und Seiten 8 bis 10, eingegangen am 1. Juli 2004,

- Figuren 1 und 2A bis 2C, eingegangen am 1. Juli 2004.

Gründe

I.

Die am 1. Juni 2004 beim Deutschen Patent- und Markenamt eingereichte Patentanmeldung 10 2004 026 933.5 mit der Bezeichnung

„System und Verfahren zur Authentifizierung eines Benutzers“

wurde durch Beschluss der Prüfungsstelle für Klasse G 06 F des Deutschen Patent- und Markenamtes vom 22. April 2013 im Umfang des damals geltenden Hauptantrags „mangels hinreichender Rechtssicherheit für Dritte“ zurückgewiesen. Insbesondere gebe der „Anspruch 1 des Hauptantrags der Allgemeinheit des

beanspruchten Schutzbegehrens keine ausreichende Rechtssicherheit für Dritte“, da „unklar [sei], was damit gemeint sein soll, dass ein geschlossener logischer Kanal zwischen der sicherheitssensiblen Ressource und dem Zugangspunkt eingerichtet wird“.

Gegen diesen Beschluss ist die Beschwerde des Anmelders gerichtet.

Zugleich hat die Prüfungsstelle ein Patent mit den Ansprüchen gemäß Hilfsantrag 1 erteilt.

Im Prüfungsverfahren wurden folgende Druckschriften genannt:

D1: WO 03/102882 A1
D2: DE 100 09 456 A1
D3: US 2002/0053035 A1
D4: US 5 553 239 A
D5: WO 2004/032019 A2
D6: DE 197 49 090 A1
D7: US 2002/0081971 A1
D8: EP 1 303 102 A2.

Darüber hinaus wurde im Rechercheverfahren nach § 43 PatG folgende Druckschrift ermittelt:

D9: EP 13 87 323 A1.

Der Anmelder stellt sinngemäß den Antrag, zuletzt mit Schriftsatz vom 22. August 2017,

> den Beschluss der Prüfungsstelle aufzuheben und das Patent auf der Grundlage folgender Unterlagen zu erteilen:

gemäß Hauptantrag mit
Patentansprüchen 1 bis 8, eingegangen am 23. August 2017,
Beschreibung, Seiten 1 und 1a, eingegangen am 28. Juli 2017, Seiten 2, 3, 5, 7 und 7a, eingegangen am 10. April 2013, Seiten 4 und 6, eingegangen am 23. August 2017 und Seiten 8 bis 10, eingegangen am 1. Juli 2004, und
Figuren 1 und 2A bis 2C, eingegangen am 1. Juli 2004.

Der seitens des Senats mit einer Gliederung versehene **Patentanspruch 1 nach Hauptantrag** lautet:

M1 „System zur Authentifizierung mindestens eines Benutzers für den Zugriff auf eine sicherheitssensible Ressource

M2 - mit mindestens einer sicherheitssensiblen Ressource, wobei die sicherheitssensible Ressource ein Datenspeicher, eine Einrichtung zum Zugreifen auf einen mobilen Datenspeicher oder eine Chipkartenschnittstelle ist,

M3 - mit mindestens einer Einrichtung zum Einlesen der Informationen mindestens einer Identifizierungseinrichtung,

M4 - mit mindestens einer Einrichtung zur Eingabe mindestens eines persönlichen Identifikationsmerkmals in Form einer persönlichen Identifikationsnummer (PIN), eines Passworts oder eines biometrischen Merkmals,

M5 - mit mindestens einem Zugangspunkt mit einer Einrichtung zum Auslesen eines Transponders und

M6 - mit mindestens einem Transponder, wobei jedem Transponder mindestens eine sicherheitssensible Ressource zugeordnet ist, und jedem persönlichen Identifikationsmerkmal genau ein Transponder zugeordnet ist,

M7 - wobei die sicherheitssensible Ressource über ein Datennetzwerk mit dem Zugangspunkt verbunden ist,

- wobei das System so ausgestaltet ist, dass

M8 - sich ein Benutzer während eines vorgegebenen Zeitabschnitts einmal durch Einlesen seiner Identifizierungseinrichtung und durch Eingabe seines persönlichen Identifikationsmerkmals als rechtmäßiger Benutzer identifiziert und

M9 nach der Identifizierung des Benutzers durch das Einlesen der Identifizierungseinrichtung und des persönlichen Identifikationsmerkmals ein geschlossener logischer Kanal zwischen der sicherheitssensiblen Ressource und dem mindestens einen Zugangspunkt eingerichtet wird, der dem Paar aus der sicherheitssensiblen Ressource und dem Transponder zugeordnet ist,

M10 - der logische Kanal zur Kommunikation zwischen dem Zugangspunkt und der sicherheitssensiblen Ressource danach als Reaktion auf das Auslesen des Transponders geöffnet wird, wenn der Benutzer seinen individuellen Transponder gegenüber dem Zugangspunkt präsentiert, und die Kennung des Transponders mit derjenigen Kennung des Transponders übereinstimmt, welcher dem persönlichen Identifikationsmerkmal zugeordnet ist,

M11 der logische Kanal nach Abschluss eines Zugriffs auf die sicherheitssensible Ressource wieder geschlossen wird."

Der seitens des Senats mit einer Gliederung versehene **Patentanspruch 7 nach Hauptantrag** lautet:

N1 „Verfahren zur Authentifizierung mindestens eines Benutzers für den Zugriff auf eine sicherheitssensible Ressource in einem System

N2 mit mindestens einer sicherheitssensiblen Ressource, wobei die sicherheitssensible Ressource ein Datenspeicher, eine Einrichtung zum Zugreifen auf einen mobilen Datenspeicher oder eine Chipkartenschnittstelle ist,

N3 mit mindestens einem Zugangspunkt und mindestens einem Transponder

N4 - wobei in das System die Informationen mindestens einer Identifizierungseinrichtung eingelesen werden

N5 - wobei die Ressource und der mindestens eine Zugangspunkt über ein Datennetzwerk miteinander kommunizieren,

N6 - wobei in das System mindestens ein persönliches Identifikationsmerkmal des Benutzers in Form einer persönlichen Identifikationsnummer (PIN), eines Passworts oder eines biometrischen Merkmals eingelesen wird,

N7 - wobei der sicherheitssensiblen Ressource mindestens ein Transponder zugeordnet wird, und jedem persönlichen Identifikationsmerkmal genau ein Transponder zugeordnet wird,

N8 - wobei der Zugangspunkt die Möglichkeit aufweist, den Transponder auszulesen,

N9 - wobei sich ein Benutzer während eines vorgegebenen Zeitabschnitts einmal durch Einlesen seiner Identifizierungseinrichtung und durch Eingabe seines persönlichen Identifikationsmerkmals als rechtmäßiger Benutzer identifiziert und

N10 nach der Identifizierung des Benutzers durch das Einlesen der Identifizierungseinrichtung und des persönlichen Identifikationsmerkmals ein geschlossener logischer Kanal zwischen der sicherheitssensiblen Ressource und dem mindestens einen Zugangspunkt eingerichtet wird, der dem Paar aus der sicherheits

sensiblen Ressource und dem Transponder zugeordnet ist,

N11 - wobei der logische Kanal zur Kommunikation zwischen dem Zugangspunkt und der sicherheitssensiblen Ressource danach als

Reaktion auf das Auslesen des Transponders geöffnet wird, wenn der Benutzer seinen individuellen Transponder gegenüber dem Zugangspunkt präsentiert, und die Kennung des Transponders mit derjenigen Kennung des Transponders übereinstimmt, welcher dem persönlichen Identifikationsmerkmal zugeordnet ist, und

N12 - wobei der logische Kanal nach Abschluss eines Zugriffs auf die sicherheitssensible Ressource wieder geschlossen wird."

Wegen der auf den Patentanspruch 1 nach Hauptantrag rückbezogenen Ansprüche 2 bis 6 und des auf den Patentanspruch 7 nach Hauptantrag rückbezogenen Patentanspruchs 8 wird auf die Akte verwiesen.

Der Anmelder macht hierzu geltend, dass die geltenden Ansprüche nach Hauptantrag zulässig und im Lichte des im Verfahren befindlichen Standes der Technik patentfähig seien.

Bezüglich der weiteren Einzelheiten wird auf den Akteninhalt verwiesen.

II.

Die zulässige Beschwerde hat in der Sache Erfolg. Sie führt zur Aufhebung des angefochtenen Beschlusses und zur Erteilung des nachgesuchten Patents in der Fassung des Hauptantrags.

1. Die Anmeldung betrifft ein System und ein Verfahren zur Authentifizierung mindestens eines Benutzers für den Zugriff auf eine sicherheitssensible Ressource. Gemäß der Beschreibungseinleitung seien aus dem Stand der Technik Systeme zur Authentifizierung von Benutzern für den Zugriff auf sicherheitssensible Ressourcen bekannt (vgl. geltende Beschreibung, S. 1, Z. 42-43).

Die bekannten Systeme und Verfahren zur Identifizierung von Benutzern erforderten aber für jeden Zugriff auf die sicherheitssensible Ressource des Systems die Eingabe eines persönlichen Identifikationsmerkmals, beispielsweise einer PIN oder eines biometrischen Merkmals. Dies erweise sich als nachteilig in Systemen, bei denen die Benutzer in einer für Dritte einsehbaren oder zugänglichen Umgebung auf die sicherheitssensiblen Ressourcen zugreifen müssten. Selbst wenn sich die sicherheitssensible Ressource an einem für Dritte nicht zugänglichen Ort befinde, so müsse sich der Benutzer vor deren Benutzung durch Eingabe seines Identifikationsmerkmals authentisieren. Geschehe dies beispielsweise in einem Laden, so hätten Dritte die Möglichkeit, die PIN des Benutzers auszuspähen und missbräuchlich zu benutzen. Darüber hinaus sei die Eingabe der PIN zeitaufwendig (vgl. geltende Beschreibung, S. 2, Z. 12-22). Besondere Relevanz erhalte das beanspruchte System durch Einführung der Gesundheitskarte zur Verknüpfung der einzelnen Institutionen, beispielsweise von Ärzten und Apothekern, staatlicher oder halbstaatlicher Gesundheitssysteme untereinander und mit den Daten der Patienten, die auf sogenannten elektronischen Gesundheitskarten (eGK) gespeichert seien. Dabei seien für den Zugriff auf die Daten auf der eGK hohe Anforderungen in Bezug auf die Datensicherheit zu stellen (vgl. geltende Beschreibung, S. 3, Z. 31 - 36).
Als **Aufgabe** wird in der geltenden Beschreibungseinleitung (S. 3, Z. 12-16) sinngemäß angegeben, ein System und ein Verfahren zur Authentifizierung eines Benutzers für den Zugriff auf mindestens eine sicherheitssensible Ressource bereitzustellen, welche einen schnellen und sicheren Zugriff auf die sicherheitsrelevanten Ressourcen ermöglichen.

Das **objektive technische Problem** liegt darin, ein System und ein Verfahren zur Authentifizierung eines Benutzers für den Zugriff auf mindestens eine sicherheitssensible Ressource bereitzustellen, bei dem verschiedene Benutzer über verschiedene Zugangspunkte auf sicherheitsrelevante Ressourcen zugreifen können, ohne dass bei jedem Zugriff eine Signaturkarte eingelesen und eine persönliche Identifikationsnummer eingegeben werden müssen.

Der zuständige **Fachmann** weist eine abgeschlossene Hochschulausbildung auf dem Gebiet der Elektrotechnik oder Informationstechnik auf und verfügt über eine mehrjährige Erfahrung auf dem Gebiet der Systemsicherheit und in der Anwendung von Authentisierungsverfahren.

Diese Aufgabe soll durch die Merkmale des auf ein System gerichteten **Anspruchs 1 nach Hauptantrag** gelöst werden, in welchem mit Hilfe eines persönlichen Identifikationsmerkmals ein geschlossener logischer Kanal zur Kommunikation zwischen einem Zugangspunkt und einer sicherheitssensiblen Ressource eingerichtet wird. Als Reaktion auf das Auslesen eines Transponders an einem Zugangspunkt wird der logische Kanal geöffnet und nach dem Zugriff auf die sicherheitssensible Ressource wieder geschlossen.

Die Aufgabe soll weiter durch die Merkmale des nebengeordneten **Anspruchs 7 nach Hauptantrag** gelöst werden, welcher entsprechende Verfahrensmerkmale umfasst.

2. Einige Merkmale bedürfen der Auslegung.

Der Anspruch 1 betrifft ein System zur Authentifizierung mindestens eines Benutzers für den Zugriff auf eine sicherheitssensible Ressource (**Merkmal M1**). In der Beschreibung wird ausgeführt, dass dieses System bevorzugt für Apotheken vorgesehen sei, um damit auf Patientendaten zugreifen zu können. Der Benutzer des Systems ist in diesem Anwendungsfall der Apotheker bzw. Apothekenmitarbeiter. Patientendaten, auf die der Apotheker zugreifen möchte, können auf der elektronischen Gesundheitskarte (eGK) eines Patienten gespeichert sein. Das System kann aber auch an ein apothekenübergreifendes Datennetzwerk angeschlossen sein, über welches die Patientendaten ausgetauscht werden können (vgl. Offenlegungsschrift, Abs. [0036] i. V. m. Abs. [0011], [0017]).

Das Auslesen und Abspeichern von Patientendaten erfolgt in diesem Beispiel über einen Rechner, der an einem zentralen Platz in der Apotheke steht (vgl. Fig. 1, Bezugszeichen 4 u. Abs. [0018]). Der zentrale Rechner umfasst mindestens eine sicherheitssensible Ressource (vgl. Fig. 1, Bezugszeichen 2, 3 Abs. [0001] u. [0037]). Bei der sicherheitssensiblen Ressource handelt es sich z. B. um einen Datenspeicher. Die Ressource kann aber auch eine Einrichtung zum Zugreifen auf einen mobilen Datenspeicher oder ein Anwendungsprogramm sein (z. B. Zugriff auf USB-Stick oder Lesegerät für Chipkarte; vgl. Abs. [0014], [0015]; vgl. **Merkmal M2**). Bei der sicherheitssensiblen Ressource handelt es sich nicht um z. B. die Health-Professional Card selbst. Vielmehr ist die sicherheitssensible Ressource als eine Einrichtung zum Auslesen einer solchen Chipkarte zu verstehen (vgl. hierzu Abs. [0015] i. V. m. Abs. [0037]).

Um auf Patientendaten zugreifen zu können, muss sich der Benutzer am System autorisieren. Hierfür dienen Einrichtungen zur Eingabe von persönlichen Identifikationsmerkmalen (z. B. Passwort, PIN, Fingerabdruck, Chipkarte; vgl. urspr. Anspruch 1 i. V. m. Abs. [0013]). So soll das System mindestens eine Einrichtung zur Eingabe einer persönlichen Identifikationsnummer (PIN), eines Passwortes oder eines biometrischen Merkmals umfassen (vgl. **Merkmal M4**). Es erhöht die Sicherheit des Systems, wenn das System zusätzlich mindestens eine Einrichtung zum Einlesen der Information einer Identifizierungseinrichtung aufweist (vgl. **Merkmal M3**). Der Fachmann versteht die Identifizierungseinrichtung als ein Ausweisdokument, die als Signaturkarte ausgebildet sein kann (vgl. Health-Professional Card). Sie berechtigt den Apotheker, auf Patientendaten zuzugreifen. Während eines vorgegebenen Zeitabschnitts, z. B. eines Arbeitstags, identifiziert sich ein Benutzer einmal als rechtmäßiger Benutzer. Die Authentifizierung erfolgt am zentralen Rechner der Apotheke durch Einlesen der Identifizierungseinrichtung (also z. B. der Signaturkarte) und durch Eingabe des persönlichen Identifikationsmerkmals (vgl. **Merkmal M8**).

Die sicherheitssensible Ressource ist über ein Datennetzwerk mit mindestens einem Zugangspunkt verbunden (vgl. Fig. 1; vgl. **Merkmal M7**). Der Zugangspunkt kann eine Verkaufsstelle bzw. ein Kassenterminal im Verkaufsraum einer

Apotheke sein (vgl. Abs. [0039]). Idealerweise verfügt das System über mehrere Verkaufsstellen, die vom zentralen Rechner räumlich getrennt sind (vgl. Abs. [0018]).

Des Weiteren verfügt das System über mindestens einen personenbezogenen Transponder. Dabei handelt es sich um eine Chipkarte, die der Benutzer mit sich trägt. Jeder Zugangspunkt verfügt über eine Einrichtung, mit der die Transponder (bevorzugt berührungslos) ausgelesen werden können (vgl. Abs. [0022]; vgl. **Merkmal M5**).

Dem jeweiligen Transponder wird mindestens eine Ressource zugeordnet. Zudem ist jedem persönlichen Identifikationsmerkmal genau ein Transponder zugeordnet (vgl. Abs. [0040]; **Merkmal M6**). Die Zugehörigkeit wird abgespeichert und es wird ein geschlossener logischer Kanal eingerichtet, der dem Transponder/Ressourcenpaar zugeordnet ist. Der geschlossene logische Kanal wird zwischen der sicherheitssensiblen Ressource und den Zugangspunkten eingerichtet (vgl. Fig. 1, Bezugszeichen 9a, 9b i. V. m. den ursprünglichen Ansprüchen 18, 19 i. V. m. Abs. [0029]); **Merkmal M9**). Damit steht der geschlossene logische Kanal zur Kommunikation zwischen einem beliebigen Zugangspunkt und der personalisierten Ressource bereit, er ist jedoch vorerst nicht freigegeben (vgl. Abs. [0040]).

Der Fachmann versteht unter dem geschlossenen logischen Kanal eine Softwareverbindung zwischen den in einem physikalischen Netz eingebundenen Netzwerkkomponenten. Er kennt diese Modellbetrachtung aus den Grundlagen der Systemtechnik, wobei in einem Datennetzwerk zunächst nur eine Socket-Verbindung aufgebaut wird, um Parameter und IP-Adressen auszutauschen. Das eigentliche Handshake findet zu diesem Zeitpunkt noch nicht statt. Erst wenn die Kennung eines detektierten Transponders mit derjenigen Kennung des Transponders übereinstimmt, welcher den persönlichen Identifikationsmerkmalen eines Benutzers zugeordnet ist, wird der logische Kanal zwischen dem jeweiligen Zugangspunkt und der sicherheitssensiblen Ressource freigeschaltet und der Benutzer kann auf die Patientendaten zugreifen (vgl. Abs. [0010]; **Merkmal M10**). Nach einem Zugriff auf die sicherheitssensible Ressource wird der logische Kanal wieder geschlossen, z. B. wenn der Transponder aus der Umgebung des

Zugangspunktes entfernt wird (vgl. Abs. [0026]; **Merkmal M11**). Der Transponder ist demnach als Nebenschlüssel im Rahmen einer Mehrfachauthentifizierung zu verstehen (vgl. Abs. [0010]).

3. Die Patentansprüche 1 bis 8 nach Hauptantrag sowie die Änderungen in der Beschreibung sind zulässig (§ 38 PatG).

Die Merkmale des Anspruchs 1 nach Hauptantrag sind durch die ursprünglichen Patentansprüche 1, 5 und 8 sowie die ursprünglich eingereichte Beschreibung (vgl. S. 1, erster Abs., S. 3, Z. 11-S. 4, Z. 35, S. 5, Z. 15 - 22, S. 6, vorletzter u. letzter Abs., S. 7, dritter Abs. u. S. 9, erster Abs.) in Verbindung mit Figur 1 als zur Erfindung zugehörend offenbart. Insbesondere ist den Anmeldeunterlagen zu entnehmen, dass sowohl die Identifiziereinrichtung (Merkmal M3) als auch die PIN (Merkmal M4) zu den persönlichen Identifikationsmerkmalen zählen. Die Einrichtungen zum Einlesen bzw. Eingeben der Identifikationsmerkmale können sowohl am Zugangspunkt als auch an der Ressource vorgesehen sein. Ursprünglich offenbart ist auch Merkmal M9, wonach nach der Identifizierung des Benutzers durch das Einlesen der Identifiziereinrichtung und des persönlichen Identifikationsmerkmals ein geschlossener logischer Kanal, der dem Paar aus der sicherheitssensiblen Ressource und dem Transponder zugeordnet ist, zwischen der sicherheitssensiblen Ressource und den Zugangspunkten bzw. dem mindestens einen Zugangspunkt eingerichtet wird (vgl. urspr. Ansprüche 18, 19 i. V. m. S. 6, vorletzter Abs. - S. 7, erster Abs. u. S. 9, Z. 9 - 11 der urspr. Beschreibung). Die Merkmale M10 und M11 waren inhaltlich bereits im ursprünglichen Anspruch 1 in Verbindung mit Seite 5, zweiter Absatz, Seite 6, vierter Absatz und Seite 9, zweiter Absatz der ursprünglichen Beschreibung enthalten.

Der nebengeordnete Verfahrensanspruch 7 nach Hauptantrag basiert auf dem ursprünglichen Patentanspruch 14 und wurde analog zum Anspruch 1 geändert. Die ursprünglichen abhängigen Ansprüche 2 bis 6, 8 und 13 sowie 15 bis 20

wurden gestrichen. Die Nummerierung der übrigen abhängigen Ansprüche sowie deren Rückbezüge wurden angepasst.

In der Beschreibung wurden redaktionelle Änderungen vorgenommen. Zudem wurde der im Prüfungsverfahren ermittelte relevante Stand der Technik gewürdigt.

4. Die nebengeordneten Patentansprüche 1 und 7 nach Hauptantrag genügen den Anforderungen des § 34 Abs. 4 PatG. Der Zurückweisungsgrund trägt daher nicht.

Die Prüfungsstelle hat ihren Beschluss darauf gegründet, dass der Gegenstand des Anspruchs 1 nach Hauptantrag „unklar“ sei, dabei jedoch offensichtlich die Beschreibung wie auch die Figuren der Anmeldung zur Erfassung des Anspruchsgegenstands nicht herangezogen.

Für die Prüfung, ob der Gegenstand des Patentanspruchs gemäß den §§ 1 bis 5 PatG patentfähig ist, ist es grundsätzlich erforderlich, dass zunächst der Gegenstand des Patentanspruchs ermittelt wird, indem der Patentanspruch unter Heranziehung von Beschreibung und Zeichnungen aus der Sicht des von der Erfindung angesprochenen Fachmanns ausgelegt wird. Denn hierbei gelten die gleichen Grundsätze wie zur Bestimmung des Schutzbereichs (BGH, Beschluss vom 17. April 2007 - X ZB 9/06, GRUR 2007, 859, Amtlicher Leitsatz b), Abschnitt III. 3. a) - Informationsübermittlungsverfahren I; BGH, Urteil vom 13. Februar 2007 - X ZR 74/05, GRUR 2007, 410, Abschnitt III. 1. - Kettenradanordnung I; BGH, Beschluss vom 11. September 2013 – X ZB 8/12, GRUR 2013, 1210, Absatz III 1. a) - Dipeptidyl-Peptidase-Inhibitoren; BGH, Urteil vom 7. November 2000 - X ZR 145/98, GRUR 2001, 232, Amtlicher Leitsatz - Brieflocher).

Eine solche Auslegung ist im vorliegenden Prüfungsverfahren nicht erfolgt. In dem angefochtenen Beschluss führt die Prüfungsstelle aus, es sei „unklar, was damit gemeint sein soll, dass ein geschlossener logischer Kanal zwischen der sicherheitssensiblen Ressource und dem Zugangspunkt eingerichtet wird“. Wie vorstehend im Abschnitt II. 2. ausgeführt, versteht der Fachmann unter dem geschlossenen logischen Kanal eine Softwareverbindung, beispielsweise eine Socket-Verbindung. Dabei werden Datenstrukturen angelegt, wodurch es möglich ist, die Parameter, die diese Verbindung betreffen, gezielt festzulegen (vgl. Offenlegungsschrift, Abs. [0010] u. [0026] - [0029] i. V. m. Fig. 1). Der Anspruch lässt zwar teilweise offen, wie die Verbindungen zwischen den Zugangspunkten und den sicherheitssensiblen Ressourcen ausgestaltet sind, dies führt aber nicht zur Unklarheit oder mangelnden Ausführbarkeit, sondern zur Verallgemeinerung des Anspruchsgegenstands. Damit stellt der Ausdruck „geschlossener logischer Kanal“ nicht die Klarheit der technischen Lehre des Anspruchs in Frage, sondern die Modellbetrachtung der Kommunikationsverbindung führt vorliegend lediglich dazu, dass unter den Anspruch eine große Anzahl von Gegenständen fällt. Ein breit gefasster Anspruch ist für sich aber kein Grund zur Beanstandung (Schulte, 10. Aufl., § 34 PatG, Rdn. 141). Vielmehr ist gemäß BGH, Urteil vom 29. November 2013 - PatAnwZ 1/12, GRUR 2014, 510 im Interesse der Rechtssuchenden der Gehalt der Erfindung mit möglichst weitreichend zu formulierenden Patentansprüchen zu schützen. Ein solcher breit gefasster Anspruch muss dann für jeden seiner umfassten Gegenstände die Voraussetzungen für eine Patentierung erfüllen, d. h. er muss u. a. neu und erfinderisch sein (Schulte, 10. Aufl., § 34 PatG, Rdn. 142). Daher wäre der Anspruchsgegenstand in seiner Breite auf Vorliegen von Neuheit und erfinderischer Tätigkeit zu prüfen gewesen.

5. Die jeweiligen Gegenstände der unabhängigen Patentansprüche 1 und 7 nach Hauptantrag sind gegenüber dem im Verfahren befindlichen Stand der Technik neu (§ 3 PatG).

a) Zum Anspruch 1 nach Hauptantrag

Druckschrift **D1** (WO 03/102882 A1) beschreibt ein Authentifizierungsverfahren während eines Bezahlvorgangs in einem Online-Shop (vgl. S. 1; Z. 3-9 u. Brückenabs. S. 7/8). Hierfür wird ein System zur Authentifizierung mindestens eines Benutzers für den Zugriff auf einen Bankserver *AA* beschrieben (vgl. Fig. 1 u. Brückenabs. S. 7/8). Zweifellos verfügt der Bankserver über einen Datenspeicher oder auch über eine Einrichtung zum Zugreifen auf einen mobilen Datenspeicher. Diese können als sicherheitssensible Ressource verstanden werden (vgl. S. 9, letzter Abs.; **Merkmale M1, M2**). Des Weiteren umfasst das System einen Zugangspunkt *PT*, welcher über ein Datennetzwerk *WE* mit der sicherheitssensiblen Ressource *AA* verbunden ist, ohne dass eine Einrichtung zum Auslesen eines Transponders genannt ist (vgl. Fig. 1; S. 6, Z. 28-30; **teilweise Merkmal M5**, **Merkmal M7**). Der Zugangspunkt *PT* weist eine Einrichtung *LC* zum Einlesen der Information einer als Identifiziereinrichtung anzusehende Chip-Karte *CP* auf (Fig. 1 u. S. 7, Z. 27-29; **Merkmal M3**). Zusätzlich weist der Zugangspunkt eine Einrichtung zur Eingabe eines persönlichen Identifikationsmerkmals *PIN* auf (vgl. S. 8, Z. 3-5 u. Z. 27-28; **Merkmal M4**). Damit ist das System so ausgestaltet, dass sich ein Benutzer während eines vorgegebenen Zeitabschnitts einmal durch Einlesen seiner Identifizierungseinrichtung und durch Eingabe seines persönlichen Identifikationsmerkmals als rechtmäßiger Benutzer identifiziert (**Merkmal M8**). Neben der Eingabe der beiden persönlichen Identifikationsmerkmale ermöglicht das System eine Anwesenheitskontrolle des Benutzers in Form einer visuellen Sicherheitsabfrage. Der Fachmann versteht die Abfrage als eine Art Captcha. Diese ist dazu bestimmt, die physikalische Präsenz des Benutzers in der unmittelbaren Nähe des Zugangspunktes während der Online-Transaktion zu verifizieren (vgl. S .4, Z. 14-16 u. S. 12, Z. 12-26). Nach der Identifizierung des Benutzers durch das Einlesen der Identifizierungseinrichtung, des persönlichen Identifikationsmerkmals und der erfolgten Anwesenheitskontrolle wird ein logischer Kanal zwischen der sicherheitssensiblen Ressource und dem Zugangspunkt eingerichtet und ein

verschlüsseltes Zertifikat an die Authentifizierungsstelle gesendet, ohne dass ein geschlossener logischer Kanal eingerichtet wird, der einem Paar aus der sicherheitssensiblen Ressource und einem Transponder zugeordnet ist (vgl. Brückenabs. S. 3/4; **teilweise Merkmal M9**). Dieser Kanal ist nach dem Aufbau offen und kann für eine Banküberweisung verwendet werden. Nach dem Abschluss eines Zugriffs auf die sicherheitssensible Ressource wird der logische Kanal wieder geschlossen (**Merkmal M11**).
Im Gegensatz zum Anspruch 1 nach Hauptantrag offenbart Druckschrift D1 aber keinen Transponder, der einer sicherheitssensiblen Ressource zugeordnet ist und am Zugangspunkt ausgelesen werden kann. Insbesondere aber wird kein mehrstufiges Authentifizierungsverfahren beschrieben, bei dem durch das Einlesen der Chipkarte und einer PIN ein geschlossener logischer Kanal zwischen der Ressource und dem Zugangspunkt eingerichtet wird, der als Reaktion auf das Detektieren eines personalisierten Transponders freigeschaltet wird (Merkmale M5, M6, M9 und M10 fehlen).

Druckschrift **D2** (DE 100 09 456 A1) offenbart ein System zur Authentifizierung mindestens eines Benutzers für den Zugriff auf einen Computer (vgl. Anspruch 1). Das Computersystem umfasst mindestens einen Datenspeicher. Dieser kann als sicherheitssensible Ressource angesehen werden (vgl. Sp. 1, Z. 8, 9; **Merkmale M1, M2**). Des Weiteren umfasst das System eine Computermaus mit einer Transponderleseeinrichtung (vgl. Fig. 1, Sp. 4, Z. 54, 55). Diese kann als Zugangspunkt mit einer Einrichtung zum Auslesen eines Transponders verstanden werden (**Merkmal M5**). Beschrieben wird auch ein vom Benutzer des Computersystems mitzuführender Transponder. Zweifellos ist der Transponder über seinen Schlüssel einem Datenspeicher des Computers zugeordnet (**teilweise Merkmal M6**), der Transponder ist jedoch keinem persönlichen Identifikationsmerkmal zusätzlich zugeordnet.
Im Gegensatz zum Anspruch 1 nach Hauptantrag offenbart Druckschrift D2 aber kein System, bei dem die sicherheitssensible Ressource über ein Datennetzwerk mit dem Zugangspunkt verbunden ist. Des Weiteren fehlen die Merkmale, welche

die mehrstufige Authentifizierung im Sinne der vorliegenden Anmeldung ausmachen (Merkmale M3, M4 u. M6 bis M11 fehlen).

Druckschrift **D3** (US 2002/0053035 A1) befasst sich mit der Authentifizierung eines Benutzers im Internet. Es wird der Computer eines Benutzers beschrieben, der über das Internet mit mehreren Datenbanken eines Host-Servers (z. B. Geldinstitut) verbunden ist (vgl. Fig. 3 u. Abs. [0008], [0026]). Die Datenbanken können als sicherheitssensible Ressource und der Personal Computer als Zugangspunkt verstanden werden, ohne eine Einrichtung zum Auslesen eines Transponders zu nennen (**Merkmale M1, M2, M7, teilweise Merkmal M5**). Das System umfasst Einrichtungen zum Einlesen der Information mindestens einer Identifiziereinrichtung und zur Eingabe mindestens eines persönlichen Identifikationsmerkmals in Form einer PIN oder eines biometrischen Merkmals (vgl. Anspruch 1, Abs. [0009], [0010], [0026] u. [0028]; **Merkmale M3, M4 und M8**). Nach der Identifizierung des Benutzers wird ein logischer Kanal zwischen der sicherheitssensiblen Ressource und dem Zugangspunkt eingerichtet und ein verschlüsseltes Zertifikat an die Authentifizierungsstelle gesendet, ohne dass ein geschlossener logischer Kanal eingerichtet wird, der einem Paar aus der sicherheitssensiblen Ressource und einem Transponder zugeordnet ist (**teilweise Merkmal M9**,). Dieser Kanal ist nach dem Aufbau offen und kann für Bankgeschäfte verwendet werden (vgl. Abs. [0026]).
Im Gegensatz zum Anspruch 1 nach Hauptantrag offenbart Druckschrift D3 keinen Transponder, der einer sicherheitssensiblen Ressource zugeordnet ist und am Zugangspunkt ausgelesen werden kann. Insbesondere aber wird kein zweistufiges Authentifizierungsverfahren beschrieben, bei dem zunächst ein geschlossener logischer Kanal zwischen der Ressource und dem Zugangspunkt eingerichtet wird, der als Reaktion auf das Detektieren eines personalisierten Transponders freigeschaltet wird (Merkmale M5, M6, M9 und M10 fehlen).

Die Druckschriften **D4** (US 5 553 239 A) und **D5** (WO 2004/032019 A2) sind nicht relevant. Druckschrift **D4** betrifft ein System zum Aufbauen einer Telekom-

munikationsverbindung zwischen einem Host und einer Vielzahl von Clients (vgl. Anspruch 1, Sp. 3, Z. 58-61). Zwischen den Clients werden TCP/IP-Verbindungen aufgebaut (vgl. Anspruch 1). Es werden weder Einrichtungen zum Einlesen oder Eingeben von persönlichen Identifikationsmerkmalen noch eine Einrichtung zum Auslesen eines Transponders beschrieben, um eine logische Verbindung zwischen den einzelnen Clients und dem Server herstellen zu können. Druckschrift **D5** betrifft ein Assetmanagementsystem in einer medizinischen Einrichtung. Dabei können einzelne Assets (d. h. Ärzte, Pfleger, Patienten sowie medizinische Geräte) mit Hilfe von RFID-Tags identifiziert und lokalisiert werden. Das Überwachungssystem umfasst einen Server sowie eine Vielzahl mobiler Geräte (vgl. S. 1, Z. 10-12 u. Ansprüche 1, 7, 13). Eine Authentifizierung wird nicht beschrieben.

Druckschrift **D6** (DE 197 49 090 A1) beschreibt ein System zum Schutz eines Computers vor einem unberechtigten Zugriff bzw. zur Authentifizierung mindestens eines Benutzers für den Zugriff auf den Computer (vgl. Anspruch 1 u. Sp. 7, Z. 35-39). Die Offenbarung geht davon aus, dass die zu schützende sicherheitssensiblen Ressourcen die Programme, Datenbanken und Speicher des Computers sind (vgl. Sp. 3, Z. 15-21 u. Sp. 7, Z. 35-39; **Merkmale M1, M2**). Der Computer weist unterschiedliche Bedienungsvorrichtungen auf (vgl. Fig. 2, Tastatur 34, Maus 36), die der Fachmann als Zugangspunkte versteht. Die Zugangspunkte sind über Verbindungsleitungen, jedoch nicht über ein Datennetzwerk, mit der sicherheitssensiblen Ressource verbunden (vgl. Fig. 2, Bezugszeichen 16, 18; **teilweise Merkmal M7**). Dabei umfasst mindestens ein Zugangspunkt eine Einrichtung zum Auslesen eines Transponders (vgl. Bezugszeichen 42, 46 in Fig. 2, 3 u. Anspruch 1-3; **Merkmal M5**). Vorgesehen sind mehrere Transponder, wobei jedem Transponder mindestens eine sicherheitssensible Ressource zugeordnet ist (vgl. Sp. 7, Z. 33-39; **Merkmal M6**). Das System ist so ausgestaltet, dass sich ein Benutzer während eines vorgegebenen Zeitabschnitts durch die Eingabe von persönlichen Identifikationsmerkmalen als rechtmäßiger Benutzer identifiziert (vgl. Anspruch 1, **Merkmal M8**). So dient die Tastatur 34 als Einrichtung zur Eingabe eines persönlichen Identifikationsmerk-

mals in Form einer persönlichen Identifikationsnummer (vgl. Fig. 2 i. V. m. Anspruch 4; **Merkmal M4**). Zudem verfügt das System über mindestens eine Einrichtung zum Einlesen der Informationen mindestens einer Identifizierungseinrichtung. Es können sowohl ein Mikrofon als auch eine Kamera zur Erzeugung von biometrischen Daten des Benutzers herangezogen werden (vgl. Sp. 6, Z. 60-65; **Merkmal M3**). Entsprechend der Beschreibung in Spalte 3, Zeilen 11 bis 32 werden die Autorisierungsdaten und die Identifikationsdaten innerhalb des Computers zusammengeführt. Werden sowohl die Autorisierungsdaten als auch die Identifikationsdaten als richtig erkannt, so wird der PC zur Benutzung freigegeben. Der Computer ermöglicht dann gegebenenfalls auch einen Zugriff auf das Netzwerk, in welches er eingebunden ist (vgl. Sp. 1, Z. 8-17).
Im Gegensatz zum Anspruch 1 nach Hauptantrag offenbart Druckschrift D6 keine Verbindung der sicherheitssensiblen Ressource und des Zugangspunktes über ein Datennetzwerk. Entgegen dem Authentifizierungsverfahren gemäß der vorliegenden Anmeldung werden gemäß der Lehre von Druckschrift D6 die Autorisierungsdaten und die Identifikationsdaten innerhalb des Computers zusammengeführt, um die sicherheitssensiblen Ressourcen des Rechner freizugeben. Dabei erfolgt die Eingabe der persönlichen Identifikationsmerkmale erst nach dem Auslesen des Transponders (vgl. Sp. 3, Z. 58-66). Zudem ist in Druckschrift D6 nicht offenbart, dass ein geschlossener logischer Kanal zwischen der Ressource und dem Zugangspunkt eingerichtet wird, der als Reaktion auf das Detektieren eines personalisierten Transponders freigeschaltet wird. Demnach wird auch nicht beschrieben, dass der logische Kanal nach Abschluss eines Zugriffs auf die sicherheitssensible Ressource wieder geschlossen wird (Merkmale M7, M9, M10 und M11 fehlen).

In Druckschrift **D7** (US 2002/0081971 A1) ist ein Funkverfahren für den Bluetooth-Standard beschrieben, dessen Vorteil es ist, eine abgerissene Funkverbindung zwischen zwei Endgeräten schnell wieder aufzubauen (vgl. Abs. [0027] - [0029]). Druckschrift D7 befasst sich in keiner Weise mit Zugriffsrechten oder vertrauens-

würdigen Kanälen, insbesondere nicht mit einer mehrstufigen Authentifizierung für den Zugriff auf sicherheitssensible Ressourcen.

Druckschrift **D8** (EP 1 303 102 A2) betrifft ein Computernetzwerk, in dem verschiedene drahtgebundene und drahtlose Geräte (*Clients*) auf einen sog. Provisioning-Server zugreifen, welcher das Verteilen von Software (z. B. *Applets*) unterstützt (vgl. Abs. [0022]). Der Server kann als sicherheitssensible Ressource und die Clients können als Zugangspunkte verstanden werden, die über ein Datennetzwerk miteinander verbunden sind (vgl. Fig. 1, Bezugszeichen 100, 110, 200; **Merkmale M2, M7**). Um ein ausgewähltes Applet herunterladen zu können, muss sich der Benutzer gegenüber der sicherheitssensiblen Ressource authentifizieren, worauf der Download beginnen kann (vgl. Abs. [0009]; **Merkmal M1**). Wird die Verbindung zwischen Client und Server unterbrochen, bevor ein Download erfolgreich abgeschlossen wurde, wird der vertrauenswürdige Kanal geschlossen. Dabei bleibt ein geschlossener logischer Kanal bestehen - solange bis ein Timer 335 abgelaufen ist. Demnach dient der Timer zum Abbauen des geschlossenen logischen Kanals, ohne dass ein geschlossener logischer Kanal eingerichtet wird, der einem Paar aus der sicherheitssensiblen Ressource und einem Transponder zugeordnet wird, und ohne dass der logische Kanal als Reaktion auf das Auslesen des Transponders geöffnet wird (vgl. Fig. 4 i. V. m. Abs. [0037]; **teilweise Merkmale M9 und M10**).
Druckschrift D8 offenbart keine zweite Authentifizierung durch die Präsentation eines Transponders, um einen geschlossenen logischen Kanal freizugeben. Der Zugriff auf die sicherheitssensible Ressource erfordert auch keine erneute Authentifizierung, wenn der logische Kanal zeitweise geschlossen wurde (zumindest die Merkmale M5, M6, M9, M10 und M11 fehlen).

Die im Rechercheverfahren nach § 43 PatG ermittelte Druckschrift **D9** (EP 1 387 323 A1) liegt nicht näher am Anmeldungsgegenstand als der im Prüfungsverfahren genannte Stand der Technik. Der Gegenstand von Druckschrift D9 betrifft eine tragbare Identifikationseinrichtung mit einer biometrischen

Authentifizierungsvorrichtung. Insbesondere fehlt es der Lehre der Druckschrift D9 an den Merkmalen bezüglich des logischen Kanals (Merkmale M9 bis M11).

Der Gegenstand des Anspruchs 1 nach Hauptantrag ist daher neu gegenüber dem im Verfahren befindlichen Stand der Technik.

b) Zum Anspruch 7 nach Hauptantrag

Wie vorstehend bereits zum Gegenstand gemäß Anspruch 1 nach Hauptantrag ausgeführt, beschreiben die im Verfahren befindlichen Druckschriften kein System zur Authentifizierung mindestens eines Benutzers für den Zugriff auf eine sicherheitssensible Ressource, welches so ausgestaltet ist, dass nach der Identifizierung des Benutzers durch das Einlesen der Identifizierungseinrichtung und des persönlichen Identifikationsmerkmals ein geschlossener logischer Kanal zwischen der sicherheitssensiblen Ressource und dem Zugangspunkt eingerichtet wird, der dem Paar aus der sicherheitssensiblen Ressource und dem Transponder zugeordnet ist, dass der logische Kanal zur Kommunikation zwischen dem Zugangspunkt und der sicherheitssensiblen Ressource als Reaktion auf das Auslesen des Transponders geöffnet wird, wenn der Benutzer seinen individuellen Transponder gegenüber dem Zugangspunkt präsentiert, und dass der logische Kanal nach Abschluss eines Zugriffs auf die sicherheitssensible Ressource wieder geschlossen wird. Den Schriften sind auch die entsprechenden Verfahrensschritte nicht zu entnehmen.

Damit ist auch das Verfahren gemäß Anspruch 7 nach Hauptantrag neu gegenüber dem im Verfahren befindlichen Stand der Technik.

6. Die Gegenstände der unabhängigen Patentansprüche 1 und 7 nach Hauptantrag beruhen auf einer erfinderischen Tätigkeit (§ 4 PatG).

Wie vorstehend ausgeführt, ist keiner der im Verfahren befindlichen Druckschriften ein System zur Authentifizierung zu entnehmen, welches so ausgestattet ist, dass entsprechend den **Merkmalen M9** und **M10** gemäß Anspruch 1 nach Hauptantrag durch das Einlesen der Signaturkarte und der PIN ein geschlossener logischer Kanal zwischen der Ressource und dem Zugangspunkt eingerichtet wird, der als Reaktion auf das Detektieren eines personalisierten Transponders am Zugangspunkt freigeschaltet wird. Auch die hierzu im nebengeordneten Anspruch 7 beanspruchten, analogen Verfahrensschritte (**Merkmale N10** und **N11**) werden im genannten Stand der Technik nicht beschrieben.

Druckschrift **D6**, die als nächstliegender Stand der Technik anzusehen ist, befasst sich - ebenso wie die vorliegende Anmeldung - mit einem zweistufigen Sicherheitsschutz, mit dem durch Eingabe von Autorisierungs- und Identifikationsdaten auf eine sicherheitssensible Ressource zugegriffen wird. Ausgehend von dieser Schrift gibt es für den Fachmann aber keine Veranlassung, die sicherheitssensible Ressource und die Zugangspunkte über ein Datennetzwerk zu verbinden. Auch ist es nicht naheliegend, zwischen der Ressource und den Zugangspunkten einen geschlossenen logischen Kanal einzurichten, der erst als Reaktion auf das Auslesen des Transponders freigeschaltet wird. Denn die Verbindung zwischen dem Zugangspunkt und der sicherheitssensiblen Ressource ist in Druckschrift D6 ein Mauskabel. Für die Einrichtung eines vertrauenswürdigen logischen Kanals findet sich in Druckschrift D6 kein Anhaltspunkt. Selbst wenn der Fachmann das Netzwerk, in welches der Computer eingebunden sein kann, als sicherheitssensible Ressource betrachten würde, so käme er dennoch nicht zum vorliegenden Anmeldungsgegenstand. Denn auch in diesem Fall, besteht für den Fachmann keine Veranlassung, einen geschlossenen logischen Kanal im Sinne der vorliegenden Anmeldung einzurichten.

Der Fachmann hat auch keine Veranlassung, eine der anderen, im Verfahren befindlichen Druckschriften in Verbindung mit Druckschrift D6 zur Lösung seiner Aufgabe heranzuziehen.

Auch ausgehend von Druckschrift **D1** ergibt sich für den Fachmann keine Veranlassung, einen Transponder als Anwesenheitskontrolle einzusetzen. Selbst wenn er einen personenbezogenen Transponder verwenden würde, um die physikalische Präsenz des Benutzers in unmittelbarer Nähe des Zugangspunktes während einer Online-Transaktion sicherzustellen, käme er nicht zum vorliegenden Anmeldegegenstand. Denn diese Maßnahme führt nicht dazu, dass zwischen der Ressource und dem Zugangspunkt ein geschlossener logischer Kanal eingerichtet wird, der als Reaktion auf das Detektieren des Transponders freigeschaltet wird.

Damit führt weder eine gemeinsame Betrachtung der Lehren der im Verfahren befindlichen Druckschriften noch eine Ergänzung der Lehren dieser Druckschriften mit dem Wissen des Fachmanns in naheliegender Weise zu den Gegenständen der geltenden Ansprüche 1 und 7 nach Hauptantrag.

Es ist daher anzuerkennen, dass die Gegenstände der Ansprüche 1 und 7 nach Hauptantrag gegenüber dem im Verfahren befindlichen Stand der Technik auf einer erfinderischen Tätigkeit beruhen und patentfähig sind.

7. Die abhängigen Ansprüche 2 bis 6 und 8 nach Hauptantrag betreffen über das Selbstverständliche hinausgehende Ausgestaltungen der Gegenstände der Ansprüche 1 und 7 und sind daher ebenfalls patentfähig.

8. Da die vorgelegten geltenden Unterlagen auch den weiteren Voraussetzungen zur Patenterteilung (§ 1, 2, 5 PatG) genügen, war auf die Beschwerde des Anmelders der Zurückweisungsbeschluss der Prüfungsstelle für Klasse G 06 F des Deutschen Patent- und Markenamts aufzuheben.

9. Der Beschluss konnte ohne mündliche Verhandlung ergehen, da dem Hauptantrag des Anmelders vollumfänglich stattgegeben wurde.

Somit ist das Patent antragsgemäß zu erteilen.

III.

Rechtsbehelfsbelehrung

Gegen diesen Beschluss steht der 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.

Wickborn Kruppa Altvater Dr. Flaschke

Me