Interner Verteilerschlüssel:

(A) [-] Veröffentlichung im ABl.
(B) [-] An Vorsitzende und Mitglieder
(C) [-] An Vorsitzende
(D) [X] Keine Verteilung

Datenblatt zur Entscheidung vom 18. Februar 2019

Beschwerde-Aktenzeichen: T 0883/17 - 3.5.06

Anmeldenummer: 10755121.0

Veröffentlichungsnummer: 2473942

IPC: G06F21/00, G07F7/10

Verfahrenssprache: DE

Bezeichnung der Erfindung:
VERFAHREN UND SYSTEM ZUM AKTIVIEREN EINES TRAGBAREN DATENTRÄGERS

Anmelder:
Giesecke+Devrient Mobile Security GmbH

Stichwort:
Aktivieren eines elektronischen Identitätsdokuments/GIESECKE

Relevante Rechtsnormen:
EPÜ Art. 84, 56

Schlagwort:
Patentansprüche - Klarheit - Hauptantrag (nein), Hilfsantrag (ja)
Erfinderische Tätigkeit - Hilfsantrag (ja)

Zitierte Entscheidungen:

Orientierungssatz:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Beschwerde-Aktenzeichen: T 0883/17 - 3.5.06

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.06
vom 18. Februar 2019

Beschwerdeführer: (Anmelder)	Giesecke+Devrient Mobile Security GmbH Prinzregentenstraße 159 81677 München (DE)
Vertreter:	Klunker IP Patentanwälte PartG mbB Destouchesstraße 68 80796 München (DE)
Angefochtene Entscheidung:	**Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 22. November 2016 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 10755121.0 aufgrund des Artikels 97 (2) EPÜ zurückgewiesen worden ist.**

Zusammensetzung der Kammer:

Vorsitzender	W. Sekretaruk
Mitglieder:	M. Müller
	G. Zucka

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung der Prüfungsabteilung vom 22. November 2016, die Europäische Patentanmeldung 10 755 121.0 zurückzuweisen mangels Klarheit, Artikel 84 EPÜ, und erfinderischer Tätigkeit, Artikel 56 EPÜ, gegenüber

D1: WO 2008/000297 A1.

Die folgenden weiteren Dokumente sind im internationalen Recherchenbericht, nicht allerdings in der Entscheidung, genannt. Sie werden hiermit eingeführt:

D2: EP 1 662 425 A1
D3: WO 2004/027715 A2
D4: WO 2004/105421 A2
D5: US 2007/0226793 A1

II. Die Anmelderin legte am 23. Januar 2017 Beschwerde gegen diese Entscheidung ein und entrichtete die fällige Beschwerdegebühr. Am 22. März 2017 ging die Beschwerdebegründung ein. Die Beschwerdeführerin beantragte, die Entscheidung aufzuheben und ein Patent auf Grundlage der ursprünglichen Beschreibung und Zeichnung sowie der Ansprüche eingegangen am 12. August 2016 zu erteilen.

III. In der Anlage zu einer Ladung zur mündlichen Verhandlung teilte die Kammer der Beschwerdeführerin mit, dass die vorliegenden Ansprüche nicht klar seien, Artikel 84 EPÜ. Eine erschöpfende Bewertung der erfinderischen Tätigkeit sei angesichts dessen nicht möglich.

IV. In Erwiderung auf die Ladung reichte die Beschwerdeführerin neue Anspruchssätze gemäß 6 neuen Hilfsanträgen ein.

V. In der mündlichen Verhandlung, die wie geplant am 18. Februar 2019 stattfand, legte die Beschwerdeführerin drei weitere Anspruchssätze gemäß Hilfsanträgen 7-9 vor. Nach Diskussion mit der Kammer zog sie alle Hilfsanträge bis auf den 9. zurück und beantragte Erteilung eines Patents auf Grundlage der Ansprüche des Hauptantrags oder des Hilfsantrags 9.

VI. Anspruch 1 des Hauptantrags lautet wie folgt.

"Verfahren zum Aktivieren eines ersten tragbaren Datenträgers (1) mit Hilfe eines zweiten tragbaren Datenträgers (2), wobei es sich bei dem ersten und dem zweiten tragbaren Datenträger um einen elektronischen Pass, ein Ausweisdokument und/ oder ein Visa handelt, bei dem:

- eine Kommunikationsverbindung zwischen dem ersten und zweiten Datenträger (1, 2) aufgebaut wird, über welche sich der erste und zweite Datenträger (1, 2) basierend auf den Authentisierungsdaten gegenseitig authentisieren und eine kryptographisch gesicherte Ende-zu-Ende-Verbindung herstellen;

- eine Aktivierung des ersten Datenträgers (1) durchgeführt wird, indem der zweite Datenträger (2) über die Ende-zu-Ende-Verbindung den ersten Datenträger (1) durch Übermitteln von Aktivierungsdaten aktiviert,

dadurch gekennzeichnet, daß

- der erste tragbare Datenträger (1) einem Benutzer in einem inaktiven Zustand bereitgestellt wird, nachdem der Benutzer den ersten Datenträger (1) mit Hilfe eines zweiten tragbaren Datenträgers (2) bei einer zentralen Instanz beantragt hat, wobei in dem inaktiven Zustand die elektronischen Funktionalitäten des ersten Datenträgers (1) außer Funktion gesetzt sind, wobei auf den ersten tragbaren Datenträger (1) Authentisierungsdaten aufgebracht werden, die eine gegenseitige Authentisierung ausschließlich mit dem zweiten tragbaren Datenträger (2) erlauben, wobei der erste und zweite tragbare Datenträger (1, 2) Zugriff auf die Authentisierungsdaten haben, und
- im Rahmen der Aktivierung alle auf dem zweiten tragbaren Datenträger (2) vorhandenen Berechtigungen und Funktionalitäten von diesem auf den ersten tragbaren Datenträger (1) übertragen werden und dieser nach abgeschlossener Aktivierung unmittelbar einsatzbereit ist und mit allen Funktionalitäten genutzt werden kann."

Der einzige unabhängige Anspruch 1 des Hilfsantrags 9 lautet wie folgt.

"Verfahren zum Aktivieren eines ersten tragbaren Datenträgers (1) mit Hilfe eines zweiten tragbaren Datenträgers (2), wobei es sich bei dem ersten und dem zweiten tragbaren Datenträger um ein elektronisches Identitätsdokument handelt, bei dem:

- eine Kommunikationsverbindung zwischen dem ersten und zweiten Datenträger (1, 2) aufgebaut wird, über welche sich der erste und zweite Datenträger (1, 2) basierend auf den Authentisierungsdaten gegenseitig

authentisieren und eine kryptographisch gesicherte Ende-zu-Ende-Verbindung herstellen;

- eine Aktivierung des ersten Datenträgers (1) durchgeführt wird, indem der zweite Datenträger (2) über die Ende-zu-Ende-Verbindung den ersten Datenträger (1) durch Übermitteln von Aktivierungsdaten aktiviert,

dadurch gekennzeichnet, daß

- der erste tragbare Datenträger (1) einem Benutzer in einem inaktiven Zustand bereitgestellt wird, wobei in dem inaktiven Zustand die elektronischen Funktionalitäten des ersten Datenträgers (1) außer Funktion gesetzt sind, wobei auf den ersten tragbaren Datenträger (1) von einer zentralen Instanz Authentisierungsdaten aufgebracht werden, die eine gegenseitige Authentisierung mit dem zweiten tragbaren Datenträger (2) erlauben, wobei der zweite tragbare Datenträger (2) im Rahmen seiner Produktion oder im Zuge einer Kontaktaufnahme zu der zentralen Instanz mit geeigneten Authentisierungsdaten versehen wird, um eine Authentisierung mit dem ersten Datenträger (1) sicherzustellen[,]
- im Rahmen der Aktivierung alle auf dem zweiten tragbaren Datenträger (2) vorhandenen Berechtigungen und Funktionalitäten von diesem auf den ersten tragbaren Datenträger (1) übertragen werden und dieser nach abgeschlossener Aktivierung unmittelbar einsatzbereit ist und mit allen Funktionalitäten genutzt werden kann."

VII. Am Ende der mündlichen Verhandlung verkündete der Vorsitzende die Entscheidung der Kammer.

Entscheidungsgründe

Die Erfindung

1. Die Anmeldung stellt fest, dass herkömmliche Verfahren zur Ausstellung neuer elektronischer Identifikationsdokumente (z.B. von Pässen) aus Sicherheitsgründen die persönliche Gegenwart des Antragstellers erfordern (vgl. Seite 1, Zeilen 15-19), und befasst sich mit der Aufgabe, dieses Erfordernis zu vermeiden.

1.1 Als Lösung wird vorgeschlagen, dass dem Benutzer, der ein neues Identifikationsdokument benötigt, dieses in inaktivem Zustand z.B. postalisch zugestellt wird (vgl. Abbildung 1. P1, S1-S4, P2). Ein Zustand wird dabei "inaktiv" genannt, wenn bei ihm "eine bestimmungsgemäße Verwendung" nicht möglich ist (siehe Seite 3, Zeilen 8-10). Damit ist unbefugte Verwendung eines auf dem Postweg abgefangenen Dokuments zunächst ausgeschlossen.

1.2 Um die Ausstellung eines voll funktionsfähigen elektronischen Dokuments abzuschließen, muss dass inaktive Dokument nun noch aktiviert werden.

1.3 Die erfindungsgemäße Lösung setzt voraus, dass der Benutzer wenigstens ein gültiges und aktiviertes Identifikationsdokument schon besitzt und schlägt vor, das neue Dokument durch das alte aktivieren zu lassen.

1.4 Zur Aktivierung wird eine "gesicherte Ende-zu-Ende-Verbindung" zwischen Alt- und Neupass hergestellt (vgl. Abbildung 1, P5, sowie Absatz zwischen Seiten 12 und 13), über die der Altpass die zur Aktivierung notwendigen Daten an den Neupass überträgt (Seite 13, Absatz 2). Wenn der Neupass den Altpass ersetzt, wird

der Altpass im Anschluss deaktiviert (vgl. Seite 15, Absatz 2; vgl. aber auch Seite 17).

1.5 Dieses Verfahren weise grundsätzlich die Gefahren auf, dass ein gefälschter Neupass aktiviert und dass eine echter Neupass durch einen falschen Altpass aktiviert und im Zuge dessen manipuliert werden könnte. Die Anmeldung schlägt vor, das dadurch zu verhindern, dass die Identitäten der Pässe "während der Antragsphase" miteinander verknüpft werden (siehe Seite 14, Absatz 2), so dass "ausschließlich eine Authentisierung zwischen" diesen möglich ist.

Klarheit, Artikel 84 EPÜ, und Anspruchsauslegung

Hauptantrag

2. Die Prüfungsabteilung war der Meinung (siehe Entscheidung, Gründe 11), dass Anspruch 1 des Hauptantrags aus zwei Gründen unklar sei.

2.1 Er fordere, dass "die auf den ersten Datenträger [aufgebrachten] Authentisierungsdaten" so beschaffen seien, dass sie eine "gegenseitige Authentisierung" der beteiligten Datenträger "ausschließlich mit dem zweiten tragbaren Datenträger" erlaubten, ohne jedoch festzulegen, wie das sichergestellt werde. Die Prüfungsrichtlinien erlaubten eine solche "negative Formulierung [...] nur im Ausnahmefall" und forderten im vorliegenden Fall aus Klarheitsgründen eine positive Formulierung.

2.2 Und er fordere, dass die - d.h. alle - Funktionalitäten des "Altpasses" erst durch Aktivierung genutzt werden könnten, wo doch wenigstens die Authentisierungs-

funktion beider Karten eine solche "Funktionalität" sei und schon für die Authentisierung gebraucht werde. Damit sei der beanspruchte inaktive Zustand wenigstens erheblich breiter auszulegen, als die Anmelderin meint (siehe auch Punkt 12, Seite 4, Absatz 2).

3. Die Kammer stimmt der Prüfungsabteilung im Hinblick auf das "Ausschließlichkeitserfordernis" zu, wie im Folgenden begründet wird. Die ebenfalls zustimmende vorläufige Meinung im Hinblick auf den inaktiven Zustand ist demgegenüber nicht entscheidungserheblich (vgl. Ladungszusatz, Punkt 6.6).

3.1 Die Prüfungsabteilung stellt richtig fest, dass der Begriff "ausschließlich" eine "negative Formulierung" markiert. Der Anspruch fordert zunächst positiv, dass die genannten Authentisierungsdaten eine "gegenseitige Authentisierung [...] erlaub[t]en" und schränkt dann mit "ausschließlich" ein, dass Authentisierung zwischen allen weiteren Paaren von Datenträgern nicht möglich sein soll.

3.2 Nach dem Wortverständnis der Kammer sind zwei Dinge erforderlich, damit die Authentifizierung des ersten Datenträgers "ausschließlich" mit dem zweiten Datenträger erfolgen kann.

a) Die auf dem ersten Datenträger vorliegenden "Authentisierungsdaten" müssen den "zweiten" Datenträger eindeutig identifizieren, typischerweise durch eine Art "Geheimnis", das kein weiterer Datenträger kennt, mit dem andernfalls die Authentisierung ebenfalls möglich wäre.
b) Und auf dem ersten Datenträger dürfen keine weiteren "Authentisierungsdaten" vorliegen, mit

denen dieser sich mit weiteren Datenträgern gegenseitig authentisieren könnte.

3.3 Die Anmeldung setzt sich nur mit dem Punkt a) auseinander, schließt aber das Vorliegen weiterer Authentisierungsdaten gemäß Option b) nicht aus.

3.3.1 Das mag beabsichtigt gewesen sein, da die explizit genannten Gefahren - Aktivierung eines gefälschten elektronischen Dokuments oder Aktivierung durch ein gefälschtes Dokument (Seite 14, Absatz 2) - auch dann verhindert werden, wenn der "erste" Datenträger mit Authentisierungsdaten für mehrere zweite ausgestattet wäre, so dass beispielsweise ein neuer Personalausweis wahlweise durch den alten Personalausweis oder den alten Reisepass aktiviert werden könnte.

3.3.2 Gleichzeitig stellt weder der Anspruchswortlaut noch die Anmeldung ausdrücklich fest, ob das Ausschließlichkeitserfordernis Möglichkeit b) umfassen solle oder nicht.

3.3.3 Der Begriff "ausschließlich" ist schon aus diesem Grund unklar, Artikel 84 EPÜ.

3.4 Die Forderung, dass Authentifizierung "ausschließlich" zwischen zwei bestimmten Datenträgern möglich sei, meint, dass er zwischen diesen möglich und zwischen allen anderen Paarungen unmöglich ist. Soweit aber die Authentifizierung zwischen zwei Karten mit bestimmten Daten möglich ist, impliziert das Ausschließlichkeitserfordernis, dass bestimmte Daten auf allen anderen Zweikarten eben nicht vorliegen.

3.4.1 Die Verwendung des Wortes "ausschließlich" definiert somit die beanspruchten Datenträger durch impliziten

Bezug auf weitere, nicht beanspruchte Datenträger. Die Existenz eines weiteren, nicht beanspruchten Datenträgers, dem geeignete Authentisierungsdaten mit dem ersten und/oder zweiten Datenträger "erlauben" würden, widerspräche dem beanspruchten Ausschließlichkeitserfordernis. Anspruch 1 jedoch enthält keine Merkmale, die die Existenz eines solchen weiteren Datenträgers ausschließen könnten.

3.4.2 Nach dem Verständnis der Kammer kann diese Invariante nur durch ein geeignetes Verhalten einer zentralen Instanz sichergestellt werden. Eine solche wird jedoch in Anspruch 1 nur insofern beansprucht als bei ihr der erste Datenträger mit Hilfe des zweiten "beantragt" wird, "wobei" geeignete Authentisierungsdaten auf diesen "aufgebracht werden". Ob und wie hingegen die zentrale Instanz die notwendige Ausschließlichkeit sicherstellt, ist nicht beansprucht.

4. Die Kammer kommt somit zu dem Ergebnis, dass Anspruch 1 des Hauptantrags schon wegen des Begriffs "ausschließlich" das Klarheitserfordernis von Artikel 84 EPÜ nicht erfüllt.

Hilfsantrag

5. Der Hilfsantrag ("9") legt fest, dass eine zentrale Instanz zu geeigneten Zeitpunkten auf den ersten und zweiten Datenträger Authentisierungsdaten aufbringt, die diesen eine gegenseitige Authentisierung erlauben. Der Fachmann entnimmt dem, dass beide Datenträger ein geeignetes "Geheimnis" teilen, beispielsweise einen gemeinsamen symmetrischen Schlüssel oder ein passendes asymmetrisches Schlüsselpaar (vgl. auch die Beschreibung, Seite 11, Zeilen 1-17). Eine "ausschließliche" Authentisierung wird nicht mehr

gefordert, so dass anspruchsgemäß eine gegenseitige Authentisierung der beanspruchten mit weiteren Datenträgern möglich bleibt. Das entsprechende Klarheitsproblem besteht somit nicht mehr.

6. Die beanspruchte gegenseitige Authentisierung der beiden Datenträger dient insbesondere dazu, den ersten Datenträger zu "aktivieren", der zunächst in einem "inaktiven Zustand" bereitgestellt wird.

6.1 Im inaktiven Zustand ist anspruchsgemäß die "bestimmungsgemäße Verwendung" des Datenträgers nicht möglich. Da beide Datenträger als "elektronische Identitätsdokumente" definiert sind, würde der Fachmann nach Meinung der Kammer als diese bestimmungsgemäße Verwendung die elektronische Funktion ansehen, die den Besitzer als den rechtmäßigen Eigentümer des ersten Datenträgers identifiziert. Wenngleich diese Auslegung der bestimmungsgemäßen Verwendung sehr breit ist, so fällt nach Meinung der Kammer die gegenseitige Authentisierung der Datenträger nicht mehr darunter, da diese die Karten selbst und nicht - oder wenigstens nicht zwingend - den Besitzer der Datenträger betrifft.

6.2 Die Möglichkeit der gegenseitigen Authentisierung beider Datenträger im "inaktiven Zustand" des ersten Datenträgers ist nun kein Widerspruch mehr, so dass der Klarheitseinwand der Prüfungsabteilung fällt (vgl. Punkt 2.2 oben).

7. Die Kammer hält den Anspruch 1 des Hilfsantrags ("9") somit für klar im Sinne von Artikel 84 EPÜ.

8. Im Übrigen ist die Kammer der Meinung, dass der in Anspruch 1 des Hilfsantrags ("9") verwendete Begriff des elektronischen Identitätsdokuments im Lichte der

Beschreibung eng auszulegen ist. Der Fachmann würde darunter nach Ansicht der Kammer ein elektronisches Dokument verstehen, das, wie z. B. ein elektronischer Pass, nur zur Verwendung durch eine Person vorgesehen ist (vgl. Beschreibung, Seite 1, Zeilen 9-11) und dessen bestimmungsgemäßer Gebrauch demnach insbesondere den Besitzer identifizieren soll, und zwar mit elektronischen Mitteln wie etwa dem automatischen Abgleich gespeicherter mit gemessenen biometrischen Daten. Weder eine Bankkarte noch eine elektronische Fahrkarte ist in diesem Sinne ein elektronisches Identitätsdokument. Beide sind grundsätzlich durch jeden Inhaber verwendbar, der ein eventuell notwendiges Geheimnis kennt, selbst wenn das unter Umständen vertraglich verboten sein sollte.

8.1 Es steht nach Meinung der Kammer dieser engen Auslegung nicht entgegen, dass das erfindungsgemäße Verfahren auch für elektronische Fahrkarten oder Bankkarten verwendbar ist (vgl. die Beschreibung, Seite 4, letzter Absatz).

8.2 Ebenso ist evident, dass dieses Verfahren auch für elektronische Identitätsdokumente verwendbar ist, die neben der Identifikationsfunktion Zusatzfunktionen wie eine Zahlfunktion aufweisen sollten. In diesem Sinne ist die Kammer der Ansicht, dass Anspruch 2 des Hilfsantrags ("9"), soweit dieser die Datenträger als "elektronische Fahrkarte" oder "elektronische Bankkarte" festlegt, eine Zusatzfunktion der elektronischen Identitätsdokumente fordert.

Stand der Technik

9. D1 offenbart ein System zur direkten ("off-line") Zahlung zwischen zwei Geldkarten ("Cash Cards"). Zwei

Arten von Geldkarten werden unterschieden: Solche, die an Kunden, und solche, die z.B. an Geschäftsinhaber ausgegeben werden ("Cash Cards" und "Administrator Cash Cards" (vgl. Seite 1, Zeilen 21-29). Kunden laden ihre Cash Cards an einem Bankautomaten auf (siehe Seite 5, Zeilen 16-31) und übertragen bei einem Kauf, vermittelt durch ein geeignetes Gerät und gegenseitiger Authentisierung mittels Verschlüsselung (siehe Abbildungen 3 und 4, und Seite 4, Zeile 29, bis Seite 5, Zeile 6) - einen Geldbetrag an eine Administrator Cash Card (vgl. Seite 5, Zeile 32, bis Seite 6, Zeile 6). Ein Kauf setzt mindestens eine Administrator Cash Card voraus, ist jedoch auch zwischen zwei solchen Karten möglich (Seite 6, Zeilen 25-29). Bei Gelegenheit kann der Besitzer der Administrator Cash Card einen Geldbetrag auf ein Bankkonto einzahlen (Seite 6, Zeile 30, bis Seite 7, Zeile 6).

10. D2 offenbart ein Verfahren, mit dem ein Benutzer die auf einer IC-Karte zur Verfügung stehenden "Services" auf eine neue IC-Karte übertragen kann, wenn bspw. die Gültigkeit der alten Karte abgelaufen ist (vgl. Absatz 3). Der Fokus von D2 liegt in diesem Zusammenhang darauf, eine Vielzahl von Services so "an einer Stelle" zu übertragen, dass der Benutzer nicht mit jedem einzelnen Serviceprovider direkt in Kontakt treten muss (vgl. Absätze 7 und 13, sowie Abbildungen 1 und 2). Zu diesem Zweck stellt D2 einen zentralen Datentransferservice 10 bereit. Eine direkte Kommunikation zwischen Alt- und Neukarte wird nicht offenbart.

11. D3 offenbart ein Verfahren, mit dem u. a. Identitätsdokumente (vgl. Seite 1, Zeilen 12-16) dezentral ausgestellt werden können, damit sie weder auf dem Postweg abgefangen werden können, noch den Besuch einer

Ausgabestelle durch den Benutzer erfordern (Seite 1, Zeilen 20-36). Als Lösung offenbart D3 eine dezentrale "personalization unit", die Sicherheitsmerkmale auf das Identifikationsdokument aufbringt (Seite 4, Zeilen 1-22) und somit ein "ID document" in ein "personalised ID document" umwandelt (vgl. Abbildung 1). Ein Altdokument wird dabei nicht benötigt, und demnach ist auch eine direkte Kommunikation zwischen Alt- und Neudokument nicht offenbart.

12. D4 offenbart ein Gerät, mit dem Informationen von einer alten SIM-Karte auf eine neue übertragen werden können ("SIM copy device COP", vgl. Abbildung 3 und Seite 6, Zeilen 21-25).

13. D5 offenbart ein Verfahren, mit dem der Benutzer einer Stammkarte ("parent card") eine Zweitkarte ("child card") direkt autorisieren kann. Bei den Karten kann es sich beispielsweise um Kreditkarten handeln, deren Kreditlimit durch die Autorisierung mit einem weiteren Kunden geteilt wird (vgl. Absatz 16). Zu diesem Zweck wird von der Stammkarte, auf der ein ("public key") Zertifikat des Kartenausstellers gespeichert ist, ein entsprechendes Zertifikat so abgeleitet, dass der Kartenaussteller die Gültigkeit des abgeleiteten Zertifikats verifizieren kann (vgl. Absätze 68-70). Insbesondere wird das neue Zertifikat mit dem privaten Schlüssel der Stammkarte verschlüsselt (Absatz 70). Ein Vertrauen des Inhabers der Stammkarte in der Zweitkarte wird vorausgesetzt und muss daher nicht überprüft werden. Es wird eine sichere Verbindung zwischen Stamm- und Zweitkarte offenbart, aber nur indirekt, nämlich vermittelt durch einen "card mediation apparatus" (vgl. etwa Abbildungen 16, 18-20 und 27, sowie Absatz 71).

Eine Authentisierung der Zweitkarte durch die Stammkarte in D5 ist nicht offenbart.

Erfinderische Tätigkeit, Artikel 56 EPÜ

14. D1 befasst sich nicht mit Identitätsdokumenten oder deren Aktivierung. Insbesondere kann nach Meinung der Kammer die Übertragung eines Geldbetrags an eine Administrator Cash Card weder als "Aktivierung" der "bestimmungsgemäße[n] Verwendung" eines elektronischen Identitätsdokuments angesehen werden noch diese nahelegen. Daher hält die Kammer das Dokument D1 nicht für einen geeigneten Ausgangspunkt für die Bewertung der erfinderischen Tätigkeit von Anspruch 1 des Hilfsantrags ("9").

15. Das nächstliegende Dokument unter den vorliegenden ist nach Ansicht der Kammer D3, weil es sich mit der Personalisierung - und damit mittelbar der "Aktivierung" - eines elektronischen Identitätsdokuments im Sinne der Anmeldung befasst. D3 offenbart nicht, dass bei der Aktivierung eines neuen Dokuments das alte zum Einsatz kommt, geschweige denn wie beansprucht zur gegenseitigen Authentisierung mit Hilfe von Authentisierungsdaten, die durch eine zentrale Instanz auf beide Dokumente aufgebracht worden wären. Auch ist die Kammer der Meinung, dass der Fachmann bei der Bemühung, das Verfahren aus D3 zu verbessern - etwa durch Erhöhung der Sicherheit - nicht auf D1 zurückgreifen würde, und es gibt keinen Hinweis darauf, dass es für den Fachmann schon aufgrund seines allgemeinen Fachwissens naheliegen würde, vor dem Hintergrund von D3 eine gegenseitige Authentisierung vom alten und neuen Dokument wie beansprucht in Betracht zu ziehen.

16. Die Kammer kommt daher zu dem Ergebnis, dass Anspruch 1 des Hilfsantrags ("9") gegenüber dem zitierten Stand der Technik die erforderliche erfinderische Tätigkeit aufweist.

17. Da der Gegenstand von Anspruch 1 des Hilfsantrag ("9") erheblich von der ursprünglich beanspruchten abweicht, ist eine Anpassung der Beschreibung an den nun beanspruchten Gegenstand notwendig. Die Kammer hält es für angemessen, diese Anpassung vom Beschwerdeführer vor der Prüfungsabteilung durchführen zu lassen.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die Entscheidung wird aufgehoben.
2. Die Sache wird an die Prüfungsabteilung mit der Anordnung zurückverwiesen, ein europäisches Patent mit den Ansprüchen 1-11 gemäß Hilfsantrag 9 vom 18. Februar 2019, der Zeichnung Fig. 1, wie ursprünglich eingereicht, und einer noch anzupassenden Beschreibung zu erteilen.

Die Geschäftsstellenbeamtin: Der Vorsitzende:

M. Schalow W. Sekretaruk

Entscheidung elektronisch als authentisch bestätigt