Interner Verteilerschlüssel:

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

Datenblatt zur Entscheidung vom 13. November 2023

Beschwerde-Aktenzeichen: T 1940/19 - 3.5.06

Anmeldenummer: 11717537.2

Veröffentlichungsnummer: 2561461

IPC: G06F21/00

Verfahrenssprache: DE

Bezeichnung der Erfindung:
VERFAHREN ZUM LESEN EINES ATTRIBUTS AUS EINEM ID-TOKEN

Anmelder:
Bundesdruckerei GmbH

Stichwort:
Lesen eines ID-Tokens/BUNDESDRUCKEREI

Relevante Rechtsnormen:
EPÜ Art. 84, 113(2)
EPÜ R. 43(7)
VOBK 2020 Art. 13(1), 13(2)

Schlagwort:
Änderung des Beschwerdevorbringens - Änderung räumt aufgeworfene Fragen aus (nein) - Änderung gibt Anlass zu neuen Einwänden (ja) - zugelassen (nein)

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 1940/19 - 3.5.06

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.06
vom 13. November 2023

Beschwerdeführer: (Anmelder)	Bundesdruckerei GmbH Oranienstraße 91 10958 Berlin (DE)
Vertreter:	Richardt Patentanwälte PartG mbB Wilhelmstraße 7 65185 Wiesbaden (DE)
Angefochtene Entscheidung:	**Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 12. Februar 2019 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 11717537.2 aufgrund des Artikels 97 (2) EPÜ zurückgewiesen worden ist.**

Zusammensetzung der Kammer:

Vorsitzender	M. Müller
Mitglieder:	M. Domingo Vecchioni
	B. Müller

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung der Prüfungsabteilung, die mit Gründen am 12. Februar 2019 zur Post gegeben wurde. Damit wurde die europäische Patentanmeldung Nr. 11 717 537.2 zurückgewiesen, weil die Anmeldungsunterlagen gemäß dem Hauptantrag und den beiden Hilfsanträgen das Erfordernis einer erfinderischen Tätigkeit, Artikel 52 (1) und 56 EPÜ, nicht erfüllten.

II. Mit der Beschwerdebegründung beantragte die Beschwerdeführerin, die Entscheidung aufzuheben und ein Patent auf der Grundlage des Hauptantrags oder eines der beiden Hilfsanträge zu erteilen, die der angefochtenen Entscheidung zugrunde lagen.

III. Mit Schreiben vom 6. September 2023 teilte die Beschwerdekammer der Beschwerdeführerin ihre vorläufige Meinung mit. Anspruch 1 aller Anträge sei aus mehreren Gründen nicht klar und nicht von der Beschreibung gestützt, Artikel 84 EPÜ. Die vorläufige Meinung der Kammer enthält außerdem eine ausführliche Analyse der erfinderischen Tätigkeit betreffend den Gegenstand von Anspruch 1 des Hauptantrags, bei weiter Auslegung im Hinblick auf die Klarheitsmängel, und kommt zu einem negativen Ergebnis, Artikel 56 EPÜ.

IV. In einem Schreiben vom 30. Oktober 2023 trug die Beschwerdeführerin vor, wie der Fachmann die Ansprüche verstehen würde und weswegen ihr Gegenstand gegenüber dem zitierten Stand der Technik nicht naheliegend sei. Sie bezog sich dabei auf Wikipedia-Artikel zu "Digital

signature", "Digitales Zertifikat" und "Transport Layer Security", die sie mit dem Schreiben einreichte.

V. In der mündlichen Verhandlung vor der Beschwerdekammer ließ die Beschwerdeführerin nach sachlicher Diskussion der anhängigen Anträge diese fallen und beantragte dann die Erteilung eines Patents auf Grundlage von neu eingereichten Ansprüchen 1-12, hilfsweise demselben Anspruchssatz, in dem Anspruch 9 gestrichen sei, und weiter hilfsweise demselben Anspruchssatz, in dem darüber hinaus auch Ansprüche 10 bis 12 gestrichen seien.

VI. Anspruch 1 lautet, identisch in allen Anträgen:

"Verfahren zum Lesen zumindest eines in einem ID-Token (106, 106') gespeicherten Attributs unter Verwendung von ersten (136), zweiten (150) und dritten (100) Computersystemen, wobei das dritte Computersystem einen Browser (112) und einen Client (113) beinhaltet, und wobei dem zweiten Computersystem ein Dienst-Zertifikat (144) zugeordnet ist, wobei das Dienst-Zertifikat einen Identifikator beinhaltet, durch welchen das zweite Computersystem identifiziert wird, wobei der ID-Token einem Nutzer (102) zugeordnet ist, mit folgenden Schritten:
- Aufbau einer ersten kryptographisch gesicherten Verbindung (TLS1) zwischen dem Browser des dritten Computersystems und dem zweiten Computersystem, wobei das dritte Computersystem ein erstes Zertifikat (176) empfängt,
- Speicherung des ersten Zertifikats durch das dritte Computersystem,
- Empfang einer signierten Attributspezifizierung (182) durch das dritte Computersystem über die erste Verbindung,
- Aufbau einer zweiten kryptographisch gesicherten

Verbindung (TLS2) zwischen dem Browser des dritten Computersystems und dem ersten Computersystem, wobei das dritte Computersystem ein zweites Zertifikat (190) von dem ersten Computersystem empfängt,
- Weiterleitung der signierten Attributspezifizierung von dem dritten Computersystem über die zweite Verbindung an das erste Computersystem,
- Zugriff auf ein Berechtigungszertifikat (186) durch das erste Computersystem, wobei das Berechtigungszertifikat sowohl den Identifikator des zweiten Computersystems als auch den Identifikator des ersten Computersystems beinhaltet anhand der Signatur der Attributsspezifierung desjenigen der zweiten Computersysteme von dem die Attributsspezifizierung signiert worden ist,
- Aufbau einer dritten kryptographisch gesicherten Verbindung (TLS3) zwischen dem ersten Computersystems und dem Client des dritten Computersystems, wobei das dritte Computersystem über die dritte Verbindung das Berechtigungszertifikat mit dem Identifikator empfängt,
- Prüfung durch den Client des dritten Computersystems, ob der Identifikator in dem ersten Zertifikat beinhaltet ist, als Nachweis dafür, dass das erste Zertifikat mit dem Dienst-Zertifikat übereinstimmt,
- Authentifizierung des Nutzers gegenüber dem ID-Token,
- Authentifizierung des ersten Computersystems (136) gegenüber dem ID-Token,
- Aufbau einer vierten kryptographisch gesicherten Verbindung mit Ende-zu-Ende Verschlüsselung zwischen dem ID-Token und dem ersten Computersystem, nach erfolgreicher Authentifizierung des Nutzers und des ersten Computersystems gegenüber dem ID-Token,
Lesezugriff des ersten Computersystems auf das zumindest eine in dem ID-Token gespeicherte Attribut über die vierte Verbindung, um die in der Attributspezifizierung spezifizierten ein oder mehrere

Attribute aus dem ID-Token auszulesen,
- Übertragung des zumindest einen Attributs nach dessen Signierung durch das erste Computersystem an das zweite Computersystem (150)."

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

Entscheidungsgründe

Die Anmeldung

1. Die Anmeldung betrifft ein Verfahren zum Lesen von zumindest einem Attribut (z.B. dem Geburtsdatum eines Nutzers) aus einem ID-Token, z.B. einem elektronischen Dokument, das es dem Nutzer ermöglicht, seine Identität gegenüber einem Online-Dienst digital mitzuteilen. Siehe Seite 1, Zeilen 3-6; Seite 2, Zeilen 14-21; Seite 3, Zeilen 23-25; Seite 6, Zeile 30 bis Seite 7, Zeile 2.

2. Am Verfahren sind insbesondere ein ID-Token (106) des Nutzers (102) sowie drei Computersysteme beteiligt: ein Nutzer-Computersystem (100) ("drittes Computersystem" in Anspruch 1), ein Dienst-Computersystem (150) ("zweites Computersystem") und ein ID-Provider-Computersystem (136) ("erstes Computersystem"), das zu einem Trust-Center gehören kann (Seite 13, Zeilen 2-4; Seite 18, Zeilen 17-22). Siehe Figur 3:

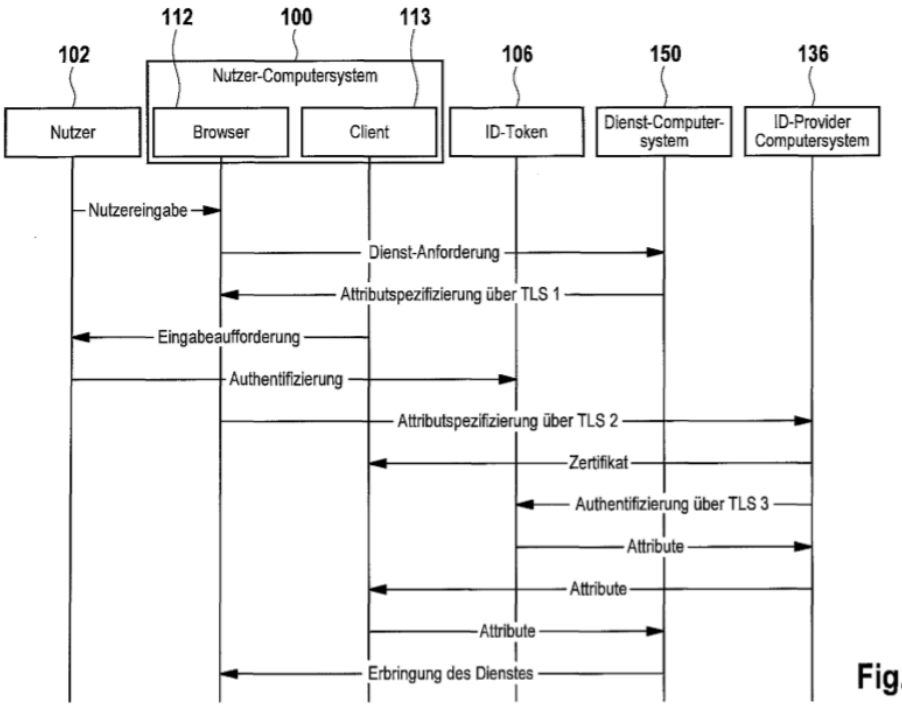

Fig. 3

3. Die Anmeldung befasst sich insbesondere damit, eine "Man-in-the-Middle-Attacke" (im Folgenden: "MITM-Angriff") im Rahmen eines solchen Verfahren abzuwehren (Seite 3, Zeilen 27/28; Seite 25, Zeilen 22-27).

4. Ein MITM-Angriff kann insbesondere beim Aufbau der ersten TLS-Verbindung ("erste kryptographisch gesicherte Verbindung (TLS1)") zwischen dem Browser (112) des Nutzer-Computersystems und dem Dienst-Computersystems stattfinden, über die der Browser eine vom Dienst-Computersystem "signierte Attributspezifizierung" empfangen soll.

Für den Aufbau dieser ersten TLS-Verbindung ist an sich der Empfang eines SSL-Zertifikats des Dienst-Computersystems ("Zertifikat ZD I 144" in Figur 1, "Dienst-Zertifikat (144)" in Anspruch 1) durch das Nutzer-Computersystem erforderlich. Ein solches Zertifikat enthält einen "Identifikator" des Dienst-Computersystems, z.B.

dessen URL oder öffentlichen Schlüssel (Seite 3, Zeile 30 bis Seite 4, Zeile 4; Seite 9, Zeilen 17-34).

Bei einem MITM-Angriff kann ein Angreifer beim Aufbau der Verbindung die Nachricht mit dem Dienstzertifikat (144) abfangen und dieses durch ein anderes Zertifikat ("Zertifikat ZA 180" in Figur 1) ersetzen, sodass das vom Nutzer-Computersystem empfangene Zertifikat ("Zertifikat Z 176" in Figur 1, "erstes Zertifikat (176)" in Anspruch 1) vom Dienstzertifikat (144) abweichen kann (Seite 10, Zeilen 5-7; Seite 20, Zeilen 23-29; Seite 26, Zeilen 16-20).

Das Verfahren gemäß Anspruch 1 zielt darauf ab, einen solchen MITM-Angriff erkennen zu können.

5. Die Erkennung erfolgt insbesondere dadurch, dass ein Client (113) des Nutzer-Computersystems über die dritte TLS-Verbindung ("dritte kryptographisch gesicherte Verbindung (TLS3)") vom ID-Provider-Computersystem ein "Berechtigungszertifikat (186)" erhält, das den Identifikator des Dienst-Computersystems enthält, und dass vom Nutzer-Computersystem geprüft wird, ob dieser Identifikator im empfangenen "ersten Zertifikat (176)" enthalten ist. Das Verfahren wird nur fortgesetzt, wenn dies der Fall ist (Seite 5, Zeilen 4-16).

6. Nach der Beschreibung wird "[u]nter einem 'Berechtigungszertifikat' [...] hier ein Zertifikat verstanden, das eine Spezifizierung von Zugriffsrechten auf in dem ID-Token gespeicherte Attribute beinhaltet" und das "einen Verweis auf ein oder mehrere Zertifikate, insbesondere SSL- oder TLS-Zertifikate, beinhalten [kann], welche dem Berechtigungszertifikat zugeordnet sind"

(Seite 6, Zeilen 1-5). Diese Berechtigung wird vom ID-Token geprüft (Seite 6, Zeilen 15-26).

In einer Ausführungsform ist es vorgesehen, dass dem ID-Provider-Computersystem mehrere Berechtigungszertifikate mit verschiedenen Leserechten vorliegen und das Computersystem eines (oder mehrere) davon auf der Basis der empfangenen signierten Attributsspezifikation auswählt, insbesondere so, dass es die zum Lesen der spezifizierten Attribute ausreichenden Leserechte aufweist (Seite 7, Zeile 32 bis Seite 8, Zeile 2; Seite 12, Zeilen 21-25) und es dem identifizierten Dienst-Computersystem zugeordnet ist (Seite 4, Zeilen 23-25; Seite 23, Zeilen 20-22).

Nicht-Zulassung der Anträge

7. Der Hauptantrag und die Hilfsanträge 1 und 2 wurden erst in der mündlichen Verhandlung eingereicht.

Laut Beschwerdeführerin dienten die Änderungen dazu, die Einwände unter Artikel 84 EPÜ zu beheben, die die Kammer in ihrer vorläufigen Meinung (Punkte 13-17) erhoben hatte.

8. Der Einwand in Punkt 13.1 der vorläufigen Meinung bezog sich auf die Merkmale von Anspruch 1 gemäß dem Hauptantrag, wonach einerseits "dem zweiten Computersystem ein Dienst-Zertifikat (144) zugeordnet ist", und andererseits das Verfahren u.a. folgende Schritte umfasst:

"Aufbau einer ersten kryptographisch gesicherten Verbindung (TLS1) zwischen dem Browser des dritten Computersystems und dem zweiten Computersystem, wobei

das dritte Computersystem ein erstes Zertifikat (176) empfängt",

"Prüfung durch den Client des dritten Computersystems, ob der Identifikator in dem ersten Zertifikat beinhaltet ist, als Nachweis dafür, dass das erste Zertifikat mit dem Dienst-Zertifikat übereinstimmt",

wobei das zweite bzw. dritte Computersystem dem Dienst- bzw. Nutzer-Computersystem entspricht.

8.1 Im Anspruch sei nicht spezifiert, welche Funktion das "Dienst-Zertifikat (144)" in Bezug auf die "erste kryptographisch gesicherte Verbindung (TLS)" hat. Es sei daher nicht vom Anspruch ableitbar, dass die Prüfung der Übereinstimmung des ersten Zertifikats mit dem Dienst-Zertifikat für das Abwehren eines MITM-Angriffs während des Aufbaus dieser Verbindung zweckdienlich sei.

Es fehle insbesondere das wesentliche Merkmal, dass für den Aufbau der ersten Verbindung (TLS1) das zweite Computersystem das Dienst-Zertifikat (144) überträgt (Seite 20, Zeilen 18-21) und daraufhin das dritte Computersystem das "erste Zertifikat" empfängt (in Anspruch 7 werde mit Bezug auf den Aufbau der zweiten Verbindung (TLS2) davon gesprochen, dass das entsprechende Zertifikat "verwendet" werde).

8.2 Die Beschwerdeführerin hat die relevanten Merkmale im geänderten Anspruch 1 unverändert gelassen. Sie argumentierte in ihrem Schreiben vom 30. Oktober 2023 (und ähnlich in der mündlichen Verhandlung), dass der Fachmann bei der Bezeichung "TLS" mitliest, dass beim Aufbau der gesicherten Verbindung das Dienst-Computersystem sich mit seinem Dienst-Zertifikat gegenüber dem

Nutzer-Computersystem identifiziert, wobei das Dienst-Zertifikat einen "Identifikator" des Dienst-Computersystems enthält. Die Beschwerdeführerin bezog sich dabei auf den Wikipedia-Artikel zu "Transport Layer Security".

8.3 Die Kammer ist von diesen Argumenten nicht überzeugt. Zum Einen ist Anspruch 1 nicht auf den Aufbau einer TLS-Verbindung beschränkt: "TLS" erscheint nur als Teil des Bezugszeichens "TLS1", dem keine einschränkende Wirkung zukommt (Regel 43 (7) EPÜ). Zum Anderen ist in Anspruch 1 nicht klar, dass das "erste Zertifikat" dasjenige Zertifikat ist, das das dritte Computersystem empfängt, wo es unter normalen Umständen (insbesondere wenn kein MITM-Angriff stattgefunden hat) das Dienst-Zertifikat empfangen müsste. Nach dem Wortlaut des Anspruchs könnte es sich beim "ersten Zertifikat" um ein anderes Zertifikat handeln, das ebenfalls beim Aufbau der Verbindung oder auch erst über die aufgebaute Verbindung empfangen wird. Der Einwand in Punkt 13.1 der vorläufigen Meinung, an dem die Kammer festhält, ist daher nicht behoben worden.

9. Die Einwände in Punkten 13.2 und 14-14.3 der vorläufigen Meinung bezogen sich auf das folgende Merkmal von Anspruch 1 gemäß dem Hauptantrag, der der Entscheidung zugrunde lag:

"Zugriff auf ein Berechtigungszertifikat (186) durch das erste Computersystem, wobei das Berechtigungszertifikat den Identifikator beinhaltet, wobei das Berechtigungszertifikat zur Autorisierung des ersten Computersystems durch das zweite Computersystem zur Durchführung einer ID-Provider Funktion dient",

wobei das erste bzw. zweite Computersystem dem ID-

Provider- bzw. dem Dienst-Computersystem entspricht.

9.1 Nach Auffassung der Kammer sei dem Anspruch nicht zu entnehmen, auf Basis welcher Information über das zweite Computersystem das erste Computersystem dieses Berechtigungszertifikat aussuchen würde. Der Erfolg der angestrebten Abwehr eines MITM-Angriffs hinge davon aber wohl ab. Wenn zum Beispiel das dritte Computersystem das (gefälschte) erste Zertifikat dem ersten Computersystem zu diesem Zwecke weiterleiten würde, so würde ggf. auch das erste Computersystem beim Zugriff auf das Berechtigungszertifikat durch den Angriff auf die erste Verbindung getäuscht.

9.2 Außerdem sei der beanspruchte Zweck des Berechtigungszertifikats "zur Autorisierung des ersten Computersystems durch das zweite Computersystem zur Durchführung einer ID-Provider Funktion" nicht klar.

Zwar könnte man annehmen, dass das Berechtigungszertifikat vom Betreiber des zweiten Computersystems für das erste Computersystem ausgestellt worden sei, aber es gebe im Anspruch keinen entsprechenden Schritt, in dem das zweite Computersystem diese Berechtigung anhand des Berechtigungszertifikats prüfen würde.

Des Weiteren stellte die Kammer Spannungen in der Beschreibung selbst hinsichtlich des Berechtigungszertifikats und seiner Verwendung fest (siehe Punkt 10.8 unten).

9.3 Die Kammer schloss mit der vorläufigen Einschätzung, dass Anspruch 1 nicht klar und nicht von der Beschreibung gestützt sei, Artikel 84 EPÜ.

10. Im (neuen) Anspruch 1 ist dieses Merkmal nun wie folgt geändert:

"Zugriff auf ein Berechtigungszertifikat (186) durch das erste Computersystem, wobei das Berechtigungszertifikat den Identifikator beinhaltet anhand der Signatur der Attributsspezifierung desjenigen der zweiten Computersysteme, von dem die Attributsspezifizierung signiert worden ist",

basierend auf Seite 4, Zeilen 23-25.

10.1 In dieser Formulierung ist zunächst unklar, worauf sich "anhand der Signatur..." bezieht. Die Kammer unterstellt im Folgenden zugunsten der Beschwerdeführerin, dass ein Komma nach "beinhaltet" fehlt, wodurch klar wird, dass "anhand der Signatur ..." sich auf den "Zugriff" bezieht.

10.2 Unklar ist auch, welches "zweite Computersysteme" gemeint ist, da Anspruch 1 nur ein "zweite[s] Computersystem" definiert.

10.3 Im neuen Merkmal ist zudem die Berechtigungsfunktion des "Berechtigungszertifikats" nun überhaupt nicht mehr definiert. Gleichzeitig enthält Anspruch 1 weiterhin keinen Schritt, in dem diese Berechtigung geprüft wird.

Damit ist in Anspruch 1 aller neuen Anträge weiter unklar, auf welche Berechtigung sich das "Berechtigungszertifikat" in Anspruch 1 bezieht. Dies macht den Umfang von Anspruch 1 unklar, Artikel 84 EPÜ.

10.4 Die Beschwerdeführerin trug in ihrem Schreiben vom 30. Oktober 2023 (Seite 4, letzter Absatz) vor, das ID-Provider-Computersystem würde "den beim ID-Provider-

Computersystem hinterlegten öffentlichen Schlüssel des Dienst-Computersystems als 'Berechtigungszertifikat" an das Nutzer-Computersystem zurück [übermitteln]".

Danach wäre das "Berechtigungszertifikat", auf das anspruchgemäß zugegriffen wird, der öffentliche Schlüssel des Dienst-Computersystems.

10.5 Dieses Verständnis von "Berechtigungszertifikat" wird jedoch von der Beschreibung nicht gestützt. Auf Seite 6, Zeile 1-24, wird festgestellt, dass "[u]nter einem 'Berechtigungszertifikat' [...] hier ein Zertifikat verstanden [wird], das eine Spezifizierung von Zugriffsrechten auf in dem ID-Token gespeicherte Attribute beinhaltet", einem Dienst-Computersystem zugeordnet ist, und vom ID-Token geprüft wird (Seite 6, Zeilen 1-24).

10.6 Dieses Verständnis steht auch im Widerspruch mit dem früheren Vortrag der Beschwerdeführerin in ihrer Beschwerdebegründung (Seiten 3, 4, 11 und 12), wonach es Kern der Erfindung sei, dass solche "Berechtigungszertifikate", die bereits zu dem im voranstehenden Absatz (Punkt 10.5) angegebenen Zweck verwendet werden, in der Erfindung zusätzlich vorteilhaft zur Abwehr von MITM-Angriffen eingesetzt würden.

Dieser frühere Vortrag entspricht eher der Beschreibung. Damit aber ist das beanspruchte Berechtigungszertifikat ein für die Erfindung - und die erfinderische Tätigkeit - zentrales Merkmal, über dessen Bedeutungsumfang Klarheit herrschen muss.

10.7 Auch ein Bezug auf die in Punkt 10.6 oben wiedergegebene Definition von "Berechtigungszertifikate" auf

Seite 6 der Beschreibung reicht zur Erfüllung des Klarheitserfordernis des Artikels 84 EPÜ nicht aus.

Erstens folgt das daraus, dass grundsätzlich die Ansprüche so weit wie möglich aus sich heraus klar sein sollen, aber auch daraus, wie in der vorläufigen Meinung bereits ausgeführt, dass die Beschreibung an anderen Stellen eine abweichende Definition des Begriffs "Berechtigungszertifikat" andeutet.

So wird z.B. auf Seite 4, Zeilen 14-16, suggeriert, dass "das erste Computersystem [...] von dem Betreiber des zweiten Computersystems, durch welches ein Dienst angeboten wird, zur Durchführung der ID-Provider Funktion autorisiert" werde, und "hierzu" ein dem zweiten Computersystem zugeordnetes Berechtigungszertifikat beim ersten Computersystem hinterlegt sei. Nach diesem Verständnis würde es sich um eine Berechtigung des ID-Provider-Computersystems gegenüber dem Betreiber des Dienst-Computersystems anstatt gegenüber dem ID-Token handeln.

11. Der Hauptantrag und die Hilfsanträge 1 und 2, die allesamt erst in der mündlichen Verhandlung eingereicht wurden, beheben somit nicht alle Einwände unter Artikel 84 EPÜ, die die Kammer in ihrer vorläufigen Meinung erhoben hatte, und führen darüber hinaus zu neuen Klarheitsproblemen.

Die Kammer entschied daher, auf Grundlage des Artikels 13 (2) VOBK und unter Anwendung der Kriterien gemäß Artikel 13(1) VOBK den Hauptantrag und die Hilfsanträge 1 und 2 nicht ins Verfahren zuzulassen.

12. Da kein zugelassener Antrag vorliegt, über den entschieden werden kann (Artikel 113 (2) EPÜ), muss die Beschwerde zurückgewiesen werden.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

Die Beschwerde wird zurückgewiesen.

Die Geschäftsstellenbeamtin: Der Vorsitzende:

L. Stridde Martin Müller

Entscheidung elektronisch als authentisch bestätigt