BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

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

Datenblatt zur Entscheidung vom 17. August 2010

Beschwerde-Aktenzeichen: T 1065/08 - 3.5.05

Anmeldenummer: 02737763.9

Veröffentlichungsnummer: 1379935

IPC: G06F 1/00

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System über ein Zugangsmedium

Patentinhaber:
ROBERT BOSCH GMBH

Einsprechender:
GIESECKE & DEVRIENT GmbH

Stichwort:
Berechtigungsprüfung anhand eines öffentlichen Schlüssels/BOSCH

Relevante Rechtsnormen:
EPÜ Art. 52(1), 56
VOBK Art. 13(1)

Schlagwort:
"Erfinderische Tätigkeit - nein (Hauptantrag und Hilfsanträge)"

Zitierte Entscheidungen:
T 0254/86

Orientierungssatz:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Aktenzeichen: T 1065/08 - 3.5.05

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.05
vom 17. August 2010

Beschwerdeführerin: (Einsprechende)
GIESECKE & DEVRIENT GmbH
Prinzregentenstrasse 159
D-81677 München (DE)

Vertreter:
Bornhäuser, Frank
Giesecke & Devrient GmbH
Prinzregentenstrasse 159
D-81677 München (DE)

Beschwerdegegnerin: (Patentinhaberin)
ROBERT BOSCH GMBH
Postfach 30 02 20
D-70442 Stuttgart (DE)

Vertreter:
-

Angefochtene Entscheidung:
Entscheidung der Einspruchsabteilung des Europäischen Patentamts, die am 28. Februar 2008 zur Post gegeben wurde und mit der der Einspruch gegen das europäische Patent Nr. 1379935 aufgrund des Artikels 101 (2) EPÜ zurückgewiesen worden ist.

Zusammensetzung der Kammer:

Vorsitzender: A. Ritzka
Mitglieder: M. Höhn
F. Blumer

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Zwischenentscheidung der Einspruchsabteilung, zur Post gegeben am 28. Februar 2008, mit der der Einspruch gegen das europäische Patent Nr. 1379935 zurückgewiesen wurde.

II. Die Beschwerdeführerin (Einsprechende) beantragte in der am 22. April 2008 eingegangenen Beschwerdeschrift, die angefochtene Entscheidung der Einspruchsabteilung aufzuheben und das Patent in vollem Umfang zu widerrufen sowie hilfsweise eine mündliche Verhandlung anzuberaumen. Die Beschwerdegebühr wurde ebenfalls am 22. April 2008 entrichtet. Die Beschwerdebegründung wurde am 24. Juni 2008 eingereicht.

Die Beschwerdeführerin stützte ihre Beschwerde auf die (entsprechend den in den Schriftsätzen im Beschwerdeverfahren verwendeten Bezeichnungen):

- Druckschrift D1: US 5 539 826;
- Druckschrift D5: N. Ryska, S. Herda: "Kryptographische Verfahren in der Datenverarbeitung", Springer-Verlag, 1980, S. 335-337, S. 348 und S. 352-355;
- Druckschrift D6: EP 0 383 985 A;
- Druckschrift D11: US 5 687 235;
- Druckschrift D12: US 5 371 794.

III. Die Beschwerdegegnerin (Patentinhaberin) beantragte mit Schriftsatz vom 14. November 2008 die Beschwerde als unbegründet zurückzuweisen (Hauptantrag), hilfsweise das Patent in geändertem Umfang gemäß dem Schriftsatz beigefügtem ersten oder zweiten Hilfsantrag aufrechtzuerhalten und eine mündlichen Verhandlung

anzuberaumen, sofern dem Hauptantrag nicht stattgegeben werden kann.

IV. Mit Schreiben vom 5. Februar 2009 nahm die Beschwerdeführerin zum Gegenstand der Hilfsanträge Stellung. Mit Schreiben vom 11. Mai 2009 führte die Beschwerdeführerin folgende weitere Druckschrift in das Verfahren ein:

- Druckschrift D13: A. Beutelspacher, A. Kersten, A. Pfau: "Chipkarten als Sicherheitswerkzeug", Springer-Verlag 1991, S. 41.

V. Mit einem Bescheid vom 29. April 2010 wurden die Parteien zur mündlichen Verhandlung am 17. August 2010 geladen. In einem Anhang zur Ladung zur mündlichen Verhandlung brachte die Kammer ihre vorläufige Meinung zum Ausdruck, dass es zweifelhaft sei, ob sich die D5 als nächstliegender Stand der Technik eignet. Die erteilte Erfindung sei neu gegenüber D5, welche einen gemeinsamen Schlüsselverwalter, von dem die öffentlichen Schlüssel bezogen werden, vorsieht und keine Zertifikate erwähnt. Daher sei es zweifelhaft, ob der Fachmann ausgehend von der D5 überhaupt eine alternative direkte Übermittlung eines öffentlichen Schlüssels (wie z.B. in der D11) in Betracht ziehen würde. Auch scheine die D5 keine Berechtigungsprüfung eines Anwenders anhand von dessen öffentlichem Schlüssel vorzunehmen. Vor diesem Hintergrund scheine die Entgegenhaltung D1 den nächstliegenden Stand der Technik darzustellen. Die Kammer gab eine vorläufige Einschätzung zur Offenbarung der D1 und zu den in der anberaumten mündlichen Verhandlung zu diskutierenden Fragen im Hinblick auf die erfinderische Tätigkeit. Die den

Unterscheidungsmerkmalen zu Grunde liegende übergeordnete objektive technische Aufgabe ausgehend von D1 scheine eine Prüfung der Berechtigung des Anwenders für einen Zugang zum System zu sein. Die zentrale Frage zur Diskussion in der mündlichen Verhandlung werde daher neben der Interpretation des Begriffs "Berechtigung" sein, ob der Fachmann ausgehend von der D1 eine Verwendung von zertifizierten öffentlichen Schlüsseln in Betracht ziehen würde, und ob es für eine Berechtigungsprüfung des Anwenders anhand des ersten öffentlichen Schlüssels einer erfinderischen Tätigkeit (Artikel 56 EPÜ) gegenüber der Offenbarung der D1 bedurfte vor dem Hintergrund des allgemeinen Fachwissens der Kommunikation mit asymmetrischer Verschlüsselung wie unter anderem aus D11 und D13 bekannt.

VI. Mit Schreiben vom 15. Juli 2010 überreichte die Beschwerdegegnerin (Patentinhaberin) einen weiteren Satz Patentansprüche als dritten Hilfsantrag und stellte nochmals zusammenfassend ihre Position dar.

VII. Am 17. August 2010 fand eine mündliche Verhandlung statt, in der die Beschwerde mit den Parteien erörtert wurde.

Die Beschwerdeführerin (Einsprechende) beantragte die Aufhebung der angefochtenen Entscheidung und den Widerruf des europäischen Patents.

Die Beschwerdegegnerin (Patentinhaberin) beantragte die Abweisung der Beschwerde, hilfsweise die Aufrechterhaltung des Patents auf der Grundlage des ersten oder des zweiten Hilfsantrags (beide eingereicht mit Schreiben vom 14. November 2008) oder des dritten

Hilfsantrags (eingereicht mit Schreiben vom 15. Juli 2010).

VIII. Anspruch 1 gemäß dem Hauptantrag (d.h. Anspruch 1 des erteilten Patents) lautet wie folgt:

"1. Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System über ein Zugangsmedium (1), wobei anwenderseitig ein erster privater und ein erster öffentlicher Schlüssel bereitgestellt werden, wobei sich der Anwender bei dem softwarebasierten System (2) anmeldet, dadurch gekennzeichnet, dass bei der Anmeldung der erste öffentliche Schlüssel zu dem softwarebasierten System (2) übertragen wird (4), dass das softwarebasierte System (2) anhand des ersten öffentlichen Schlüssels eine Berechtigung des Anwenders überprüft (6), dass einem berechtigten Anwender von dem softwarebasierten System (2) eine Zeichenkette mit dem ersten öffentlichen Schlüssel codiert und ein zweiter öffentlicher Schlüssel jeweils übertragen werden (8), dass anwenderseitig diese Zeichenkette mit dem ersten privaten Schlüssel decodiert wird und mit dem zweiten öffentlichen Schlüssel wieder codiert zu dem softwarebasierten System zurück übertragen wird (9) und dass das softwarebasierte System den Anwender als authentifiziert erkennt (11), falls die vom Anwender empfangene und mit einem zweiten privaten Schlüssel decodierte Zeichenkette der von dem softwarebasierten System (2) codierten Zeichenkette entspricht."

IX. Anspruch 1 des ersten Hilfsantrags lautet wie folgt:

"1. Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem Diensteserver über ein Zugangsmedium (1), wobei anwenderseitig ein erster privater und ein erster öffentlicher Schlüssel bereitgestellt werden, wobei sich der Anwender bei dem Diensteserver (2) anmeldet, dadurch gekennzeichnet, dass bei der Anmeldung der erste öffentliche Schlüssel zu dem Diensteserver (2) übertragen wird (4), dass der Diensteserver (2) anhand des ersten öffentlichen Schlüssels eine Berechtigung des Anwenders dadurch überprüft (6), dass entweder der Diensteserver selbst anhand einer Datenbank überprüft, ob der Anwender bereits registriert wurde, oder dass ein Registrierungsserver für den Diensteserver überprüft, ob der Anwender bereits registriert wurde, dass einem berechtigten Anwender von dem Diensteserver (2) eine Zeichenkette mit dem ersten öffentlichen Schlüssel codiert und ein zweiter öffentlicher Schlüssel jeweils übertragen werden (8), dass anwenderseitig diese Zeichenkette mit dem ersten privaten Schlüssel decodiert wird und mit dem zweiten öffentlichen Schlüssel wieder codiert zu dem Diensteserver zurück übertragen wird (9), und dass der Diensteserver den Anwender als authentifiziert erkennt (11), falls die vom Anwender empfangene und mit einem zweiten privaten Schlüssel decodierte Zeichenkette der von dem Diensteserver (2) codierten Zeichenkette entspricht."

X. Anspruch 1 des zweiten Hilfsantrags lautet wie folgt:

"1. Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem Diensteserver über ein

Zugangsmedium (1), wobei anwenderseitig ein erster privater und ein erster öffentlicher Schlüssel bereitgestellt werden, wobei sich der Anwender bei dem Diensteserver (2) anmeldet, dadurch gekennzeichnet, dass bei der Anmeldung der erste öffentliche Schlüssel zu dem Diensteserver (2) übertragen wird (4), dass der Diensteserver (2) anhand des ersten öffentlichen Schlüssels eine Berechtigung des Anwenders dadurch überprüft (6), dass der Diensteserver selbst anhand einer Datenbank überprüft, ob der Anwender bereits registriert wurde, dass einem berechtigten Anwender von dem Diensteserver (2) eine Zeichenkette mit dem ersten öffentlichen Schlüssel codiert und ein zweiter öffentlicher Schlüssel jeweils übertragen werden (8), dass anwenderseitig diese Zeichenkette mit dem ersten privaten Schlüssel decodiert wird und mit dem zweiten öffentlichen Schlüssel wieder codiert zu dem Diensteserver zurück übertragen wird (9), und dass der Diensteserver den Anwender als authentifiziert erkennt (11), falls die vom Anwender empfangene und mit einem zweiten privaten Schlüssel decodierte Zeichenkette der von dem Diensteserver (2) codierten Zeichenkette entspricht."

XI. Anspruch 1 des dritten Hilfsantrags lautet wie folgt:

"1. Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System über ein Zugangsmedium (1), wobei anwenderseitig ein erster privater und ein erster öffentlicher Schlüssel bereitgestellt werden, wobei sich der Anwender bei dem softwarebasierten System (2) anmeldet, dadurch gekennzeichnet, dass bei der Anmeldung der erste öffentliche Schlüssel zu dem softwarebasierten System (2)

übertragen wird (4), dass das softwarebasierte System (2) anhand des ersten öffentlichen Schlüssels eine Berechtigung des Anwenders überprüft (6), dass, wenn ein Anwender als nicht berechtigt erkannt wird, dies dem Anwender als Nachricht übertragen wird (12), dass einem berechtigten Anwender von dem softwarebasierten System (2) eine Zeichenkette mit dem ersten öffentlichen Schlüssel codiert und ein zweiter öffentlicher Schlüssel jeweils übertragen werden (8), dass anwenderseitig diese Zeichenkette mit dem ersten privaten Schlüssel decodiert wird und mit dem zweiten öffentlichen Schlüssel wieder codiert zu dem softwarebasierten System zurück übertragen wird (9) und dass das softwarebasierte System den Anwender als authentifiziert erkennt (11), falls die vom Anwender empfangene und mit einem zweiten privaten Schlüssel decodierte Zeichenkette der von dem softwarebasierten System (2) codierten Zeichenkette entspricht."

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

Entscheidungsgründe

1. *Zulässigkeit der Beschwerde*

Die Beschwerdeschrift und die Beschwerdebegründung wurden wirksam und fristgerecht eingereicht. Die Beschwerdegebühr wurde ebenfalls fristgerecht entrichtet (siehe Sachverhalt und Anträge, Punkt II). Die Beschwerde ist daher zulässig.

2. *Verspätete Vorlage von D13*

Die Beschwerdegegnerin hat weder im schriftlichen Verfahren, noch während der mündlichen Verhandlung Einwände gegen die Zulassung der Entgegenhaltung D13 erhoben. Die Kammer hat diesbezüglich auch keine Bedenken, weil D13 keine neuen Sachverhalte einführt, sondern lediglich eine einzelne Textseite zum Beleg von technischem Hintergrundwissen im Rahmen der mit der Beschwerdebegründung vorgebrachten Argumente und in Reaktion auf Gegenargumente der Beschwerdegegnerin vorgelegt wurde. Die Kammer hat daher D13 im Rahmen ihres Ermessens gemäß Artikel 13(1) VOBK in das Verfahren zugelassen.

3. Die Kammer nimmt im Rahmen der Entscheidungsbegründung auf die folgende Merkmalsgliederung des Anspruchs 1 (Hauptantrag) mit den Teilmerkmalen a), b1) bis b4), c), d) und e) Bezug:

a) Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System über ein Zugangsmedium (1), wobei anwenderseitig ein erster privater und ein erster öffentlicher Schlüssel bereitgestellt werden, wobei sich der Anwender bei dem softwarebasierten System (2) anmeldet, dadurch gekennzeichnet, dass

b1) bei der Anmeldung der erste öffentliche Schlüssel zu dem softwarebasierten System (2) übertragen wird (4),

b2) dass das softwarebasierte System (2) anhand des ersten öffentlichen Schlüssels eine Berechtigung des Anwenders überprüft (6),

b3) dass einem berechtigten Anwender von dem softwarebasierten System (2) eine Zeichenkette mit dem ersten öffentlichen Schlüssel codiert und

b4) ein zweiter öffentlicher Schlüssel jeweils übertragen werden (8),

c) dass anwenderseitig diese Zeichenkette mit dem ersten privaten Schlüssel decodiert wird und

d) mit dem zweiten öffentlichen Schlüssel wieder codiert zu dem softwarebasierten System zurück übertragen wird (9) und

e) dass das softwarebasierte System den Anwender als authentifiziert erkennt (11), falls die vom Anwender empfangene und mit einem zweiten privaten Schlüssel decodierte Zeichenkette der von dem softwarebasierten System (2) codierten Zeichenkette entspricht.

4. Die angefochtene Entscheidung, mit der der Einspruch als unbegründet zurückgewiesen wurde, geht von D1 als nächstliegendem Stand der Technik aus. Die Einspruchsabteilung argumentiert im wesentlichen, dass weder die D1 noch die anderen angezogenen Dokumente zum Stand der Technik offenbaren oder nahelegen, dass ein öffentlicher Schlüssel des Anwenders bei der Anmeldung zu dem softwarebasierten System übertragen wird und dass dieses anhand des öffentlichen Schlüssels eine Berechtigung des Anwenders überprüft, entsprechend den Teilmerkmalen b1) und b2).

5. Die Einsprechende und Beschwerdeführerin begründet ihre Beschwerde im wesentlichen damit, dass es dem Gegenstand des erteilten Anspruchs 1 nach Hauptantrag sowie nach den Hilfsanträgen einerseits ausgehend von der D5 und andererseits ausgehend von der D1, jeweils in Kombination mit der D11, an der notwendigen

erfinderischen Tätigkeit (Artikel 56 EPÜ) mangelt. Die Beschwerdeführerin argumentiert im wesentlichen damit, dass nach Anspruch 1 des Streitpatents offen bleibe welcher Art die Berechtigung ist, auf die geprüft wird. Es werde in Teilmerkmal b2) lediglich "eine Berechtigung" des Anwenders geprüft. Bei einer Verwendung zertifizierter Schlüssel erfolge in der Regel eine Überprüfung der Echtheit des Zertifikats und damit verbunden eine Berechtigungsprüfung des Anwenders anhand eines öffentlichen Schlüssels, nämlich ob der Anwender zur Benutzung des öffentlichen Schlüssels berechtigt sei. Laut Ausführungsbeispiel in den Absätzen [0008], [0014] und [0017] des Streitpatents erfolge eine Berechtigungsprüfung durch Prüfung, ob der erhaltene öffentliche Schlüssel registriert sei. Dies sei jedoch bei der Überprüfung zertifizierter Schlüssel mitunter genau so (mit Verweis auf D11, Spalte 2, Zeilen 43 bis 51).

5.1 Mit Verweis auf Kapitel 7.2.3.2 der D5 mit den Schritten T2.3, T2.6 und T2.7 argumentiert die Beschwerdeführerin, dass sich die Lehre der D5 vom Gegenstand des Anspruchs 1 gemäß Hauptantrag nur dadurch unterscheide, dass der erste und der zweite öffentliche Schlüssel nicht direkt zwischen dem Anwender und dem System ausgetauscht würden, sondern jeweils bei einem Dritten, einem vertrauenswürdigen Schlüsselverwalter, beschafft würden. Dies sei jedoch aus der D11 nahegelegt (siehe Verweis auf Spalte 1, Zeilen 59 bis 64), wonach es eine übliche Alternative darstelle, dem Kommunikationspartner seinen eignen öffentlichen Schlüssel während des Authentisierungsvorgangs zu übermitteln und dafür zertifizierte Schlüssel zu verwenden. Dabei hätte eine nicht erfolgreiche Prüfung des übermittelten

zertifizierten öffentlichen Schlüssels im zentralen Register zwangsläufig auch einen Abbruch des Authentifizierungsverfahrens zur Folge, weil der Anwender mangels zertifzierten Schlüssels nicht zur Authentifizierung berechtigt sei. In diesem Zusammenhang verwies die Beschwerdeführerin auch auf D13, einen Auszug aus einem Fachbuch, zum Beleg des Wissens des Fachmanns, warum und wie der öffentliche Schlüssel vor seiner Verwendung mit Hilfe eines Zertifikats überprüft wird. Darüber hinaus würden gültige Zertifikate üblicherweise in einem directory service DS und damit an einem zentralen Ort auf einem Registrierungsserver gehalten, auf den bei einer Berechtigungsprüfung ähnlich dem oben genannten Ausführungsbeispiel in den Absätzen [0008], [0014] und [0017] des Streitpatents zugegriffen würde (siehe Verweis auf D11, Spalte 2, Zeilen 45 bis 51). Damit sei auch der Gegenstand des Anspruchs 1 gemäß erstem Hilfsantrag nahegelegt. Des weiteren offenbare die D11 auch eine Alternative mit einer lokalen Datenbank in Form einer "certificate revocation list" (CRL), auf die bei einer Berechtigungsprüfung des Anwenders direkt zugegriffen würde (siehe Verweis auf D11, Spalte 2, Zeilen 57ff), wodurch der Gegenstand des Anspruchs 1 nach erstem und zweitem Hilfsantrag nahegelegt sei. Auch die weitere Maßnahme des dritten Hilfsantrags sei fachüblich.

5.2 Entgegen der Auffassung der Einspruchsabteilung offenbare die D1 nicht nur eine Authentifizierung des Autors einer Nachricht, sondern auch der Quelle der Nachricht (siehe Verweis auf D1, Spalte 2, Zeilen 24 und 25, sowie Spalte 5, Zeilen 42 bis 50). Da die D1 unter anderem auch die Möglichkeit offenbare, dass die eigentliche Datennachricht separat versendet wird, so

würde zunächst lediglich deren Versender authentifiziert, bevor die Nachricht tatsächlich versendet würde. Somit offenbare die D1 ein Verfahren zur Authentifizierung eines Anwenders beim Zugang zu einem softwarebasierten System im Sinne des Teilmerkmals a) von Anspruch 1 gemäß Hauptantrag. Darüber hinaus offenbare die D1 ein dem weiteren Gegenstand des Anspruchs 1 entsprechendes Protokoll (mit Verweis auf D1, Spalte 3, Zeilen 52 bis 59, und Spalte 6, Zeilen 14 bis 19). Dadurch, dass der öffentliche Schlüssel des Senders für den Antwortenden "apparent" und damit offensichtlich sei, wäre es für den Fachmann offensichtlich, dass dieser Schlüssel entweder aus einer Datenbank geladen würde oder aber vom Sender mitgeschickt würde. Diese Varianten seien, wie anhand der D11 bei einer Kombination mit der D5 erläutert, austauschbar. Bei einer naheliegenden Durchführung des Verfahrens der D1 mit zertifizierten Schlüsseln erfolge daher inhärent eine Überprüfung der Berechtigung des Anmelders wie bereits im Zusammenhang mit einer Kombination der D5 mit der D11 erläutert. Vor diesem Hintergrund führte auch eine Kombination der D1 mit der D11 zum Gegenstand des Anspruchs 1 nach Haupt- und Hilfsanträgen.

6. Darüber hinaus sei auch aus der D6 und der D12 bekannt, bei der Anmeldung bei einem softwarebasierten System diesem den öffentlichen Schlüssel des Anmelders zur Überprüfung mitzuschicken (mit Verweis auf D6, Seite 3, Zeilen 39 bis 41, und D12, Spalte 7, Zeilen 48 bis 64).

7. Die Beschwerdegegnerin und Patentinhaberin tritt dem entgegen und argumentiert im wesentlichen, dass sich aus der D1 nicht ergebe, dass ein softwarebasiertes System anhand eines öffentlichen Schlüssels eine Berechtigung

eines Anwenders überprüft. Dabei wird auf einen Unterschied zwischen einer Authentifizierung und einer Autorisierung eines Anwenders verwiesen. Durch einen in der D1 als "offensichtlich" bezeichneten öffentlichen Schlüssel werde keine anspruchsgemäße Überprüfung einer Berechtigung des Anwenders nahegelegt, sondern die D1 führe vielmehr explizit davon weg, eine Berechtigung des Senders vorzunehmen, bevor weitere Schritte folgen. Auch aus der weiteren Druckschrift D11 ergebe sich hierzu keine Veranlassung. Eine Authentifizierung eines öffentlichen Schlüssels entspräche nicht einer anspruchsgemäßen Überprüfung einer Berechtigung des Anwenders anhand eines öffentlichen Schlüssels.

8. Auch aus der D5 ergebe sich nicht, dass ein softwarebasiertes System anhand eines öffentlichen Schlüssels eine Berechtigung eines Anwenders überprüft, um nur einem berechtigten Anwender weitere Verfahrensschritte zu ermöglichen. Es würde lediglich offenbart, öffentliche Schlüssel durch einen Schlüsselverwalter bereitzustellen, damit eine Übermittlung der öffentlichen Schlüssel zwischen den Kommunikationspartnern entfallen könne. Würde der Fachmann ausgehend von der D5 zusätzlich die D11 heranziehen, so würde er lediglich dazu gelangen, eine Übermittlung eines zweiten öffentlichen Schlüssels anhand eines Zertifikats durchzuführen, welches lediglich eine Authentifizierung eines öffentlichen Schlüssels nahelege. Eine Berechtigungsprüfung eines Anwenders, ob dieser bereits zuvor registriert wurde, würde damit nicht nahegelegt.

Der Gegenstand von Anspruch 1 würde daher weder ausgehend von der D1, noch ausgehend von der D5, jeweils in Kombination mit der D11, nahegelegt.

Hauptantrag

9. Materiellrechtliche Prüfung des Standes der Technik

9.1 Die Kammer stimmt der Beschwerdegegnerin zu, dass der Gegenstand von Anspruch 1 neu gegenüber der Offenbarung von D5 und D1 ist.

9.2 Gegenüber der D5 unterscheidet sich dieser darin, dass kein Übermitteln der öffentlichen Schlüssel zwischen den Kommunikationspartnern offenbart ist (siehe Teilmerkmale b1) und b4)), sondern diese über einen gemeinsamen Schlüsselverwalter bezogen werden. Entgegen der Auffassung der Beschwerdeführerin offenbart D5 jedoch, selbst wenn man eine breite Auslegung des Wortlauts "eine Berechtigung" in Teilmerkmal b2) annähme, keine Verwendung zertifizierter Schlüssel, sondern einen Austausch der öffentlichen Schlüssel über einen gemeinsamen Schlüsselverwalter (siehe Kapitel 7.2.3.2, erster Absatz). Damit erfolgt in der D5 auch keine Überprüfung der Echtheit eines Zertifikats, ob der Anwender zur Benutzung des öffentlichen Schlüssels berechtigt ist. Somit stellt auch Teilmerkmal b2) einen Unterschied dar.

Die übergeordnete objektive Aufgabe dieser Unterscheidungsmerkmale besteht daher nicht lediglich in einer alternativen Art und Weise des Austauschs der öffentlichen Schlüssel, sondern in der Prüfung der Berechtigung des Anwenders (so auch die

Einspruchsabteilung in der angefochtenen Entscheidung, Punkt 4.7).

Da D5, wie bereits erwähnt, einen gemeinsamen Schlüsselverwalter vorsieht und keine Zertifikate erwähnt, ist zweifelhaft, ob der Fachmann ausgehend von D5 überhaupt eine alternative direkte Übermittlung eines öffentlichen Schlüssels (wie z.B. in der D11) in Betracht ziehen würde. Auch nimmt D5 keine Berechtigungsprüfung eines Anwenders anhand von dessen öffentlichem Schlüssel vor.
Die Beschwerdeführerin hat mit Verweis auf die Schritte T2.3, T2.6 und T2.7 in D5 dem anspruchsgemäßen Anwender den Kommunikationspartner A, dem anspruchsgemäßen softwarebasierten System den Kommunikationspartner B und der anspruchsgemäßen Zeichenkette den Identifikator I_A gegenübergestellt. Zwar erwähnt D5 allgemein aus Sicht von B, dass aufgrund einer Entschlüsselung mit dem privaten Schlüssel von B für A klar sei, dass dieser mit B kommuniziert (siehe S. 353, letzter Absatz), jedoch fehlt ein solcher Hinweis umgekehrt für eine Authentifizierung von A wie diese nach Anspruch 1 des Streitpatents erfolgt (vgl. Teilmerkmale b3), c) und teilweise e)). Anders als nach Anspruch 1, wonach eine Authentifizierung von A erfolgen müsste, wenn ein Vergleich der von B codiert gesendeten Zeichenkette mit der von A mittels dessen privatem Schlüssel decodierter zurückerhaltener Zeichenkette erfolgreich wäre, tritt dieser Effekt nach D5 nicht auf, weil der vergleichbare Identifikator I_A ursprünglich von A stammt (siehe Schritt T2.3) und dieser damit von vornherein in Kenntnis der Zeichenkette ist. Damit wird der Effekt einer Authentifizierung wie in Anspruch 1 bei der Lehre von D5 nicht erreicht. Vielmehr dient der Identifikator I_A als

Basis für einen Blockzähler in der nachfolgenden Kommunikation zur Prüfung der Folgeechtheit (vgl. S. 354 oben). Die Kammer hält daher D5 nicht für den nächstliegenden Stand der Technik.

9.3 Vor diesem Hintergrund wird die Entgegenhaltung D1 als nächstliegender Stand der Technik angesehen, da diese mit dem Anspruchsgegenstand in den strukturellen und funktionalen Merkmalen besser übereinstimmt und das erfolgversprechendere Sprungbrett darstellt (siehe Entscheidung T 0254/86, ABl. 1989, 115 sowie Rechtsprechung der Beschwerdekammern des Europäischen Patentamts, Kapitel I, D. 3 "Nächstliegender Stand der Technik"). Anders als bei D5 erfolgt nach D1 eine Authentifizierung eines Anwenders aus Sicht eines softwarebasierten Systems mit Hilfe einer anspruchsgemäßen Zeichenkette (siehe "authentication string" in D1, Spalte 3, Zeilen 51 bis 63). Die Schritte 2 bis 5 der Figur 2 in D1 mit dem zugehörigen Text der Beschreibung (siehe Spalte 5, Zeile 39ff) offenbaren die Teilmerkmale a), b3) und c) von Anspruch 1, indem ein Sender S ein "authentication request" "req." zu einem Empfänger R überträgt (Schritt 2), R eine mit dem öffentlichen Schlüssel von S verschlüsselte Zeichenkette "st" an S zurücksendet (Schritt 3), die von S mit dessen privatem Schlüssel decodiert wird (Schritt 5). Dabei sieht die Kammer im Hinblick auf Teilmerkmal b3) den Sender S aus der Sicht des Empfängers R als "berechtigten Benutzer" an, da R bereitwillig mit S kommuniziert (entgegen Seite 3, vorletzter Absatz der angefochtenen Entscheidung).

Die Beschwerdeführerin legt den Begriff "eine Berechtigung" in Teilmerkmal b2) so breit aus, dass auch

die Berechtigung des Anwenders zur Benutzung des öffentlichen Schlüssels darunter zu verstehen ist. Da D1 zwar keine Übertragung der öffentlichen Schlüssel, aber eine lokale Schlüsselhaltung offenbare, werde eine Berechtigung als gegeben angenommen, weil ja die öffentlichen Schlüssel vorlägen. Daher sei Teilmerkmal b2) implizit in D1 offenbart. Die Kammer ist jedoch der Auffassung, dass der Gattungsbegriff des Anspruchs 1 eine engere Interpretation impliziert. Da Anspruch 1 auf ein Verfahren zur Authentifizierung eines Anwenders bei einem softwarebasierten System gerichtet ist, ist der Ausdruck "Berechtigung" in Anspruch 1 nur auf diesen Zweck und somit auf eine Berechtigung zum Zugang zum System zu beziehen. Demnach ist auch in Teilmerkmal b2) ein Unterschied gegenüber D1 zu sehen.

Somit unterscheidet sich der Gegenstand von Anspruch 1 von der Offenbarung der D1 zunächst darin, dass ein Übermitteln der öffentlichen Schlüssel zwischen den Kommunikationspartnern (siehe Teilmerkmale b1) und b4)) sowie eine Berechtigungsprüfung des Anwenders anhand des ersten öffentlichen Schlüssels (Teilmerkmal b2)) nicht explizit offenbart sind.

9.4 Entgegen der Argumentation der Beschwerdeführerin besteht jedoch auch der weitere Unterschied, dass in D1 ein Vergleich nicht direkt mit der Zeichenkette (siehe Teilmerkmale d) und e)) erfolgt, sondern allgemeiner mit einer Funktion, die die Zeichenkette beinhaltet (vgl. D1, Spalte 3, Zeilen 55 bis 59). Dies wurde von der Beschwerdeführerin während der mündlichen Verhandlung auch nicht weiter bestritten.

Die Beschwerdegegnerin hat in der mündlichen Verhandlung mit Verweis auf Schritt 6 in Fig. 2 sowie auf Spalte 5, Zeile 65f. und Spalte 6, Zeile 1f. von D1 argumentiert, dass ein wesentlicher Unterschied zu Teilmerkmal e) darin bestünde, dass S eine "authentication message" als eine Funktion "Auth(m, st)" nicht nur von der Zeichenkette st, sondern auch von der Nachricht m an R zurücksende. Lasse man die Komponente der Nachricht m einfach weg, so funktioniere Schritt 6 in Fig. 2 von D1 nicht mehr ohne weiteres. Der Fachmann würde daher ausgehend von D1 nicht in Betracht ziehen, dass der Empfänger R einen direkten Vergleich der gesendeten Zeichenkette st mit ausschließlich der empfangenen und decodierten Zeichenkette aus "Auth(m, st)" vornimmt.

Die Kammer stimmt jedoch der Beschwerdeführerin zu, dass der letztere Unterscheid gegenüber D1 alleine keine erfinderische Tätigkeit begründet, sondern eine naheliegende Variante des gleichen Konzeptes darstellt. Anspruch 1 ist auf eine Authentifizierung eines Anwenders gerichtet. Zu diesem gleichen Zweck dient in D1 jedoch in erster Linie die verschlüsselte und wieder entschlüsselte Zeichenkette st, nicht jedoch die Komponente der Nachricht m. Zudem ist das Teilmerkmal e) so breit formuliert, dass auch ein Vergleich der vom Anwender empfangenen und mit einem zweiten privaten Schlüssel decodierten Zeichenkette mit der von dem softwarebasierten System codierten Zeichenkette in verarbeiteter Form unter den Anspruchswortlaut fällt.

Des weiteren besteht kein Synergieeffekt zwischen den beiden oben genannten Unterscheidungsmerkmalen, nämlich einem Übermitteln der öffentlichen Schlüssel zwischen den Kommunikationspartnern und einer

Berechtigungsprüfung anhand des öffentlichen Schlüssels einerseits und einem direkten Vergleich der Zeichenkette andererseits.

9.5 Als die den übrigen Unterscheidungsmerkmalen b1), b2) und b4) zu Grunde liegende übergeordnete objektive technische Aufgabe ausgehend von D1 wird, in Übereinstimmung mit der Beschwerdegegnerin, eine Prüfung der Berechtigung des Anwenders für einen Zugang zum System angesehen (siehe auch die angefochtene Entscheidung, Punkt 4.7).

9.6 Austausch öffentlicher Schlüssel (Teilmerkmale b1) und b4))

Unabhängig davon, wie der Fachmann die Formulierung "apparent sender's public key" (D1, Spalte 3, Zeile 55) verstehen würde, geht D1 davon aus, dass den Kommunikationspartnern die jeweiligen öffentlichen Schlüssel bekannt sind. Dies ist jedoch eine Eigenschaft, die bereits durch den Ausdruck "öffentlich" einem solchen Schlüssel inhärent ist. Es war bereits vor dem Prioritätstag des Streitpatents bekannt, dass neben einem Bezug öffentlicher Schlüssel von einer Datenbank alternativ der direkte Austausch zwischen den Kommunikationspartnern die einfachste Form zum Gebrauch öffentlicher Schlüssel darstellt. Dieses allgemeine Fachwissen wird durch die weitere Entgegenhaltung D11 belegt und ist bereits dort als bekannter technologischer Hintergrund beschrieben (vgl. D11, Spalte 1, Zeilen 62 bis 64). Insofern ist die Kammer der Auffassung, dass der Fachmann einen direkten Austausch der öffentlichen Schlüssel zwischen den Kommunikationspartnern gemäß den Teilmerkmalen b1) und

b4) von Anspruch 1 ohne erfinderische Überlegungen als fachüblich in Betracht ziehen würde.

9.7 Berechtigungsprüfung (Teilmerkmal b2))

Die Beschwerdegegnerin hat grundsätzlich auf einen Unterschied zwischen einer Authentifizierung in D1 und einer Autorisierung eines Anwenders nach Anspruch 1 verwiesen. Die Kammer versteht Autorisierung und Authentifizierung jedoch nicht als sich gegenseitig ausschließenden Begriffe, sondern es wird vielmehr auch bei einer Autorisierung zunächst eine Authentifizierung erfolgen, um dann bei erfolgreicher Identitätsprüfung eine entsprechende Berechtigung zu erteilen.

Die Lehre von D1 sieht neben einer Authentifizierung des Senders (siehe D1, Spalte 3, Zeilen 60f "authentication of the sender's identity") auch eine Autorisierung vor (siehe Spalte 5, Zeile 39ff "authorisation request message"), welche unabhängig von der eigentlichen Nachricht versendet werden kann. Zwar erfolgt eine Authentifizierung der Quelle einer Nachricht (vgl. D1, Spalte 2, Zeilen 24 bis 25), jedoch ist die Kammer nicht davon überzeugt, dass in D1 mit einer solchen "authorisation request message" über eine Berechtigung des Senders S zum Zugang zum System R entschieden wird. Insbesondere erfolgt dies nicht anhand eines öffentlichen Schlüssels des Senders S, da die D1 keinen Hinweis auf eine Überprüfung des öffentlichen Schlüssels des Senders gibt.

9.8 Die Beschwerdeführerin hat argumentiert, dass der Fachmann die Lehre von D1 mit der von D11 kombinieren würde und damit eine Verwendung von zertifizierten

öffentlichen Schlüsseln in Betracht ziehen würde. Die Überprüfung des Zertifikats des öffentlichen Schlüssels des Senders bzw. Anwenders käme einer Berechtigungsprüfung anhand eines öffentlichen Schlüssels im Sinne von Teilmerkmal b2) von Anspruch 1 gleich, weil im Fall eines fehlerhaften Zertifikats der zugehörige öffentliche Schlüssel nicht zur Verwendung komme.

9.9 Dem ist die Beschwerdegegnerin mit dem Argument entgegen getreten, dass der Fachmann ausgehend von D1 Zertifikate nicht in Betracht ziehen würde, da D1 ohnehin von einem "non-malleable cryptography" System ausgehe (mit Verweis auf Spalte 5, Zeilen 10ff.). Eine Verwendung von Zertifikaten sei vor diesem Hintergrund nicht erforderlich.

9.10 Die Beschwerdeführerin ist hingegen der Auffassung, dass sich gerade aus dem Erfordernis eines "non-malleable cryptography" Systems eine Motivation zum Einsatz zertifizierter öffentlicher Schlüssel ergibt. Hintergrund in D1 sei der Versuch, einen "man in the middle" Angriff zu verhindern (vgl. Figuren 1 und 3). Zu diesem Zweck sei in den Schritten 13 und 14 von Figur 3 sowie in Spalte 6, Zeile 43f ("S's public key is non-malleable") eine klare Aufforderung zu sehen, dass der öffentliche Schlüssel von S nicht manipuliert werden kann. Genau zu diesem Zweck seien Zertifikate eingeführt worden. Aus Sicht der Kammer hat die Beschwerdeführerin damit überzeugend dargelegt, weshalb der Fachmann ausgehend von der Lehre der Entgegenhaltung D1 zertifizierte Schlüssel verwenden würde.

9.11 Die Kammer stimmt weiter der Ansicht der Beschwerdeführerin zu, dass unter der Annahme einer naheliegenden Verwendung eines zertifizierten öffentlichen Schlüssels für den Sender S damit implizit auch eine Gültigkeits- und Echtheitsprüfung des Zertifikats einhergeht. Es war bekannt, dass bei Verwendung eines Zertifikats neben dem öffentlichen Schlüssel im Klartext dieser öffentliche Schlüssel auch in einer mit dem privaten Schlüssel der Zertifizierungsbehörde verschlüsselten Form im Zertifikat verwendet wird (vgl. D13, Seite 41, Zeilen 29 bis 32, oder alternativ D11, Spalte 1, Zeile 65 bis Spalte 2, Zeile 13).

Die Echtheitsprüfung des Zertifikats erfolgt durch Entschlüsselung mit Hilfe des öffentlichen Schlüssels der Zertifizierungsbehörde und durch anschließenden Vergleich von entschlüsseltem Zertifikat mit der Klartextversion des öffentlichen Schlüssels (vgl. z.B. D11, Spalte 1, Zeilen 54 bis 59; D13, Seite 41, Zeile 27ff). Somit erfolgt eine Verifizierung eines Zertifikats "anhand des … öffentlichen Schlüssels" eines Senders wie in Teilmerkmal b2) beansprucht.

9.12 Weiter erfolgt für den Fall einer fehlgeschlagenen Verifizierung eines Zertifikats keine weitere Authentifizierung des Inhabers des öffentlichen Schlüssels. Unter der Annahme einer Verwendung von zertifizierten öffentlichen Schlüsseln im Rahmen der D1 würde bei einer fehlgeschlagenen Verifizierung des Zertifikats der öffentliche Schlüssel nicht verwendet werden und damit auch keine Verschlüsselung des "authentication string" (vgl. D1, Spalte 3, Zeile 52ff) mit diesem öffentlichen Schlüssel im Sinne der weiteren

Kommunikation erfolgen (vgl. Figur 2 von D1). Damit hat eine Verifizierung des Zertifikats des öffentlichen Schlüssels den Effekt einer Berechtigungsprüfung und damit die Wirkung von Teilmerkmal b2). Damit handelt es sich, entgegen der Auffassung der Beschwerdegegnerin, ebenfalls um ein zweistufiges Verfahren.

9.13 Der Fachmann würde somit ausgehend von D1 kombiniert mit der Lehre von D11 über die Grundlagen der asymmetrischen Verschlüsselung auf naheliegende Weise eine Verwendung von zertifizierten öffentlichen Schlüsseln in Betracht ziehen, und mit einer Überprüfung des Zertifikats als Bonus-Effekt eine Berechtigungsprüfung eines Anwenders anhand eines öffentlichen Schlüssels im Sinne des Teilmerkmals b2) von Anspruch 1 vornehmen. Weiter würde der Fachmann aus D11 auch einen direkten Austausch der öffentlichen Schlüssel zwischen den Kommunikationspartnern gemäß den Teilmerkmalen b1) und b4) von Anspruch 1 ohne erfinderische Überlegungen als fachüblich in Betracht ziehen (siehe Punkt 9.6). Der Gegenstand von Anspruch 1 ist daher durch eine Kombination von D1 mit D11 nahegelegt (Artikel 52(1) und Artikel 56 EPÜ).

Erster und zweiter Hilfsantrag

10. Der jeweilige Anspruch 1 dieser Anträge ist anstelle auf ein softwarebasiertes System auf einen Diensteserver gerichtet und weist das weitere Teilmerkmal auf, dass der Diensteserver selbst anhand einer Datenbank überprüft, ob der Anwender bereits registriert wurde (der erste Hilfsantrag in Form einer Alternative).

10.1 Die Beschwerdeführerin hat in diesem Zusammenhang argumentiert, dass es z.B. aus D11 bekannt war, eine sogenannte "certificate revocation list" CRL als lokale Datenbank zu laden (vgl. D11, Spalte 3, Zeile 8f) und zu prüfen, ob das Zertifikat (welches ja den öffentlichen Schlüssel beinhaltet) dort registriert und damit ungültig sei (vgl. D11, Spalte 2, Zeile 57ff). Bereits damit wäre eine Prüfung auf Registrierung anhand einer lokalen Datenbank und damit indirekt auch anhand des öffentlichen Schlüssels verbunden. Dabei sei jeder "server node" 104a bis 104n in Figur 1 von D11 als anspruchsgemäßer Diensteserver anzusehen.

10.2 Die Beschwerdegegnerin hat dem entgegen gehalten, dass es sich bei CRL um eine Negativliste handele, welche keine Prüfung einer Berechtigung zum Zugang ermögliche, denn die Tatsache, dass ein Zertifikat nicht in der CRL vertreten sei, berechtige nicht zum Zugang.

10.3 Die Kammer teilt jedoch die von der Beschwerdeführerin während der mündlichen Verhandlung geäußerte Auffassung, dass in D11 bei einer Prüfung auf einen Zugang zu einem der Server 104 die sogenannte "certificate revocation list" CRL als lokale Datenbank nicht isoliert betrachtet werden darf, sondern im Zusammenhang mit dem Schritt 302 in Figur 3A zu sehen ist. Darin wird vorab geprüft, ob ein Zertifikat überhaupt von der gültigen Zertifizierungsinstanz signiert ist und damit systemzugehörig (vgl. auch D13, Zeilen 37 und 38) ist. Wenn das systemzugehörige Zertifikat nicht in der CRL als abgelaufen deklariert ist, erfolgt die weiter oben erläuterte Prüfung des öffentlichen Schlüssels anhand des Zertifikats, und zwar anspruchsgemäß auf einem einzelnen Server 104.

10.4 Nach der Auffassung der Kammer sind die zusätzlichen Merkmale des jeweiligen Anspruchs 1 in Form einer lokalen Datenbank mit einer "certificate revocation list" CRL, auf die bei einer Berechtigungsprüfung des Anwenders direkt zugegriffen wird, mit einer vorangehenden Prüfung auf Systemzugehörigkeit des Zertifikats aus D11, Spalte 2, Zeilen 57ff sowie aus den Figuren 3A und 3B bekannt. Die zusätzlichen Merkmale fügen daher dem Gegenstand des Anspruchs 1 nach dem Hauptantrag nichts Erfinderisches hinzu, weshalb auch der jeweilige Gegenstand des Anspruchs 1 nach erstem und zweitem Hilfsantrag durch eine Kombination von D1 mit D11 nahegelegt ist (Artikel 52(1) und Artikel 56 EPÜ).

Dritter Hilfsantrag

11. Bei Anspruch 1 dieses Antrags handelt es sich um eine Kombination der erteilten Ansprüche 1 und 3. Der Gegenstand weist gegenüber dem Anspruch 1 des Hauptantrags das weitere Teilmerkmal auf, dass, wenn ein Anwender als nicht berechtigt erkannt wird, dies dem Anwender als Nachricht übertragen wird.

11.1 Die Beschwerdegegnerin hat argumentiert, dadurch würde erreicht, dass der Anwender wisse, dass ein Zugang zum System an der Ungültigkeit seines öffentlichen Schlüssels gescheitert sei. Nirgends in D1 oder D11 wäre ein Hinweis zu entnehmen, den Aufwand für eine solche Benachrichtigung vorzunehmen.

11.2 Die Beschwerdeführerin hielt dem entgegen, es sei für den Fachmann naheliegend, für den Fall einer Verweigerung des Zugriffs aktiv zu reagieren. Dies

ergebe sich unter anderem aus der Formulierung "the user is denied access to the network's resources…" in D11, Spalte 7, Zeile 1, was nahelege, dass nicht lediglich der Prozess stoppt, sondern dies dem Benutzer auch mitgeteilt werde. Ohne eine Nachricht an den Anwender riskiere der Fachmann zudem, dass der Anwender sofort noch einmal versucht, einen Zugang zum System zu erlangen.

11.3 Insbesondere das letzte Argument überzeugt die Kammer, dass der Fachmann eine Nachricht an den Anwender auch im Rahmen der Lehre von D11 auf naheliegende Weise in Betracht ziehen würde, weil der technische Aufwand hierfür gering ist im Vergleich zu dem technischen Aufwand, der erforderlich wäre, um eine Blockierung des Systems durch anhaltende erneute Anmeldeversuche des Anwenders am System zu verhindern. Die Kammer stimmt der Beschwerdeführerin weiter zu, dass eine Nachricht an den Anwender bei einer Zugriffsverweigerung bereits vor dem Prioritätstag eine fachnotorisch bekannte Maßnahme darstellte. Daher ist auch der Gegenstand des Anspruchs 1 nach dem dritten Hilfsantrag durch eine Kombination von D1 mit D11 und dem allgemeinen Fachwissen nahegelegt (Artikel 52(1) und Artikel 56 EPÜ).

12. Damit erfüllt keiner der Anträge der Beschwerdegegnerin das Erfordernis der erfinderischen Tätigkeit nach Artikel 56 EPÜ.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Das Patent wird widerrufen.

Die Geschäftsstellenbeamtin Die Vorsitzende

K. Götz A. Ritzka