BUNDESPATENTGERICHT

IM NAMEN DES VOLKES

URTEIL

Verkündet am
7. Juni 2018
…

2 Ni 22/16 (EP)

(Aktenzeichen)

In der Patentnichtigkeitssache

…

ECLI:DE:BPatG:2018:070618U2Ni22.16EP.0

…

betreffend das europäische Patent EP 1 320 012
(DE 602 41 341)

hat der 2. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf Grund der mündlichen Verhandlung vom 7. Juni 2018 unter Mitwirkung des Vorsitzenden Richters Guth sowie der Richterin Hartlieb und der Richter Dipl.-Ing. Baumgardt, Dipl.-Phys. Dr. Forkel und Dipl.-Ing. Hoffmann

für Recht erkannt:

I. Das europäische Patent 1 320 012 wird mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland für nichtig erklärt.

II. Die Beklagte hat die Kosten des Rechtsstreits zu tragen.

III. Das Urteil ist gegen Sicherheitsleistung in Höhe von 120% des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

T a t b e s t a n d

Die Nichtigkeitsklage betrifft das am 11. Dezember 2002 in der Verfahrenssprache Englisch angemeldete, die Prioritäten zweier US-Anmeldungen vom 12. Dezember 2001 und vom 12. Februar 2002 beanspruchende und am 19. Oktober 2011 veröffentlichte europäische Patent **EP 1 320 012 B1** (Streitpatent) mit der Bezeichnung „System and method for providing distributed access control to secured items“.

Das Streitpatent umfasst 8 Patentansprüche, von denen die Ansprüche 1 und 5 nebengeordnet, die Unteransprüche 2 bis 4 auf den Patentanspruch 1 und die Patentansprüche 6 bis 8 auf den Patentanspruch 5 unmittelbar oder mittelbar rückbezogen sind.

Die Ansprüche 1 und 5 des Streitpatents lauten in der Verfahrenssprache Englisch jeweils mit einer Gliederung versehen:

Anspruch 1:

M1 **1.** A distributed access control system adapted to restrict access of a user to secured items, said system comprising:

M1.1 a central server (500) having a server module (502) adapted to provide overall access control;

M1.1.1 wherein the access control, performed by said central server (500), is adapted to operate to permit or deny an access request of the user to the secured items in accordance with access privileges granted to the requesting user and access rules (229) in the secured items;

characterized by

M1.2 a plurality of local servers (570) coupled to the central server (500), each of said local servers (570) including a local module (572) adapted to provide local access control to a group of designated users;

M1.2.1 wherein the access request by the user is processed in a distributed manner by one or more of said local servers (570); and

M1.2.2 wherein, when the access request is processed in said local server (570), the requesting user is granted access to the secured items without having

to access said central server (500) when the access privileges of the requesting user are permitted by the access rules (229) in the secured items.

Anspruch 5:

M5 **5.** A method used in a distributed access control system, the method comprising:

M5.1 providing overall access control by a server module (502) in a central server (500);

M5.1.1 wherein the access controls, performed by said central server (500) operates to permit or deny an access request to the secured items by a requesting user in accordance with access privileges granted to the requesting user and access rules (229) in the secured items;

characterized by

M5.2 providing local access control to a group of designated uses by a local module (572) respectively provided in local servers (570), wherein the local servers (670) are coupled to the central server (600);

M5.2.1 wherein the access request by the user is processed in a distributed manner by one or more of said local servers (570); and

M5.2.2 wherein, when the access request is processed in said local server (570), the requesting user is granted access to the secured items without having to access said central server (500) when the access privileges of the requesting user are permitted by the access rules (229) in the secured items.

Hinsichtlich des Wortlauts der weiteren Patentansprüche 2 bis 4 und 6 bis 8 wird auf die Patentschrift verwiesen.

Die Beklagte verteidigt das Streitpatent in vollem Umfang und hilfsweise mit den Hilfsanträgen 1 bis 6.

Anspruch 1 des **Hilfsantrags 1** hat - unter Kenntlichmachung der Unterschiede zum Hauptantrag - folgenden Wortlaut:

H1-M1 A distributed access control system adapted to restrict access of a user to secured items **including executable code**, said system comprising:

M1.1 a central server (500) having a server module (502) adapted to provide overall access control;

M1.1.1 wherein the access control, performed by said central server (500), is adapted to operate to permit or deny an access request of the user to the secured items in accordance with access privileges granted to the requesting user and access rules (229) in the secured items;

~~characterized by~~

M1.2 a plurality of local servers (570) coupled to the central server (500), each of said local servers (570) including a local module (572) adapted to provide local access control to a group of designated users;

M1.2.1 wherein the access request by the user is processed in a distributed manner by one or more of said local servers (570); and

M1.2.2 wherein, when the access request is processed in said local server (570), the requesting user is granted access to the secured items without having to access said central server (500) when the access privileges of the re-

questing user are permitted by the access rules (229) in the secured items.

Anspruch 1 des **Hilfsantrags 2** hat - unter Kenntlichmachung der Unterschiede zum Hauptantrag - folgenden Wortlaut:

M1 A distributed access control system adapted to restrict access of a user to secured items, said system comprising:

H2-M1.1 a central server (500) having a server module (502) adapted to provide overall access control**, wherein the server module in the central server maintains a database that includes a list of users and corresponding access privileges**;

M1.1.1 wherein the access control, performed by said central server (500), is adapted to operate to permit or deny an access request of the user to the secured items in accordance with access privileges granted to the requesting user and access rules (229) in the secured items;

~~characterized by~~

H2-M1.2 a plurality of local servers (570) coupled to the central server (500), each of said local servers (570) including a local module (572) adapted to provide local access control to a group of designated users**, wherein the local module is a copy or a subset of the server module**;

M1.2.1 wherein the access request by the user is processed in a distributed manner by one or more of said local servers (570); and

M1.2.2 wherein, when the access request is processed in said local server (570), the requesting user is granted access to the secured items without having to access said central server (500) when the access privileges of the re-

questing user are permitted by the access rules (229) in the secured items.

Anspruch 1 des **Hilfsantrags 3** hat - unter Kenntlichmachung der Unterschiede *zum Hilfsantrag 2* - folgenden Wortlaut:

M1 A distributed access control system adapted to restrict access of a user to secured items, said system comprising:

H3-M1.1 a central server (500) having a server module (502) adapted to provide overall access control, wherein the server module in the central server maintains a database that includes a list of users and corresponding access privileges, **wherein the access privileges specify membership in one or more user groups**;

M1.1.1 wherein the access control, performed by said central server (500), is adapted to operate to permit or deny an access request of the user to the secured items in accordance with access privileges granted to the requesting user and access rules (229) in the secured items;

H2-M1.2 a plurality of local servers (570) coupled to the central server (500), each of said local servers (570) including a local module (572) adapted to provide local access control to a group of designated users, wherein the local module is a copy or a subset of the server module;

M1.2.1 wherein the access request by the user is processed in a distributed manner by one or more of said local servers (570); and

M1.2.2 wherein, when the access request is processed in said local server (570), the requesting user is granted access to the secured items without having to access said central server (500) when the access privileges of the re-

questing user are permitted by the access rules (229) in the secured items.

Anspruch 1 des **Hilfsantrags 4** hat - unter Kenntlichmachung der Unterschiede *zum Hilfsantrag 3* - folgenden Wortlaut:

M1 A distributed access control system adapted to restrict access of a user to secured items, said system comprising:

H4-M1.0 **a user authentication process (600) for authenticating the user before being able to access secured items;**

H3-M1.1 a central server (500) having a server module (502) adapted to provide overall access control, wherein the server module in the central server maintains a database that includes a list of users and corresponding access privileges, wherein the access privileges specify membership in one or more user groups;

M1.1.1 wherein the access control, performed by said central server (500), is adapted to operate to permit or deny an access request of the user to the secured items in accordance with access privileges granted to the requesting user and access rules (229) in the secured items;

H2-M1.2 a plurality of local servers (570) coupled to the central server (500), each of said local servers (570) including a local module (572) adapted to provide local access control to a group of designated users, wherein the local module is a copy or a subset of the server module;

M1.2.1 wherein the access request by the user is processed in a distributed manner by one or more of said local servers (570); and

M1.2.2 wherein, when the access request is processed in said local server (570), the requesting user is granted access to the secured items without having

to access said central server (500) when the access privileges of the requesting user are permitted by the access rules (229) in the secured items.

Anspruch 1 des **Hilfsantrags 5** hat - unter Kenntlichmachung der Unterschiede *zum Hilfsantrag 4* - folgenden Wortlaut:

H1-M1 A distributed access control system adapted to restrict access of a user to secured items **including executable code**, said system comprising:

H4-M1.0 a user authentication process (600) for authenticating the user before being able to access secured items;

H3-M1.1 a central server (500) having a server module (502) adapted to provide overall access control, wherein the server module in the central server maintains a database that includes a list of users and corresponding access privileges, wherein the access privileges specify membership in one or more user groups;

M1.1.1 wherein the access control, performed by said central server (500), is adapted to operate to permit or deny an access request of the user to the secured items in accordance with access privileges granted to the requesting user and access rules (229) in the secured items;

H2-M1.2 a plurality of local servers (570) coupled to the central server (500), each of said local servers (570) including a local module (572) adapted to provide local access control to a group of designated users, wherein the local module is a copy or a subset of the server module;

M1.2.1 wherein the access request by the user is processed in a distributed manner by one or more of said local servers (570); and

M1.2.2 wherein, when the access request is processed in said local server (570), the requesting user is granted access to the secured items without having to access said central server (500) when the access privileges of the requesting user are permitted by the access rules (229) in the secured items.

Anspruch 1 des **Hilfsantrags 6** hat - unter Kenntlichmachung der Unterschiede *zum Hilfsantrag 5* - folgenden Wortlaut:

H1-M1 A distributed access control system adapted to restrict access of a user to secured items including executable code, said system comprising:

H4-M1.0 a user authentication process (600) for authenticating the user before being able to access secured items;

H2-M1.1 a central server (500) having a server module (502) adapted to provide overall access control, wherein the server module in the central server maintains a database that includes a list of users and corresponding access privileges~~, wherein the access privileges specify membership in one or more user groups~~;

M1.1.1 wherein the access control, performed by said central server (500), is adapted to operate to permit or deny an access request of the user to the secured items in accordance with access privileges granted to the requesting user and access rules (229) in the secured items;

H2-M1.2 a plurality of local servers (570) coupled to the central server (500), each of said local servers (570) including a local module (572) adapted to provide local access control to a group of designated users, wherein the local module is a copy or a subset of the server module;

M1.2.1 wherein the access request by the user is processed in a distributed manner by one or more of said local servers (570); and

M1.2.2 wherein, when the access request is processed in said local server (570), the requesting user is granted access to the secured items without having to access said central server (500) when the access privileges of the requesting user are permitted by the access rules (229) in the secured items.

Die Klägerin begründet die Klage mit dem Nichtigkeitsgrund der fehlenden Patentfähigkeit, insbesondere der fehlenden Neuheit. Schriftsätzlich hat die Klägerin die weiteren Nichtigkeitsgründe der mangelnden Ausführbarkeit und der unzulässigen Erweiterung hinsichtlich der Hilfsanträge geltend gemacht.

Sie stützt ihr Vorbringen auf die nachstehend genannten Dokumente

NK6	US 5 495 533 A
NK7	US 6 064 656 A
NK8, 8a, 8d	BEA WebLogic Server
NK9	US 2001 / 7 133 A1
NK10	EP 0 672 991 A2
NK11	US 5 933 498 A
NK12	EP 0 447 339 A2

sowie

NK6b – STEINER, J.G. et al.: Kerberos: An Authentication Service For Open Network Systems. In: Usenix Conference Proceedings, Februar 1988, pp. 191 - 202

NK13 – Gutachten Prof. Dr. R…

NK15 – SINHA, Pradeep K.: Distributed Operating Systems, Concepts and Design. IEEE Press, 1997 (Auszüge)

NK16 – Windows NT 3.5 Guidelines for Security, Audit, and Control. Microsoft Press, 1994 (Auszüge)

NK17 – Internet Security Glossary RFC 2828, Mai 2000, page 94

NK18 – SPANIOL, O.: Sicherheit in Kommunikationsnetzen. Skript zur Vorlesung an der RWTH Aachen, korrigierte erste Fassung, 14. Juli 2000, Kapitel 7: Kerberos

NK19 – The Kerberos Network Authentication Service (V5), Network Working Group, Protokoll RFC 1510, September 1993, pp. 1 - 47

In Ergänzung seines ersten Hinweises hat der Senat mit weiterem Hinweis die folgenden beiden Druckschriften als Beleg für das Fachwissen des Durchschnittsfachmanns in das Verfahren eingeführt:

D1 NK6 Reference 8: Steiner, J.G. et al.: Kerberos: An Authentication Service For Open Network Systems, Usenix Conference Proceedings, pp. 183 - 190, February 1988 (erwähnt in **NK6** Sp. 4 Z. 5 - 8)

D2 Security Model von Windows NT, zitiert aus **US 6 308 274 B1** Sp. 4 Z. 29 ff. und Figur 2, Figur 3.

Die Klägerin ist der Ansicht, das Streitpatent sei nicht patentfähig, weil die Druckschriften **NK6**, **NK7**, **NK8**, **NK9** und **NK10** sämtliche Merkmale der Ansprüche 1 und 5 neuheitsschädlich vorwegnähmen oder weil die Ansprüche jedenfalls ausgehend von den Entgegenhaltungen **NK7**, **NK11** mit **NK6** bzw. **NK7** und von **NK12** in Verbindung mit **NK6** nahegelegt seien. Die zusätzlichen Merkmale der Unteransprüche seien vom Stand der Technik gemäß **NK9**, **NK7** sowie **NK6** bis **NK11** vorweggenommen oder durch diesen nahegelegt. Die vom Senat eingeführten Entgegenhaltungen **D1** und **D2** beinhalteten zum Prioritätszeitpunkt des

Streitpatents bereits allgemein bekanntes Fachwissen, wie auch etwa die Unterlagen **NK15** und **NK6** sowie **NB5**, **NK17** und **NB7**, **NK18** zeigten.

Der Gegenstand von Hilfsantrag 1 sei nicht neu, gegenüber **NK6** bis **NK10** und ausgehend von **NK11** nahegelegt. Die Ansprüche 1 und 3 gemäß Hilfsantrag 2 seien nicht ausführbar, unklar, gegenüber **NK6** nicht neu bzw. beruhten ausgehend von **NK6** in Verbindung mit **D1** oder **NK6** in Verbindung mit **D2** ergänzt durch **NK16** nicht auf erfinderischer Tätigkeit, ebenso wie ausgehend von **NK9**.
Anspruch 1 gemäß Hilfsantrag 3 sei – auch den Schutzbereich betreffend - unzulässig erweitert, und beruhe nicht auf erfinderischer Tätigkeit gegenüber **NK6** in Verbindung mit dem Kerberos-Server gemäß **NK15**, **NK18**, **NK19** oder auch mit dem Betriebssystem Windows NT gemäß **D2**. Dies gelte im Wesentlichen auch für die Hilfsanträge 4, 5 und 6.

Die Klägerin stellt den Antrag,

> das europäische Patent 1 320 012 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland in vollem Umfang für nichtig zu erklären.

Die Beklagte stellt den Antrag,

> die Klage abzuweisen,
> hilfsweise
> unter Klageabweisung im Übrigen das europäische Patent 1 320 012 dadurch teilweise für nichtig zu erklären, dass seine Patentansprüche die Fassung eines der Hilfsanträge 1 und 2 vom 20. Oktober 2017, weiter hilfsweise die Fassung eines der Hilfsanträge 3 bis 6 in der Fassung vom 7. Juni 2018, in dieser Reihenfolge, erhalten.

Die Beklagte erklärt, dass sie die Patentansprüche nach Hauptantrag und Hilfsanträgen jeweils als geschlossene Anspruchssätze versteht, die jeweils in ihrer Gesamtheit beansprucht werden.

Die Beklagte tritt der Argumentation der Klägerin in vollem Umfang und hilfsweise beschränkt mit sechs Hilfsanträgen entgegen.

Sie ist der Meinung, die vom Senat eingeführten Entgegenhaltungen **D1** und **D2** seien als Beleg für allgemeines Fachwissen nicht geeignet. Auch werde der Zeitpunkt der Veröffentlichung der **D1** bestritten.

Das Streitpatent unterscheide streng zwischen Authentifizierung und Autorisierung.

Das streitpatentgemäße Zugangskontrollsystem beruhe - funktional getrennt - einerseits auf Zugangsprivilegien, die die Identitätsfeststellung eines Benutzers beträfen und ausschließlich auf einem zentralen Server hinterlegt seien, sowie andererseits auf Zugangsregeln, die in den gesicherten Elementen hinterlegt seien und die bestimmten, ob ein bestimmter identifizierter Benutzer über bestimmte Zugriffsrechte verfüge. Der zentrale Server sei in der Lage, die Gesamtzugangskontrolle im Hinblick auf den Zugriff auf ein gesichertes Element bereitzustellen und übermittle in diesem Rahmen die Zugangsprivilegien an den lokalen Server.

Keine der Entgegenhaltungen zeige eine solche zeitgleiche, zweigeteilte Speicherung der zugriffsrelevanten Informationen an zentraler Stelle und in gesicherten Elementen oder lege diese nahe. Insbesondere offenbare das Kerberos-Ticket der **NK6**, die auf einem fundamental anderen Sicherungsmechanismus beruhe, nämlich auf einem Archiv zur Verteilung von kryptographischen Schlüsseln, jedenfalls nicht das gleichzeitige Vorhandensein eines anspruchsgemäßen zentralen Servers und gesicherten Elementen mit darin enthaltenen Zugangsregeln als auch das gleichzeitige Vorhandensein von lokalen Servern und gesicherten Elementen und auch nicht designierte Benutzer, die einem lokalen Server zugeordnet sind.

Außerdem hätte der Fachmann weder **D1** noch **D2** zur Lösung der Aufgabe des Streitpatents herangezogen, da dort keine zweigeteilte Speicherung von autorisierungsbezogenen Daten offenbart sei.

Jedenfalls aber sei das Streitpatent in der Fassung der zulässigen Hilfsanträge bestandsfähig, deren Lehre ursprünglich offenbart und ausführbar sei. Keine der Entgegenhaltungen offenbare gesicherte Dateien mit einem ausführbaren Code. Eine zweiteilige Speicherung der für die Autorisierung des anfragenden Benutzers benötigten Daten sei ebenfalls nicht im Stand der Technik beschrieben oder durch diesen nahegelegt. Insbesondere handele es sich bei dem der Authentifizierung - der dann eine Autorisierung folgen könne - dienenden „Kerberos-Ticket“ nicht um ein Zugangsprivileg im Sinne des Streitpatents.

Hierzu bezieht sie sich auf die folgenden Dokumente:

NB2 – Wikipedia: Server

NB3 – Internet Security Glossary RFC 2828, Mai 2000, pp. 1 – 18, p. 212

NB4 – LI GONG, C.L. et al.: User Authentication and Authorization in the Java Platform. In: Proceedings of the 15th Annual Computer Security Applications Conference, Dezember 1999 (6 Seiten)

NB5 – KABAY, M.E.: Identification, Authentication and Authorization on the World Wide Web. ICSA White Paper, 1997, pp. 1 - 33

NB6 – PESANTE, Linda: Introduction to Information Security. Carnegie Mellon University, 2008

NB7 – SPANIOL, O.: Sicherheit in Kommunikationsnetzen. Skript zur Vorlesung an der RWTH Aachen, korrigierte erste Fassung, 14. Juli 2000, Kapitel 5: Authentifizierungssysteme

In der mündlichen Verhandlung hat die Beklagte noch zwei Schaubilder („Handouts“) eingereicht:

– „Vorläufiges Verständnis des Senats der **NK6**“
– „**NK16**: Keine untrennbare Verbindung zwischen Ressourcen und Access Control Lists“

Wegen der weiteren Einzelheiten wird auf den Akteninhalt verwiesen.

E n t s c h e i d u n g s g r ü n d e

Die Klage, mit der u. a. der Nichtigkeitsgrund der fehlenden Patentfähigkeit (Artikel II § 6 Absatz 1 Nr. 1 IntPatÜG, Artikel 138 Abs. 1 lit. a) EPÜ i. V. m. Artikel 54 Absatz 1, 2 und Artikel 56 EPÜ) geltend gemacht wird, ist zulässig.

Sie ist auch begründet. Das Streitpatent hat weder in der erteilten Fassung nach Hauptantrag noch in der Fassung eines der Hilfsanträge 1 bis 6 Bestand, da ihm in jeder dieser Fassungen der Nichtigkeitsgrund der fehlenden Patentfähigkeit entgegensteht. Es bedarf daher keiner abschließenden Entscheidung, ob den Ansprüchen des Streitpatents in der Fassung der Hilfsanträge auch die geltend gemachten Nichtigkeitsgründe der unzulässigen Erweiterung oder der fehlenden Ausführbarkeit entgegenstehen.

I.

Das Streitpatent ist in der erteilten Fassung (Hauptantrag) nicht patentfähig, da die mit den unabhängigen Patentansprüchen 1 und 5 beanspruchte Lehre sich für den Fachmann in naheliegender Weise aus dem Stand der Technik ergab (Artikel II § 6 Absatz 1 Nr. 1 IntPatÜG, Artikel 138 Abs. 1 lit a) EPÜ i. V. m. Artikel 56 EPÜ).

1. Das Streitpatent betrifft den Schutz von Daten in Unternehmensumgebungen und insbesondere ein System und ein Verfahren zur Bereitstellung eines um-

fassenden Zugriffsschutzes für digitale Inhalte in einem verteilten Unternehmensnetzwerk (siehe Streitpatentschrift Abs. [0001], [0014], [0017]).

Hierzu war es beispielsweise vorbekannt, in einem verteilten System mit einem zentralen Speicher für medizinische Datensätze einen zentralen Server vorzusehen, der für die gesamte Zugriffssteuerung bzw. -kontrolle zuständig war (siehe Absatz [0006]), oder die Zugriffssteuerung auf mehrere Server zu verteilen (siehe Absatz [0007] u. a.).

Als **Aufgabenstellung** des Streitpatents ist in Absatz [0024] angegeben, einen generischen Sicherungsmechanismus bereitzustellen, der geschützte „digitale Werte“ (‘digital assets‘, siehe Abs. [0031]) unter allen Umständen schützen kann. Insbesondere soll es durch das beanspruchte System und Verfahren möglich werden, die geschützten Werte (in Form von Dateien) auch dann noch abrufen zu können, wenn ein zentraler Sicherheits-Server nicht in Betrieb oder nicht erreichbar ist (siehe z. B. Absatz [0019]).

2. Der Patentanspruch 1 in der erteilten Fassung (in der Verfahrenssprache Englisch, mit der Merkmalsgliederung der Klägerin gemäß Anlage **NK5**) ist oben im Tatbestand aufgeführt.

Eine vom Senat bereinigte deutsche Übersetzung lautet:

M1 **1.** Verteiltes Zugangskontrollsystem, das dafür ausgelegt ist, den Zugang eines Benutzers zu geschützten Elementen zu beschränken, wobei das System Folgendes umfasst:

M1.1 einen zentralen Server (500) mit einem Servermodul (502), das dafür ausgelegt ist, eine Zugangskontrolle für das gesamte System bereitzustellen;

M1.1.1 wobei die durch den zentralen Server (500) durchgeführte Zugangskontrolle dafür ausgelegt ist zu wirken, um eine Zugangsanforderung des Be-

nutzers zu den geschützten Elementen zu gestatten oder zu verweigern entsprechend
– dem anfordernden Benutzer gewährten Zugangsberechtigungen, und
– Zugangsbedingungen (229) in den gesicherten Elementen;

gekennzeichnet durch

M1.2 mehrere mit dem zentralen Server (500) gekoppelte lokale Server (570), wobei jeder der lokalen Server (570) ein lokales Modul (572) umfasst, das dafür ausgelegt ist, lokale Zugangskontrolle für eine Gruppe von designierten Benutzern bereitzustellen;

M1.2.1 wobei die Zugangsanforderung des Benutzers durch einen oder mehrere der lokalen Server (570) auf verteilte Weise verarbeitet wird; und

M1.2.2 wobei, wenn die Zugangsanforderung in dem lokalen Server (570) verarbeitet wird, dem anfordernden Benutzer Zugang zu den geschützten Elementen gewährt wird, ohne auf den zentralen Server (500) zugreifen zu müssen, wenn die Zugangsberechtigungen des anfordernden Benutzers die Zugangsbedingungen (229) in den gesicherten Elementen erfüllen.

3. Zum nebengeordneten Verfahrensanspruch 5, dessen Patentfähigkeit auch nach Ansicht der Parteien nicht anders als der Patentanspruch 1 zu beurteilen ist, wird auf die Streitpatentschrift sowie auf Anlage **NK5** verwiesen.

4. Einige Begriffe des Patentanspruchs 1 bedürfen einer Auslegung, wobei von der Verfahrenssprache Englisch ausgegangen wird.

4.1 distributed access control (verteilte Zugangskontrolle)
Der Begriff bezieht sich auf die Zugriffssteuerung bzw. -kontrolle in einem verteilten Rechnersystem, wie es beispielsweise Figur 1B des Streitpatents zeigt: Es gibt demnach (einige) lokale Server 104, die ggf. auch räumlich an unterschiedlichen

Orten stehen können, welche über ein Netzwerk 108 untereinander und mit einem zentralen Server 106 verbunden sind. Sie sind jeweils für (mehrere) Einzelcomputer 102 – aus Sicht des Systems: Client-Rechner – zuständig (vgl. Abs. [0051] / [0052]). Dabei macht das Adjektiv ‘distributed‘ deutlich, dass die Zugriffssteuerung nicht allein von dem zentralen Server abhängt, sondern zum Teil auch lokal erfolgt bzw. erfolgen kann (vgl. Abs. [0019]).

4.2 secured items (geschützte Elemente)

Der Ausdruck kommt im Streitpatent (außer in den Patentansprüchen) nicht vor. Der Begriff ‘item‘ ist in den Absätzen [0011] und [0083] kurz erwähnt, dort in Verbindung mit dem in der übrigen Beschreibung häufiger verwendeten Ausdruck ‘secured document‘ (vgl. Abs. [0018], [0021] bis [0023] u. a.). Absatz [0024] nimmt in diesem Zusammenhang Bezug auf ‘secured digital assets‘ – siehe dazu noch Abs. [0031] / [0033].

Die Definition in Absatz [0031] beschreibt die beanspruchten ‘items‘ am besten. Demnach handelt es sich um digitale Daten in beliebiger Form – jede Art von digitalen Objekten, wie zum Beispiel Dateien für Dokumente, Multimedia, ausführbaren Code, Bilder und Texte, aber auch Streaming-Daten, dynamische oder statische Daten. Diese sollen durch das beanspruchte Verfahren „geschützt“ werden im Sinne von Abs. [0033], dass der Zugriff auf sie nur durch Erfüllen der Schutzbedingungen möglich ist.

In den nachfolgenden Ausführungen werden die geschützten Elemente meist als „Dateien“ bezeichnet. Dies darf jedoch gegenüber den genannten Streaming-Daten, dynamischen oder statischen Daten nicht beschränkend verstanden werden.

4.3 access privileges (Zugangsberechtigungen)

Der Ausdruck bezeichnet Berechtigungen eines Benutzers in Bezug auf geschützte Dateien, so wie sie etwa in den Tabellen der Figuren 5B.1 und 5D i. V. m.

Abs. [0128] zum Ausdruck kommen – speziell, was der Benutzer mit Dateien tun darf (nur lesen, ändern, drucken, kopieren …), z. B. in Form eines Rechte-Levels, und erlaubte Zugriffszeiten, Zugriffsorte usw. (vgl. Abs. [0037]).

4.4 access rules (Zugangsbedingungen)

Der Ausdruck bezeichnet Bedingungen, welche einer geschützten Datei zugeordnet sind und erfüllt werden müssen, damit Zugriff auf die Datei genommen werden darf (siehe Abs. [0038]). Beispiele für solche Zugangsbedingungen sind in Figur 2A (204) i. V. m. Abs. [0059] (‘…determine or regulate who and/or how the document 200, once secured, can be accessed. In some cases … also determine or regulate when or where the document 200 can be accessed‘) und in den Abs. [0068] / [0069] dargestellt. Die Bedingungen sollen anspruchsgemäß „in“ der geschützten Datei enthalten sein (Abs. [0059]: z. B. ‘included in the header 206‘).

4.5 Vergleich der ‘access privileges‘ und ‘access rules‘

Beim Vergleich der ‘access privileges‘ und ‘access rules‘ zeigt sich, dass sich die „Berechtigungen“ und die „Bedingungen“ auf identische Gegebenheiten beziehen können, vgl. etwa die Berechtigungen betreffend den User Dell und bestimmte Uhrzeiten (Abs. [0128] Seite 19 oben) mit den Bedingungen betreffend bestimmte Benutzer und Uhrzeiten (Abs. [0069]). Als Unterscheidungskriterium wird verstanden, dass die Berechtigungen (privileges) den Benutzern (oder Benutzergruppen) zugeordnet sind, während die Bedingungen (rules) den Dateien bzw. Daten zugeordnet sind.

4.6 central server / local server – Frage der räumlichen Trennung

Im Hinblick auf die Patentfähigkeit kommt der Frage, ob der zentrale Server und die lokalen Server „räumlich getrennt voneinander“ angeordnet sind, keine Bedeutung zu. Denn dem Fachmann war die Alternative eines „virtuellen Servers“, der sich physikalisch in einem beliebigen Rechner befinden kann, geläufig und lag

für ihn in jedem Fall, d. h. in Verbindung mit jeder der Entgegenhaltungen nahe (was auch durch das Privatgutachten **NK13** indirekt bestätigt wird).

5. Damit ergibt sich als technische Lehre des erteilten Patentanspruchs 1 ein (verteiltes) Zugangskontrollsystem für den Zugriff von Benutzern auf geschützte Daten, insbesondere Dateien (**M1**), welches zunächst auf einem zentralen Server 500 beruht, der für das gesamte System die Zugangskontrolle „bereitstellt", d. h. sämtliche Benutzerrechte und Zugangsbedingungen verwalten und eine Zugriffsanforderung prüfen kann; all dies erfolgt durch ein Servermodul 502 (**M1.1**).

Der Zugriffsschutz besteht darin, dass „in" den geschützten Dateien Zugangsbedingungen enthalten sind, und den System-Benutzern Zugangsberechtigungen zugeordnet sind (für deren Art, Umfang und Speicherort der Patentanspruch keine Festlegung trifft). Der Zentralserver gestattet oder verweigert den Zugriff eines Benutzers auf eine bestimmte geschützte Datei abhängig davon, ob die Zugangsbedingungen der Datei durch die Zugangsberechtigungen des Benutzers erfüllt werden (**M1.1.1**).

Darüber hinaus sind mit dem Zentralserver gekoppelte Lokalserver 570 vorgesehen, die mittels eines lokalen Moduls 572 jeweils eine lokale Zugangskontrolle für eine Gruppe (Untermenge) von Benutzern vornehmen (**M1.2**). Die Zugangsanforderung eines Benutzers wird durch einen oder mehrere der Lokalserver bearbeitet, und zwar als „verteilte" Zugangskontrolle ('in an distributed manner') (**M1.2.1**).

Demgemäß wird einem anfordernden Benutzer durch den Lokalserver 570 Zugang zu den geschützten Dateien gewährt, wenn seine Berechtigungen mit den Bedingungen in den geschützten Dateien übereinstimmen, „ohne auf den zentralen Server (500) zugreifen zu müssen".

Die Beschreibung gibt Beispiele an, wie diese Forderung realisiert werden kann: nämlich indem das lokale Modul 572 eine Kopie oder eine Teilmenge („subset") des Servermoduls 502 sein soll (Abs. [0111], [0127] / [0128]; Unteranspruch 3).

Dass die geschützten Dateien verschlüsselt sein sollen, und der Zugriff eines Benutzers durch den Zugriff auf die jeweilige Schlüsseldatei erfolgt, mit der die geschützte Datei entschlüsselt werden kann (Abs. [0021]), ist nicht Gegenstand des Hauptanspruchs.

6. Als **Fachmann**, der mit der Aufgabe betraut wird, einen verbesserten Sicherungsmechanismus für Daten bzw. Dateien in einem verteilten Unternehmensnetzwerk bereitzustellen, der auch dann noch wirkt, wenn ein zentraler Sicherheitsserver nicht in Betrieb oder nicht erreichbar ist, ist ein Informatiker oder Netzwerktechniker mit Hochschul- oder Fachhochschulabschluss und mehrjähriger Berufserfahrung im Bereich verteilter IT-Systemarchitektur und der Erstellung von IT-Sicherheitskonzepten anzusehen.

7. Der Gegenstand des erteilten Patentanspruchs 1 ergab sich bereits vor dem frühesten Prioritätstag des Streitpatents (12. Dezember 2001) in naheliegender Weise aus dem Stand der Technik.

7.1 Als nächstkommenden Stand der Technik sieht der Senat die Druckschrift **NK6** (US 5 495 533 A) an. Für einen Vergleich mit der Lehre des Patentanspruchs 1 des Streitpatents ist von dem „erweiterten Verfahren“ (‘enhanced method‘) gemäß **NK6** Spalte 8 Zeile 46 ff. auszugehen, in Verbindung mit einem gemeinsamen Authentifizierungs- und Personal Key Server (Figur 6: 66, Figur 7: 75).

Die Druckschrift **NK6** schlägt einen Zugangsschutz für beliebige Dateien vor (Spalte 6 Zeile 11: files or databases … stored on servers 2 … or on user computers 16), der auf einer Verschlüsselung der jeweiligen Datei mit einem ‘file encryption key‘ beruht. Dieser ‘file encryption key‘ wird mit einem weiteren Schlüssel (‘control key‘) verschlüsselt und zusammen mit einer Zugangsliste derjenigen Nutzer, denen ein Zugriff auf die Datei erlaubt ist, und der Index-Nummer des ‘control key‘ im Header der Datei (siehe Figur 8) abgespeichert (außerdem ein mit demselben „control key“ verschlüsseltes ‘message authentication check field‘, das eine

Modifikation des Headers verhindern soll). Die ‘control keys‘ sind auf einem zentralen Server 66, 75 hinterlegt.

Um Zugriff auf eine geschützte Datei (= ‘secured item‘ – Merkmal **M1** ohne ‘distributed‘) erhalten zu können, muss sich der Benutzer vorab beim zentralen Server 66, 75 authentisieren (‘user authentication‘ Spalte 2 Zeile 61 ff., insbes. „Kerberos“ Spalte 3 Z. 10 ff.): er meldet sich mit seiner User-ID und seinem Passwort dort an und erhält, falls erfolgreich, ein „Ticket“ zurück, welches ihn zukünftig im Netzwerk identifiziert. Der zentrale Server 66, 75 führt insoweit die Zugangskontrolle durch (Teil der ‘overall access control‘, Merkmal **M1.1**).

Wenn nun der so authentifizierte Benutzer auf eine geschützte Datei zugreifen will, werden gemäß Spalte 9 Zeile 42 ff. der Datei-Header und das Authentisierungs-Ticket des Benutzers vom Client des Benutzers an den zentralen Server 66, 75 gesendet. Der zentrale Server holt anhand der Index-Nummer im Header den ‘control key‘ aus seinem Speicher und überprüft das ‘message authentication check field‘. Wenn die Prüfung positiv ausfällt, d. h. wenn der Header nicht manipuliert wurde, vergleicht der zentrale Server das Benutzer-Ticket mit der Zugangsliste des Headers. (Nur) wenn der durch das Ticket authentifizierte Benutzer in der Zugangsliste gefunden wird, entschlüsselt der zentrale Server anhand seines ‘control key‘ den ‘file encryption key‘ und sendet ihn an den Client des Benutzers zurück, welcher die Datei damit entschlüsseln kann, wodurch der Zugriff auf die Datei gewährt wird.

Sonach wird hier durch den zentralen Server (zweiter Teil von Merkmal **M1.1**) eine Zugangskontrolle durchgeführt basierend auf dem Authentisierungs-Ticket des Benutzers und den Zugangsbedingungen in den gesicherten Elementen (Zugangsliste). Dabei ist in der **NK6** eine differenzierte Festlegung unterschiedlicher Benutzerberechtigungen (‘access privileges‘) zwar nicht unmittelbar beschrieben. Dennoch wird deutlich, dass der Benutzer durch sein Ticket hier „alle“ Berechtigungen für einen Zugriff erhält, vgl. etwa **NK6** Spalte 9 Z. 42 ‘when a file is acessed (both for *reading* and for *updates*)‘. Das Ticket verleiht somit eine „all-

gemeine", unspezifische (nicht differenzierte) Autorisierung = 'one or more rights a user may have with respect to a secured file or secured document' (Streitpatent Absatz [0037]), womit das Merkmal **M1.1.1** in einer allgemeinen, unspezifischen Form erfüllt ist.

Darüber hinaus entnimmt der Fachmann der **NK6** die Lehre, den „zentralen Server" des Systems auf lokale Rechner zu replizieren. So gibt etwa Spalte 6 Zeile 46 bis 49 den Hinweis: 'If required by an installation, the Personal Key Server may be replicated on multiple computers, using the techniques described in reference 4, in order to improve operational reliability'. Hier wird also vorgeschlagen, aus Gründen der Zuverlässigkeit (Ausfallsicherheit) die Funktion des zentralen Servers auf mehrere Computer zu replizieren; d. h. die Zugangskontrolle soll auf andere Server „ausgelagert" werden, wobei diese jeder für sich in einem „verteilten System" die vollständige Zugangskontrolle abwickeln könnten. Diese „mehreren Computer" entsprechen den lokalen Servern des Merkmals **M1.2**, welche damit eine „lokale Zugangskontrolle" bereitstellen. Dass dies „für einer Gruppe von designierten Benutzern" geschieht, ergänzt der Fachmann aufgrund seines Wissens über größere Firmennetzwerke ganz automatisch (vgl. – rein beispielhaft – **NK12** Figur 1 und zugeh. Beschreibung, oder **NK15** Seite 604 letzter Absatz '…multiple Kerberos servers …each responsible for a subset of users and servers').

Die Merkmale **M1.2.1** und **M1.2.2** (sowie das 'distributed' des Merkmals **M1**) leiten sich aus der Maßnahme einer Replikation des Zentralmoduls automatisch und zwangsläufig ab. Hier ist ebenfalls einzuräumen, dass beim Vorgehen gemäß **NK6** keine differenzierte Prüfung von 'access privileges' stattfindet. Wenn man aber davon ausgeht, dass in einem System ohne dezidierte Berechtigungszuweisungen der Benutzer grundsätzlich „alle" benutzerbezogenen Berechtigungen besitzt, ist das Teilmerkmal 'when the access privileges of the requesting user are permitted by the access rules in the secured items' bereits durch die Bedingung, dass der anfragende Benutzer in der Liste der berechtigten Benutzer im Header einer Datei eingetragen sein muss, erfüllt.

Zusammenfassend ergeben sich sonach alle Merkmale des erteilten Patentanspruchs 1 für den Fachmann, unter Einbeziehung seines Fachwissens (hier insbesondere über verteilte Firmen-Netzwerke), aus der Druckschrift **NK6**.

7.2 Die gegen eine solche Beurteilung gerichtete Argumentation der Beklagten hat nicht überzeugt.

7.2.1 Soweit die Beklagte vorträgt, die Ausführungsform der **NK6**, in welcher ein zentraler Server als Kombination von Authentifizierungs-Server und Personal Key Server beschrieben ist (das „erweiterte Verfahren“ gemäß Spalte 6 Zeile 58 ff., Spalte 8 Zeile 46 ff.), gebe nicht die Lehre, diese beide auf andere Computer zu replizieren, sowie Spalte 6 Zeile 46 bis 49 beziehe sich ausdrücklich nur auf den Personal Key Server, greift eine solche Beurteilung zu kurz. Zwar betrifft der Vorschlag einer Replikation in Spalte 6 Zeile 46 bis 49 tatsächlich nur den Personal Key Server. Das liegt aber daran, dass sich der zugrundeliegende Absatz Spalte 6 Zeile 39 bis 49 auf Figur 4 bezieht, welche eine Trennung zwischen Authentifizierungs-Server 34 und Personal Key Server 32 vorsieht. Erst später (Figur 6 / 7) wird ein gemeinsamer Authentifizierungs- und Personal Key Server 66, 75 vorgeschlagen. Der Fachmann wird hier ganz selbstverständlich mitlesen, dass sich der Vorschlag einer Replikation dann auf diesen gemeinsamen Server beziehen lässt.

Unabhängig davon war dem Fachmann das zugrundeliegende Problem der möglichen Blockierung des gesamten Systems bei einem Ausfall des Zentralservers schon lange vertraut, und er kannte die Maßnahme einer Replikation als typische Lösung dafür. Hierzu kann beispielhaft auf den in **NK6** Spalte 4 Zeile 5 zitierten Artikel „Reference 8: Steiner, J.G. et al.: Kerberos … Usenix Conference Proceedings … Februar 1988“ verwiesen werden, der als Anlage **NK6b** vorliegt. Im dortigen Abschnitt 5.3 „Database Replication“ (Seite 197 / 198) werden Vor- und Nachteile einer Replikation der „Kerberos authentication database“ erläutert. Auch in der Druckschrift **NK15** findet sich auf Seite 606 in Absatz 3 der Hinweis: „Kerberos supports replication of the Kerberos server“.

Somit ist festzustellen, dass die Lehre einer Replikation eines „zentralen“ Servers, auch eines Authentifizierungs-Servers wie Kerberos, dem Fachmann für verteilte Datenverarbeitung und Client-Server-Systeme zum Prioritätszeitpunkt vertraut war, und zwar für den offensichtlichen Zweck, eine Zugangskontrolle auch dann zu ermöglichen, wenn der zentrale Server nicht erreichbar sein sollte. Mit einer solchen Replikation und mit seinem Fachwissen über große Firmennetzwerke mit Gruppen von designierten Benutzern gelangte der Fachmann ohne erfinderische Tätigkeit zum Merkmal **M1.2**.

7.2.2 Gemäß dem Verständnis der Beklagten verfolge das Streitpatent einen gegenüber der **NK6** fundamental unterschiedlichen Sicherungsmechanismus: das Streitpatent betreffe ein regelbasiertes Zugangskontrollsystem, wohingegen die Lehre der **NK6** auf einem Archiv zur Verteilung von kryptographischen Schlüsseln beruhe. Hieraus ergäben sich wesentliche Unterschiede.

Nach der Lehre des Streitpatents dienten die Benutzernamen in der Datenbank des zentralen Servers zur Authentifizierung, wohingegen die Zugangsprivilegien (Berechtigungen) und Zugangsregeln (Bedingungen) zur Autorisierung dienten. Die Authentifizierung regele dabei nicht den Zugriff auf die geschützten Elemente, sondern diene nur zur Durchführung einer verifizierten Anmeldung eines Benutzers am Gesamtsystem. Von zentraler Bedeutung für die Lehre des Streitpatents sei die darüber hinausgehende Zweiteilung der für die Autorisierung erforderlichen Daten in Zugangsberechtigungen, welche im zentralen Server hinterlegt und den Benutzern zugeordnet seien, und in Zugangsbedingungen, welche in den geschützten Elementen enthalten seien. Eine solche zweigeteilte Autorisierung sei der **NK6** nicht zu entnehmen.

Hierzu ist festzustellen, dass die Begriffe „Authentisierung“ und „Autorisierung“ im Patentanspruch 1 nicht vorkommen. Auch dass die Zugangsberechtigungen (‘access privileges‘) im Zentralserver gespeichert und dort den Benutzern zugeordnet sein sollten, lässt sich der Formulierung des Patentanspruchs 1 nicht entnehmen. Das Merkmal **M1.1.1** (und ähnlich das Merkmal **M1.2.2**) bezieht sich nur ganz all-

gemein auf ‘access privileges granted to the requesting user‘, ohne weiter festzulegen, wo und wie diese ‘access privileges‘ gespeichert sein sollen. Zwar gibt die Beschreibung des Streitpatents entsprechende Beispiele, insbesondere in Form der Zuordnungstabellen gemäß Figur 5B und Figur 5D (vgl. dazu auch Abs. [0050] / [0051]); Ausführungsbeispiele schränken einen Patentanspruch jedoch nicht ein (BGH GRUR 2007, 309 – *Schussfädentransport*).

Die von der Beklagten vorgenommene Auslegung des Patentanspruchs 1 ist somit als eine „einengende“ Auslegung eines an sich breiter gefassten Patentanspruchs zu verstehen, die gerade im Nichtigkeitsverfahren zur Begründung einer Schutzfähigkeit nicht zulässig ist (BGH GRUR 2004, 47 – *Blasenfreie Gummibahn I*).

Weil der Patentanspruch 1 in der erteilten Fassung keine Vorgabe zum Speicherort und zur Speicherart für die ‘access privileges‘ macht, wird nach dem Verständnis des Senats das ganz allgemein formulierte Teilmerkmal ‘access privileges granted to the requesting user‘ durch implizite, nicht ausdrücklich gespeicherte Berechtigungen, wie sie der Lehre der **NK6** zugrundeliegen, mit erfüllt.

7.2.3 Das vorhergehende Argument ergänzend, verweist die Beklagte auf die Formulierung „privileges“ in den Anspruchsmerkmalen **M1.1.1** und **M1.2.2**. Dem Plural komme hier eine besondere Bedeutung zu – damit werde zum Ausdruck gebracht, dass eine Menge (im mathematischen Sinn) unterschiedlicher Berechtigungen vorgesehen sei, welche mit der Menge von in der Datei gespeicherten Bedingungen verglichen werden müsse. Die Lehre der **NK6** beschränke sich auf die Bedingungen im Header der Datei. Auch könne es eine „unspezifische“ Autorisierung nicht geben, weil eine Autorisierung immer spezifisch sein müsse.

Dem ist entgegenzuhalten, dass dem Fachmann die grundsätzliche Möglichkeit, unterschiedliche Berechtigungen (Plural) vorzusehen, geläufig war (siehe z.B. **NK6** Spalte 9 Zeile 42 „when a file is acessed (both for *reading* and for *updates*)“, **NK6b** Seite 192 rechte Spalte Zeile 7 / 8 „In order to determinate what each user is able to *read* or *modify*“, **NK15** Seite 605 Kapitel 11.5 „Access Control“, insbes.

Abschnitt 1 „possible operations may be Read, Write and Execute“; **NK9** Absatz [0008], u. a.). Wenn ein Zugangsschutzsystem wie das in der **NK6** erläuterte keine unterschiedlichen Benutzerberechtigungen beschreibt, wird der Fachmann erwarten, dass ein angemeldeter Benutzer mit seiner Authentifizierung implizit „jede mögliche“ Berechtigung, also „alle Berechtigungen“ erhält. Dies rechtfertigt die vom Senat gesehene Übereinstimmung mit der Plural-Formulierung „Berechtigungen“, auch ohne dass gleich eine Verwaltung unterschiedlicher Berechtigungen vorgesehen sein müsste – **NK6** beschreibt eine Zugangskontrolle, um eine Zugangsanforderung des Benutzers zu den geschützten Elementen zu gestatten oder zu verweigern ‘in accordance with access privileges granted to the requesting user‘ – also in Übereinstimmung mit allen (denkbaren, möglichen) Berechtigungen, die der Benutzer allein durch sein Authentifizierungs-Ticket erhält – ‘and access rules in the secured items‘ (**NK6** Spalte 9 Zeile 50 bis 53: ‘… compares the accessor's name (from the ticket) against … the names in the access control list‘, wobei die ‘access control list‘ gemäß Figur 8 und Spalte 8 Zeile 46 ff. im Header der geschützten Datei enthalten sein kann).

In diesem Sinne besteht die Möglichkeit einer unspezifischen Autorisierung, wenn ein Benutzer allein mit seiner Anmeldung „alle möglichen“ Autorisierungen erhält, so wie es in den Anfangsjahren der Datenverarbeitung und insbesondere bei Einzelplatzsystemen häufig der Fall war.

8. Mit dem Patentanspruch 1 fällt der nebengeordnete Patentanspruch 5, der nicht anders als der Patentanspruch 1 zu beurteilen ist (s. o. Abschnitt **3.**); damit fällt auch der gesamte Hauptantrag – in Übereinstimmung mit der Erklärung der Beklagten, die einzelnen Anträge stellten geschlossene Anspruchssätze dar, die jeweils in ihrer Gesamtheit beansprucht würden.

II.

Die sechs Hilfsanträge sind nicht günstiger zu beurteilen. Auch bei Berücksichtigung der jeweils hinzugenommenen Merkmale muss festgestellt werden, dass die damit beanspruchte Lehre für den Fachmann nahelag (Artikel II § 6 Absatz 1 Nr. 1 IntPatÜG, Artikel 138 Abs. 1 lit a EPÜ i. V. m. Artikel 56 EPÜ).

1. Der Hilfsantrag 1 hat keinen Erfolg, weil sich das zusätzliche Merkmal seines Patentanspruchs 1 ebenfalls aus der Druckschrift **NK6** ergibt und im Übrigen für den Fachmann keine Besonderheit darstellte.

1.1 Beim Hilfsantrag 1 wird das Merkmal **M1** des Patentanspruchs 1 des Hauptantrags folgendermaßen ergänzt:

H1-M1 A distributed access control system adapted to restrict access of a user to secured items **including executable code**, said system comprising:

D.h. es sollen (nur noch) solche Dateien durch die beanspruchte Lehre geschützt werden, die einen ausführbaren Code beinhalten.

1.2 Die Beklagte trägt hierzu vor, die Erfinder hätten erkannt, dass die streitpatentgemäß verteilte Autorisierung anhand von Zugangsberechtigungen und Zugangsbedingungen im geschützten Element gerade bei ausführbarem Code technisch besonders vorteilhaft sei. Gerade Dateien mit ausführbarem Code bedürften in Computernetzwerken eines besonderen Zugriffsschutzes, z. B. im Hinblick auf schädlichen Programmcode (wie z. B. Viren); sie dürften nur von berechtigten Personen (z. B. Systemadministrator) ausgeführt werden können.

Die **NK6** beschäftige sich hingegen ausschließlich mit einem Zugangsschutz für Datendateien („data files“, vgl. **NK6**, Spalte 4, Zeilen 61-64). Insbesondere basiere das Grundprinzip der **NK6** darauf, Datendateien kryptografisch zu verschlüsseln

und nur auf eine Zugangsanfrage hin zu entschlüsseln. Ein solches Vorgehen mache jedoch bei ausführbaren Programmen, welche typischerweise um Größenordnungen mehr Datenvolumen umfassten, für den Fachmann aus Effizienzgründen keinen Sinn, weshalb der Fachmann die **NK6** schon nicht heranziehen würde.

1.3 Dem kann nicht gefolgt werden.

Zunächst wird der Fachmann die Lehre der **NK6** keinesfalls als auf Daten-Dateien beschränkt verstehen (vgl. **NK6** Spalte 6 Zeile 11: files or databases … stored on servers 2 … or on user computers 16). Aber selbst wenn man von einer derartigen Beschränkung ausginge, hätte der Fachmann kein Problem, die Lehre auf Programm-Dateien zu übertragen; ob der Aufwand für die Verschlüsselung die dadurch ggf. verringerte Effizienz rechtfertigt oder nicht, wäre lediglich als fachmännisches Abwägen von bekannten Vor- und Nachteilen zu beurteilen (es gab im Übrigen schon immer auch „kleine“ Programm-Dateien und „große“ Daten-Dateien, wie etwa Videodateien).

Unabhängig davon ist noch darauf zu verweisen, dass auch Daten-Dateien, wie sie der **NK6** fraglos entnehmbar sind, ausführbaren Code enthalten können (so z. B. Microsoft-Office-Dokumente mit Makros in Visual-Basic-Code).

Und schließlich ist auch nicht nachvollziehbar, dass die Erfinder den besonderen Vorteil des streitpatentgemäßen Verfahrens für ausführbaren Code erkannt hätten. „Executable code“ ist überhaupt nur in den Absätzen [0017] und [0031] des Streitpatents erwähnt, und zwar an beiden Fundstellen in einer Aufzählung als eine beliebige von mehreren Möglichkeiten. Dass die Lehre des Streitpatents gerade für Dateien mit ausführbarem Code einen besonderen Vorteil böte, lässt sich dem Streitpatent nirgends entnehmen. Zwar wird die Rechtsprechung des Bundesgerichtshofs dahingehend verstanden, dass es zulässig ist, Vorteile einer Erfindung zur Begründung der erfinderischen Tätigkeit nachzubringen (vgl. etwa Schulte, PatG, 10. Auflage (2017), § 4 Rn. 156 m. Nachw.). Dies soll aber ausgeschlossen sein, wenn dadurch – wie hier beim Hilfsantrag 1 – die offenbarte Lehre erst ihren

eigentlichen Sinn erhalten würde (Schulte, a. a. O. unter Bezug u. a. auf BGH GRUR 1960, 542 – *Flugzeugbetankung*: „Soll nach der Verteidigung des Patentinhabers im Nichtigkeitsverfahren ein von ihm behaupteter Vorteil das eigentliche Wesen der Erfindung ausmachen und die Ausnutzung des Vorteils der Befolgung der gegebenen Lehre erst ihren eigentlichen Sinn geben, so muss dieser Vorteil, wenn er patentbegründend sein soll, in der Patentschrift offenbart sein“).

Die vorgenommene Ergänzung mag daher als Einschränkung auf eine von mehreren der in Abs. [0017] oder [0031] genannten Möglichkeiten zwar zulässig sein; das Vorliegen einer erfinderischen Tätigkeit kann damit aber nicht begründet werden.

1.4 Mit dem Patentanspruch 1 fällt der gesamte Hilfsantrag 1 (vgl. oben **I. 8.**).

2. Dem Hilfsantrag 2 kann nicht gefolgt werden, weil der Gegenstand seines Patentanspruchs 1, ausgehend von der Druckschrift **NK6** und dem Fachwissen des Durchschnittsfachmanns, nicht auf einer erfinderischen Tätigkeit beruht.

2.1 Beim Hilfsantrag 2 werden die Merkmale **M1.1** und **M1.2** des Patentanspruchs 1 des Hauptantrags in folgender Weise ergänzt:

H2-M1.1 a central server (500) having a server module (502) adapted to provide overall access control**, wherein the server module in the central server maintains a database that includes a list of users and corresponding access privileges**;

…

H2-M1.2 a plurality of local servers (570) coupled to the central server (500), each of said local servers (570) including a local module (572) adapted to provide local access control to a group of designated users**, wherein the local module is a copy or a subset of the server module**;

D. h. das Modul im zentralen Server, welches eine Zugangskontrolle für das gesamte System bereitstellt, soll eine Datenbank führen, welche eine Liste von Benutzern und zugehörige Zugangsberechtigungen umfasst; und das lokale Modul, welches eine lokale Zugangskontrolle bereitstellt, soll eine Kopie oder eine Teilmenge des Servermoduls (sinngemäß zu ergänzen: aus dem zentralen Server) sein.

2.2 Die Beklagte erläutert, mit dem ergänzten Merkmal **H2-M1.1** komme nunmehr die wesentliche Idee des Streitpatents deutlich zum Ausdruck, eine zweigeteilte Autorisierung mit Benutzerberechtigungen (‘access privileges‘), welche in einer Tabelle im Zentralserver gespeichert seien, und Zugriffsbedingungen in den geschützten Dateien vorzunehmen. Eine gespeicherte Tabelle mit Benutzerberechtigungen lasse sich der **NK6** nicht entnehmen, es gebe auch keinen Anlass für eine solche zusätzliche Maßnahme.
Erst dadurch lasse sich aber ein durchgehender, vom jeweils verwendeten Dateizugriffssystem unabhängiger Schutz der Dateien gewährleisten, der zudem (mittels der gewährten ‘access privileges‘) flexibel an geänderte Anforderungen anpassbar sei.

2.3 Auch das auf diese Weise eingeschränkt beanspruchte Zugangskontrollsystem war dem Durchschnittsfachmann jedoch nahegelegt.

Als nächstkommender Stand der Technik ist unverändert die Druckschrift **NK6** anzusehen.

Von der ‘enhanced method‘ der **NK6** in Verbindung mit dem dort ebenfalls beschriebenen gemeinsamen Authentication Server und Personal Key Server, wie es oben im Abschnitt **I. 7.1** erläutert wurde, unterscheidet sich die Lehre des Patentanspruchs 1 nach Hilfsantrag 2 i. w. in folgenden zwei Punkten:

a) Nach erfolgreicher Authentisierung erhält der Nutzer bei dem Verfahren der **NK6** vom zentralen Server 66, 75 ein „Ticket“ zurück, welches ihn im Netzwerk

identifiziert. Der zentrale Server führt für diesen Zweck eine Liste von Benutzern und deren Passworten (siehe **NK6** Spalte 3 Zeile 10 bis 12). Von differenzierten Zugangsberechtigungen für die bekannten Benutzer (und einer entsprechenden Datenbank im zentralen Server) ist in der **NK6** jedoch keine Rede.

b) **NK6** beschreibt keine lokalen Server „mit einer zugeordneten Gruppe von designierten Benutzern“ (Merkmal **M1.2**), welche ihre Dienste für eine bestimmte Gruppe von Benutzern bzw. Client-Computern oder für einen bestimmten Ort anbieten. Die **NK6** geht von einem Zentralserver für die Zugangskontrolle aus. Dass solche lokale Server eine lokale Zugangskontrolle durchführen könnten, basierend jeweils auf einer Kopie oder einem Subset des Zugangskontrollmoduls des zentralen Servers, ist der **NK6** nicht explizit entnehmbar.

2.3.1 Zum ersten Punkt: ‘… central server maintains a database that includes a list of users and corresponding access privileges‘

Mit Recht hat die Beklagte geltend gemacht, dass die Lehre der **NK6** nur die Authentifizierung der Systembenutzer verlangt, ihnen aber keine unterschiedlichen Zugangsberechtigungen zuordnet.

Der Fachmann, der mit Sicherungsmechanismen in verteilten Unternehmens-Netzwerken vertraut war (s. o. **I. 6.**), erkannte diesen Teil der Lehre der **NK6** im Jahr der Priorität des Streitpatents (2001) jedoch als veraltet. Schon lange waren Systeme bekannt, welche differenzierte Zugangsberechtigungen für einzelne Nutzer oder für Nutzergruppen anboten, z. B. im Rahmen der verschiedenen UNIX-Distributionen oder auch bei Microsoft® Windows-NT.

Rein beispielhaft hat der Senat hierzu auf die Druckschrift **D2** (US 6 308 274 B1) hingewiesen (wobei es nicht auf die in dieser Druckschrift diskutierte Erfindung ankommt, sondern allein auf die Beschreibung des Zugangsschutzmechanismus von Windows NT in Spalte 4 Zeile 29 bis Spalte 6 Zeile 4, i. V. m. Figur 2 / 3). Ähnliches ist auch der Druckschrift **NK16** entnehmbar.

Das „Security Model“ von Windows NT kennt bereits eine Berücksichtigung von Benutzergruppen mit Zuordnung von Berechtigungen (vgl. **D2** Spalte 4 Zeile 52 bis 58; **NK16** Seite 34, Seite 36). Hier erhält ein Benutzer bei erfolgreicher Anmeldung ein „access token 60“ (**D2** Figur 2), das gewissermaßen eine Weiterbildung des Kerberos-Tickets der **NK6** darstellt. Es umfasst neben der User-SID auch Gruppen-SIDs und Berechtigungen ($Privilege_1$ … $Privilege_m$), und es stammt vom zentralen Sicherheitsmodul (vgl. **NK16** Seite 36 Absatz 2). D. h. es gibt im zentralen Sicherheitsmodul eine (zentrale) Datenbank, welche eine Liste von Benutzern und zugehörige Zugangsprivilegien umfasst (**NK16** Seite 36 Absatz 2: ‘The Security Account Manager compares the user account name and password to the domain’s database of users … also downloads information about the user, such as account privileges…‘ – Merkmal **H2-M1.1**).

Darüber hinaus umfasst das geschützte Objekt 72 (**D2** Figur 3) einen ‘Security Descriptor‘ 76 „in dem geschützten Element“, im Sinne von Merkmal **M1.1.1**.

Wenn der Fachmann die bereits 1994 angemeldete Lehre der **NK6** an aktuelle Weiterentwicklungen (im Jahr 2001) anpassen wollte und das Prinzip der Berücksichtigung von Benutzergruppen, wie es von UNIX oder Windows NT her bekannt war, auf die Lehre der **NK6** anwendete, gelangte er zwangsläufig zu einer zentralen Datenbank, welche eine Liste von Benutzern und zugehörige Zugangsberechtigungen umfasst, wohingegen die Zugangsregeln in den geschützten Elementen gespeichert blieben.

Somit lag die Berücksichtigung von spezifischen Berechtigungen für einzelne Benutzer oder Benutzergruppen im Sinne des obigen „Unterschied **a)**“ für den Fachmann nahe, wenn er die Lehre der Druckschrift **NK6** an inzwischen übliche Sicherheitsmechanismen anpassen wollte.

2.3.2 Zum zweiten Punkt: lokale Server / ‘a copy or a subset of the server module‘

Lokale Server „mit einer zugeordneten Gruppe von designierten Benutzern“, welche ihre Dienste für eine Benutzergruppe oder z. B. für einen bestimmten Standort einer Firma anbieten, waren lange vor dem Zeitrang des Streitpatents aus verteilten Rechnersystemen z. B. mit einem Gateway-Server (**NK12** Figur 1) allgemein bekannt. Allein schon um den Zugang in einem solchen Standortsystem bei einer eventuellen Störung des Zugriffs auf den zentralen Server nicht zu blockieren, hätte der Fachmann die in **NK6** (Spalte 6 Zeile 46 bis 49, vgl. oben Abschnitt **I. 7.2.1**) gefundene Anregung einer Replikation (vgl. auch **NK6b** Abschnitt 5.3, **NK15** Seite 606 Absatz 3) aufgegriffen und etwa die lokalen Gateway-Server eines Standorts mit einer Kopie oder einem Subset des Zugangskontroll-Moduls des zentralen Servers ausgerüstet (vgl. oben **I. 7.1** / **7.2.1**).

Damit ergab sich das als „Unterschied **b)**“ Geschilderte als naheliegende Anwendung der Lehre der Druckschrift **NK6** bei einem über mehrere Standorte verteilten Rechnersystem.

2.3.3 Nachdem die beiden erörterten Unterschiede unabhängig voneinander sind und die beiden für den Fachmann, ausgehend von **NK6** und seinem Fachwissen, naheliegenden Maßnahmen – die Aktualisierung auf den aktuellen Stand der IT-Sicherheitstechnik durch benutzerbezogene Berechtigungen, und die Anwendung auf verteilte Rechnersysteme mit lokalen Servern für Benutzergruppen – sich nicht gegenseitig beeinflussen, so dass kein kombinatorischer Effekt entsteht, beruht der Gegenstand des Patentanspruchs 1 von Hilfsantrag 2 nicht auf einer erfinderischen Tätigkeit.

2.4 Die dagegen gerichteten Argumente der Beklagten führen zu keiner anderen Beurteilung.

2.4.1 Insbesondere hat die Beklagte angeführt, dass der Sicherheitsmechanismus von Windows NT keine Regeln (Bedingungen) „in den geschützten Elementen“ aufweise. Für die geschützten Objekte seien etwa gemäß **D2** Spalte 4 Zeile 66 ff. Sicherheits-Deskriptoren 76 des „Kernel-Levels“ zuständig. Diese Deskriptoren (die gemäß **D2** Figur 3 die beanspruchten ‘rules‘ enthalten können)

seien nicht „in“ dem Objekt gespeichert, sondern diesem nur zugeordnet, in der Art eines Zeigers, der auf einen tatsächlichen Speicherort im Kernel verweist. Auch in **NK16** Seite 34 Zeile 3 / 4 heiße es ‘security descriptor for the file‘, nicht ‘in the file’. Gemäß **NK16** Seite 42 gehöre die ‚access control list‘ für Dateien (files) zum File Manager, nicht zur Datei.

Der Senat sieht darin jedoch kein Hindernis. Entscheidend ist, dass die Lehre der **NK6** eine Speicherung „in“ den geschützten Elementen vorbeschreibt. Zwar geht sie allein von einer einfachen Authentifizierung des Benutzers aus und kennt keine Vergabemöglichkeiten für differenzierte Benutzerberechtigungen; wie ausgeführt, waren differenzierte Benutzerberechtigungen im Jahr des Zeitrangs des Streitpatents jedoch allgemein üblich.
Um die Lehre der **NK6** an den aktuellen „Stand der Technik“ anzupassen, hätte der Fachmann allein diesen Aspekt (Tabelle mit Benutzerberechtigungen) von damals üblichen Betriebssystemen wie UNIX oder Windows NT auf die Lehre der **NK6** übertragen, ohne dabei aber den Ablageort der in **NK6** beschriebenen „Bedingungen“ („access control list“, siehe **NK6** Figur 8) im Header der Datei zu verändern.

Unabhängig davon ist die von der Beklagten beschriebene Lücke im Schutzmechanismus, falls Dateien ohne die zugeordneten Berechtigungen kopiert würden (vgl. das in der mündlichen Verhandlung vorgelegte Handout „NK16: Keine untrennbare Verbindung …“) derart offensichtlich, dass der Fachmann (s. o. **I. 6.**) sie niemals zugelassen hätte. Dabei setzt ein lückenloser Schutz aber nicht voraus, dass die Zugriffsbedingungen physikalisch „in“ der jeweiligen Datei gespeichert sind. Es kommt vielmehr auf eine lückenlose Zuordnung an, vor allem dass sie bei jeder Dateiweitergabe mitgegeben werden. Das ist in einem geschützten Dateisystem aber ohne Weiteres auch dann möglich, wenn eine im Kernel gespeicherte Liste zu der jeweiligen Datei nur zugeordnet ist (z. B. durch einen Pointer).

So auch das Streitpatent, wo es in Abs. [0059] heißt: ‘A set of access rules 204 for the document 200 is received and associated with a header 206 … Depending on

an exact implementation, the security information can be entirely included in a header or pointed to by a pointer that is included in the header.' **NK6** als „Stand der Technik" beschreibt den Header mit den 'rules' ebenfalls so: 'The header may be associated with the file in a number of ways: as the first few bytes of the file, or as a trailer at the end of the file, or stored in the file's directory entry, or in a separate area associated with the file's directory entry, or in a local database.' Von dem den hier zuständigen Fachmann werden die beiden Möglichkeiten (Speicherung unmittelbar in der Datei, oder durch Pointer verknüpft) demnach als **gleichwertig** beurteilt.

2.4.2 Den Anlass, die Lehre der **NK6** entsprechend abzuändern sieht der Senat darin, dass die im Jahr 1994 zum Patent angemeldete Lehre der **NK6**, welche nur eine „einfache" Benutzer-Authentifizierung beinhaltete, im Jahr 2001 (frühester Zeitrang des Streitpatents: 12. Dezember 2001) nicht mehr zeitgemäß war. Denn angesichts zahlreicher damals bekannter verbreiteter Betriebssysteme, welche eine differenzierte Benutzer-Autorisierung vorsahen, hätte der Fachmann die Lehre der **NK6** (wie beschrieben) dem allgemeinen Fortschritt und den Verbesserungen der Technik folgend entsprechend angepasst.

2.5 Der Gegenstand des Patentanspruchs 1 nach Hilfsantrag 2 stellt sich sonach lediglich als naheliegende Aktualisierung der Lehre der **NK6** für aktuelle Betriebssysteme und als fachmännische Anwendung auf ein auf mehrere Standorte oder Benutzergruppen verteiltes Rechnersystem dar.

Mit dem Patentanspruch 1 fällt der gesamte Hilfsantrag 2 (s. o. **I. 8.**).

3. Der Hilfsantrag 3 ist nicht günstiger zu beurteilen.

3.1 Der Patentanspruch 1 des Hilfsantrags 3 beruht auf dem Anspruch 1 des Hilfsantrags 2 mit dessen Merkmalen **H2-M1.1** und **H2-M1.2** (siehe oben **2.1**), wobei das Merkmal **M1.1** zusätzlich ergänzt wird:

H3-M1.1 a central server (500) having a server module (502) adapted to provide overall access control, wherein the server module in the central server maintains a database that includes a list of users and corresponding access privileges**, wherein the access privileges specify membership in one or more user groups**;

D.h. die Benutzerberechtigungen sollen eine Zugehörigkeit zu einer oder zu mehreren Benutzergruppen spezifizieren.

3.2 Die Beklagte trägt dazu vor, das ergänzte Merkmal **H3-M1.1** bringe den Unterschied zur Lehre der Druckschrift **NK6** noch deutlicher zum Ausdruck, denn **NK6** kenne keine Benutzergruppen.

3.3 Es kann dahinstehen, ob dieses Merkmal so wie nun beansprucht auch ursprünglich offenbart ist. Denn wie oben in **II. 2.3.1** ausgeführt, kennt der Fachmann Benutzergruppen und -berechtigungen, die einer Benutzergruppe zugeordnet sind, von bereits vor dem Zeitrang des Streitpatents üblichen Betriebssystemen wie UNIX oder Windows NT, vgl. etwa **D2** Spalte 5 Zeile 18 ff. oder **NK16** Seite 41 '… list of groups to which the user belongs …'. Der Fachmann hätte die hier explizit beanspruchte Spezifizierung in Form der Zugehörigkeit zu einer oder zu mehreren Benutzergruppen bei der „Aktualisierung" der Lehre der Druckschrift **NK6** (vgl. oben **II. 2.3.1, 2.4.2**) automatisch mit übernommen.

Mit der angegebenen Ergänzung des Merkmals **M1.1** kann das Vorliegen einer erfinderischen Tätigkeit gegenüber der Anspruchsfassung gemäß Hilfsantrag 2 daher nicht begründet werden.

4. Auch der Hilfsantrag 4 kann nicht günstiger als die Hilfsanträge 2 und 3 beurteilt werden.

4.1 Der Patentanspruch 1 des Hilfsantrags 4 geht aus von Anspruch 1 gemäß Hilfsantrag 3 mit dessen Merkmalen **H3-M1.1** und **H2-M1.2** (siehe oben **II. 3.1**,

2.1) wobei zwischen den Merkmalen **M1** und **H3-M1.1** noch als zusätzliches Merkmal eingefügt wird:

H4-M1.0 **a user authentication process (600) for authenticating the user before being able to access secured items;**

Damit soll zum Ausdruck gebracht werden, dass der Authentifizierungsprozess dem Zugriff auf die gesicherten Elemente und der zugehörigen Autorisierung ausdrücklich **vorgelagert** ist.

4.2 Die Beklagte trägt hierzu vor, das Kerberos-Ticket der **NK6** sei allenfalls für den nun im Anspruch ausdrücklich erwähnten Authentifizierungsprozess von Bedeutung, nicht aber für die nachfolgende Autorisierung von Zugangsanforderungen anhand von Zugangsprivilegien und Zugangsregeln. Durch das zusätzliche Merkmal sollte die Trennung in zwei Phasen (Authentifizierung / Autorisierung) deutlicher zum Ausdruck gebracht werden.

4.3 In der Beurteilung als „für den Fachmann naheliegend“ ergibt sich dadurch aber kein Unterschied.

Schon die Lehre der **NK6** allein zeigt eine erste, vorgelagerte Phase der Benutzer-Authentifizierung (Spalte 2 Zeile 61 bis Spalte 3 Zeile 16), welche als Ergebnis das Benutzer-Ticket liefert. Mit diesem kann der Benutzer dann in einer zweiten Phase auf geschützte Dateien zugreifen (Spalte 3 Zeile 16 bis 22 u. a.). In dieser Hinsicht geschieht auch bei Windows NT nichts anderes (vgl. **D2** Spalte 4 Zeile 46 ff., Zeile 61 ff.) Daher ist das zusätzliche Merkmal des Hilfsantrags 4 im gegebenen Kontext vorbekannt. Zu den übrigen Merkmalen wird auf die obige Argumentation betreffend die Hilfsanträge 2 und 3 verwiesen.

5. Die Hilfsanträge 5 und 6 haben ebenfalls keinen Erfolg.

5.1 Beim Hilfsantrag 5 wird das Merkmal **M1** des Patentanspruchs 1 des

Hilfsantrags 4 – genauso wie beim Hilfsantrag 1 im Vergleich mit dem Hauptantrag – um den Ausdruck **‘including executable code‘** ergänzt, d. h. hier sollen wieder (nur noch) solche Dateien durch die beanspruchte Lehre geschützt werden, die einen ausführbaren Code beinhalten.

Der Patentanspruch 1 gemäß Hilfsantrag 6 stimmt mit dem Patentanspruch 1 des Hilfsantrags 5 überein mit der einzigen Ausnahme, dass das (im Hilfsantrag 3 hinzugekommene) Teilmerkmal ’wherein the access privileges specify membership in one or more user groups‘ gestrichen ist.

5.2 Für die Beurteilung der Ergänzung im Patentanspruch 1 des Hilfsantrags 5 gilt das zum Hilfsantrag 1 Ausgeführte in gleicher Weise (s. o. **II. 1.3**: „das Vorliegen einer erfinderischen Tätigkeit kann damit nicht begründet werden“).

Der Hilfsantrag 5 kann daher nicht anders als Hilfsantrag 4 beurteilt werden.

5.3 Diese Beurteilung kann sich auch nicht dadurch ändern, dass gemäß Hilfsantrag 6 das Teilmerkmal ’wherein the access privileges specify membership in one or more user groups‘ gestrichen, also nicht mit beansprucht wird.

Der Hilfsantrag 6 kann daher nicht anders als Hilfsantrag 5 beurteilt werden.

6. Da die Hilfsanträge jeweils als geschlossene Anspruchssätze beansprucht werden, fallen mit den jeweiligen Hauptansprüchen auch die jeweiligen Anspruchssätze insgesamt (siehe auch oben unter I. Ziff. 8).

III.

Die Kostenentscheidung beruht auf § 84 Abs. 2 PatG i. V. m. §§ 91 Abs. 1 Satz 1 ZPO.

Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus § 99 Abs. 1 PatG i. V. m. § 709 Satz 1 und 2 ZPO.

IV.

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

Gegen dieses Urteil ist das Rechtsmittel der Berufung gemäß § 110 PatG gegeben.

Die Berufungsfrist beträgt einen Monat. Sie beginnt mit der Zustellung des in vollständiger Form abgefassten Urteils, spätestens aber mit dem Ablauf von fünf Monaten nach Verkündung. Die Berufung ist durch einen in der Bundesrepublik Deutschland zugelassenen Rechtsanwalt oder Patentanwalt schriftlich beim Bundesgerichtshof, Herrenstraße 45a, 76133 Karlsruhe, einzulegen.

Die Berufungsschrift muss

- die Bezeichnung des Urteils, gegen das die Berufung gerichtet ist, sowie
- die Erklärung, dass gegen dieses Urteil Berufung eingelegt werde,

enthalten. Mit der Berufungsschrift soll eine Ausfertigung oder beglaubigte Abschrift des angefochtenen Urteils vorgelegt werden.

Guth Hartlieb Baumgardt Dr. Forkel Hoffmann

prö