BUNDESPATENTGERICHT

IM NAMEN DES VOLKES

URTEIL

Verkündet am
22. Januar 2024
…

5 Ni 45/20 (EP)

(Aktenzeichen)

In der Patentnichtigkeitssache

…

ECLI:DE:BPatG:2024:220124U5Ni45.20EP.0

betreffend das europäische Patent EP 1 579 621
(DE 603 46 535.8)

hat der 5. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf Grund der mündlichen Verhandlung vom 22. Januar 2024 durch die Vorsitzende Richterin Dr. Schnurr sowie die Richter Heimen, Dipl.-Phys. Univ. Bieringer, Dr.-Ing. Ball und Dipl.-Phys. Christoph

für Recht erkannt:

I. Die Klage wird abgewiesen.

II. Die Klägerin trägt die Kosten des Rechtsstreits.

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

Tatbestand

Die Beklagte war Inhaberin des mittlerweile durch Ablauf der Schutzdauer erloschenen europäischen Patents EP 1 579 621 (Streitpatent), das – unter Inanspruchnahme der Priorität der US 306494 vom 27. November 2002 – am 12. November 2003 angemeldet wurde. Die Erteilung des europäischen Patents wurde am 23. Juli 2014 veröffentlicht. Das in englischer Sprache gefasste Streitpatent trägt die Bezeichnung “DOMAIN-BASED DIGITAL-RIGHTS MANAGEMENT SYSTEM WITH EASY AND SECURE DEVICE ENROLLMENT“,

übersetzt „DOMÄNENGESTÜTZTES VERWALTUNGSSYSTEM FÜR DIGITALE RECHTE MIT LEICHTER UND SICHERER EINRICHTUNGSREGISTRATION”. Es umfasst in der zuletzt geltenden Fassung insgesamt 13 Patentansprüche, und zwar den Verfahrensanspruch 1 und die auf diesen unmittelbar oder mittelbar rückbezogenen Unteransprüche 2 bis 8, sowie den nebengeordneten Vorrichtungsanspruch 9 und die auf diesen rückbezogenen Unteransprüche 10 bis 13.

Zwischen den Parteien ist ein Verletzungsrechtsstreit anhängig.

Die erteilten unabhängigen Patentansprüche 1 und 9 lauten in der Verfahrenssprache Englisch bzw. in deutscher Übersetzung gemäß der Streitpatentschrift wie folgt:

	Verfahrenssprache	Übersetzung
1.	A method for registering a new device as part of a domain of devices, which share rights associated with a common account, for use in accessing protected digital content within a digital-rights management system, the method comprising the steps of:	Verfahren zur Eintragung einer neuen Vorrichtung als Teil einer Domain aus Vorrichtungen, die Rechte in Zusammenhang mit einem gemeinsamen Konto teilen, zur Verwendung bei Zugriff auf geschützten digitalen Inhalt innerhalb eines Verwaltungssystems für digitale Rechte, wobei das Verfahren die folgenden Schritte aufweist:
	receiving, over a short range link, domain information corresponding to the domain of devices from a device existing within the domain of devices;	Empfangen, über eine Kurzstrecken-Verbindung, von Domain-Informationen, die der Vorrichtungsdomain entsprechen, von einer Vorrichtung die innerhalb der Vorrichtungsdomain besteht;
	providing the domain information to a key issuer, which is separate from the domain of devices, causing the key issuer to issue a private key to the new device,	Bereitstellen der Domain-Informationen für einen Schlüsselaussteller, der unabhängig von der Vorrichtungsdomain ist, wodurch der Schlüsselaussteller einen privaten Schlüssel für die neue Vorrichtung ausstellt,

wherein the private key is based on the domain information and is utilized by all devices within the domain of devices; and	wobei der private Schlüssel auf den Domain-Informationen basiert und von allen Vorrichtungen innerhalb der Vorrichtungsdomain verwendet wird; und
receiving the private key from the key issuer for use in accessing the protected digital content within the digital rights management system.	Empfangen des privaten Schlüssels vom Schlüsselaussteller zur Verwendung bei Zugriff auf den geschützten digitalen Inhalt innerhalb des Verwaltungssystems für digitale Rechte.

9.	An apparatus comprising: communication circuitry for receiving, over a short range link, domain information from a device existing within a domain of devices, which share rights associated with a common account, for use in accessing protected digital content within a digital rights management system;	Gerät, das Folgendes aufweist: einen Kommunikationskreis zum Empfangen, über eine Kurzstrecken-Verbindung, von Domain-Informationen von einer Vorrichtung, die innerhalb einer Domain aus Vorrichtungen besteht, die Rechte in Zusammenhang mit einem gemeinsamen Konto teilen, zur Verwendung bei Zugriff auf geschützten digitalen Inhalt innerhalb eines Verwaltungssystems für digitale Rechte;
	storage for storing the domain information; and logic circuitry for providing the domain information to a key issuer which is separate from the domain of devices, causing the key issuer to issue a private key for use in accessing protected digital content to the apparatus,	einen Speicher zum Speichern der Domain-Informationen; und einen Logikkreis zur Bereitstellung der Domain-Informationen für einen Schlüsselaussteller, der unabhängig von der Vorrichtungsdomain ist, wodurch der Schlüsselaussteller einen privaten Schlüssel zur Verwendung bei Zugriff auf geschützten digitalen Inhalt für das Gerät ausstellt,
	wherein the private key is based on the domain information and is utilized by all devices within the domain of devices.	wobei der private Schlüssel auf den Domain-Informationen basiert und von allen Vorrichtungen innerhalb der Vorrichtungsdomain verwendet wird.

Wegen des Wortlauts der unmittelbar oder mittelbar auf den Anspruch 1 rückbezogenen Ansprüche 2 bis 8 und der auf Anspruch 9 rückbezogenen Ansprüche 10 bis 13 wird auf die Streitpatentschrift EP 1 579 621 B1 verwiesen.

Die Klägerin macht die Nichtigkeitsgründe der fehlenden Patentfähigkeit, nämlich mangelnde Neuheit und mangelnde erfinderische Tätigkeit, sowie der unzulässigen Erweiterung geltend (Art. II § 6 Abs. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 Buchst. a), c) i. V. m. Art. 54, 56, 123 EPÜ).

Sie stützt ihren Vortrag u. a. auf die nachfolgenden Unterlagen und Druckschriften:

NK3 WO 2004/051916 A1 – Offenlegungsschrift zum Streitpatent,

NK4 Prioritätsdokument der Voranmeldung US 10/306,494 vom 27. November 2002,

D1 US 2002 / 0 166 047 A1,

D2 US 2002 / 0 157 002 A1,

D3 GB 2 367 925 A,

D4 US 2002 / 0 087 625 A1,

D5 US 2002 / 0 147 819 A1,

D6 US 2002 / 0 115 426 A1,

D7 US 2002 / 0 016 153 A1,

D8 US 6 148 205 A,

D9 US 2002 / 0 174 354 A1,

D10 van den Heuvel et al.: „SECURE CONTENT MANAGEMENT IN AUTHORISED DOMAINS“, Januar 2002,

D11 Menezes et al.: „HANDBOOK of APPLIED CRYPTOGRAPHY“, Juni 1996,

D12 Mäki, S.: „Security Fundamentals in Ad-hoc Networking“, 25. Mai 2000,

D13 Nokia, „Proposal for DVB Content Protection & Copy Management Technologies“, Version 1.0, Oktober 2001,

D13a DVB CPT CfP, Rev. 1.2, Juli 2001,

D13b Information Disclosure Statement vom 26. März 2004,

D13c CPT Report von X … , Micronas a DVB Member

Company, November 2001,

D14 Rosenblatt W., Trippe W., Mooney S.: „Digital Rights Management - Business and Technology“, M&T Books, Kapitel 2, 4 und 5, 2002.

Die Klägerin vertritt die Auffassung, der Gegenstand der Patentansprüche 1 und 9 gehe über den Inhalt der Anmeldung in der ursprünglich eingereichten Fassung hinaus, und das Streitpatent sei wegen unzulässiger Erweiterung für nichtig zu erklären. Sie vertritt dazu die Auffassung, dass nicht ursprungsoffenbart sei, dass die Geräte einer Domain die mit einem Account verbundenen Rechte teilten und zudem nicht offenbart sei, dass der Schlüsselaussteller unabhängig von der Vorrichtungsdomain sei. Sie ist ferner der Auffassung, der Gegenstand der angegriffenen Patentansprüche sei jeweils nicht neu gegenüber jeder der Druckschriften D1, D3 und D13. Des Weiteren beruhe der Gegenstand gegenüber einer Zusammenschau von D13 und D11, von D13 und D2, von D2 und D4 sowie von D2 und D5 nicht auf einer erfinderischen Tätigkeit. Dies gelte auch ausgehend von der Druckschrift D2 in Kombination mit dem Fachwissen. Insbesondere habe für den Fachmann eine Kurzstreckenverbindung und eine asymmetrische Verschlüsselung nahegelegen. Die Klägerin vertritt zudem die Auffassung, die Druckschrift D13 sei als Beitrag zum DVB-Projekt zur Standardisierung des Digitalfernsehens noch vor dem Prioritätstag des Streitpatents der Öffentlichkeit zugänglich gemacht worden.

Auf den qualifizierten Hinweis des Senats vom 15. Dezember 2023 haben die Parteien ergänzend vorgetragen.

Die Klägerin beantragt,

das europäische Patent EP 1 579 621 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland in vollem Umfang für nichtig zu erklären.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte verteidigt das Streitpatent in der geltenden Fassung und tritt der Klage in allen Punkten entgegen. Die erteilten Ansprüche gingen nicht über die ursprünglich eingereichten Unterlagen hinaus. Der Gegenstand des Streitpatents sei neu, jedenfalls erfinderisch gegenüber dem Stand der Technik. Die Beklagte ist insbesondere der Auffassung, es habe für den Fachmann an einem Anlass gefehlt, aus dem Stand der Technik zu dem Gegenstand des Streitpatents zu gelangen. Die Beklagte bestreitet, dass die Druckschrift D13 vorveröffentlicht sei.

Wegen der weiteren Einzelheiten des Vorbringens der Parteien wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen und den weiteren Inhalt der Akte Bezug genommen.

Entscheidungsgründe

Die Klage ist zulässig. Das erforderliche Rechtsschutzbedürfnis besteht auch nach Ablauf der Schutzdauer des Streitpatents, da zwischen den Parteien ein Patentverletzungsverfahren anhängig ist. Die Klage bleibt jedoch ohne Erfolg, denn das Streitpatent ist rechtsbeständig.

I. Zum Streitpatent

1. Das Streitpatent betrifft im Allgemeinen die Verwaltung digitaler Rechte („Digital Rights Management“; DRM), insbesondere ein Verfahren und eine Vorrichtung zur Durchführung einer domaingestützten Verwaltung digitaler Rechte

mit einfacher und sicherer Geräteregistrierung bzw. -einbindung („enrollment“; vgl. Streitpatentschrift, Abs. [0001]). Werthaltige digitale Inhalte würden durch die Verwaltung digitaler Rechte geschützt, welche durch sichere und fälschungsresistente elektronische Geräte implementiert werden (vgl. Streitpatentschrift, Abs. [0002]). Ausgangspunkt ist ein Verfahren zum Schutz digitaler Rechte, bei dem erlaubt ist, (digitale) Inhalte innerhalb einer Domain von Geräten freizugeben („share“). Geräte einer solchen Domain könnten beispielsweise eine gemeinsame Zahlungsmethode bzw. gemeinsame Kontoinformationen wie diejenigen einer Kreditkarte oder eine Kontonummer verwenden. Beispielsweise könne ein Nutzer für den Zugriff auf ein digitales Werk für eine bestimmte Zeit zahlen. Soweit die Geräte Teil einer Domain sind, welche die Kontoinformation teilen, könne jedes dieser Geräte auch auf das digitale Werk zugreifen, wohingegen allen anderen Geräten der Zugriff verwehrt bleibe. In ähnlicher Weise könne ein Nutzer für jeden Zugriff auf ein digitales Werk zahlen, wobei das Konto dann beim Zugriff von jedem Gerät innerhalb der Domain belastet werde. Ein derartiges Verfahren habe zwei Nachteile: Es sei erstens ein Problem für den Benutzer, jedes seiner Geräte zu registrieren, und es sei zweitens ein Problem, dass die Sicherheit des digitalen Inhalts dadurch gefährdet sei, dass über Fernzugriff Geräte registriert werden könnten, die sich innerhalb einer großräumig verteilten Domain befinden.

Zum druckschriftlichen Stand der Technik nennt die Streitpatentschrift in Absatz [0005] ein System zum Schützen von Inhalten, die auf einem tragbaren Gerät gespeichert sind, wobei dem Benutzer erlaubt werde, diese Inhalte nahtlos zu Hause und darüber hinaus zu verwenden, während gleichzeitig die Rechte des Rechteinhabers geschützt werden könnten. Dabei handele es sich um „IBM’s xCP Cluster Protocol“, wonach der geschützte Inhalt in einem dynamischen Cluster eines Netzwerks aus Aufnahme- und Wiedergabegeräten eingebunden werde, so dass der Inhalt dieser Geräte unter einem einzigen Sicherheitsschema unabhängig von speziellen Speicher- oder Übertragungsschnittstellen und -Protokollen verwaltet werden könne. Innerhalb eines Heimnetzwerks bildeten die Geräte ein Cluster einer verschlüsselten Domain. Weiterhin nennt die Streitpatentschrift in

Absatz [0006] die Offenlegungsschrift US 2002/0157002 A1, welche ein domainbasiertes DRM beschreibe, wobei die Geräte der Domain einen gemeinsamen kryptographischen Schlüssel verwendeten. Dabei werden von einer Domain-Instanz/Stelle in Verbindung mit einem DRM-Modul in den Kommunikationsgeräten selektiv Geräte zu einer oder mehreren Domains registriert oder abgemeldet sowie der Zugriff auf die verschlüsselten digitalen Informationen gesteuert.

In diesem technischen Kontext bestehe daher Bedarf an einer domainbasierten Verwaltung digitaler Rechte mit einfacher und sicherer Eintragung („enrollment“) von Geräten, um die Sicherheit des (digitalen) Inhalts zu erhöhen (vgl. Streitpatentschrift, Abs. [0004] u. [0008]).

2. Die erteilten nebengeordneten Patentansprüche 1 und 9 lassen sich in der maßgeblichen englischen Verfahrenssprache wie folgt gliedern:

1 A method for registering a new device as part of a domain of devices, which share rights associated with a common account, for use in accessing protected digital content within a digital-rights management system, the method comprising the steps of:

1.1 receiving, over a short range link, domain information corresponding to the domain of devices from a device existing within the domain of devices;

1.2 providing the domain information to a key issuer, which is separate from the domain of devices, causing the key issuer to issue a private key to the new device,

1.2.1 wherein the private key is based on the domain information and

1.2.2 is utilized by all devices within the domain of devices; and

1.3 receiving the private key from the key issuer for use in accessing the protected digital content within the digital rights management system.

9 An apparatus comprising:

9.1 communication circuitry for receiving, over a short range link, domain information from a device existing within a domain of devices, which share rights associated with a common account, for use in accessing protected digital content within a digital rights management system;

9.2 storage for storing the domain information; and

9.3 logic circuitry for providing the domain information to a key issuer which is separate from the domain of devices, causing the key issuer to issue a private key for use in accessing protected digital content to the apparatus,

9.3.1 wherein the private key is based on the domain information and

9.3.2 is utilized by all devices within the domain of devices.

3. Der hier angesprochene Fachmann weist einen ingenieurwissenschaftlichen Studienabschluss der Nachrichtentechnik (Univ. oder Master) auf und hat mehrere Jahre Berufserfahrung auf dem Gebiet von Systemen zur Verwaltung digitaler Rechte (DRM-Systeme). Darüber hinaus verfügt der Fachmann über Kenntnisse von netzwerkbasierten Systemen und kryptographischen Verfahren.

4. Der Senat versteht das Streitpatent vor dessen technischem Hintergrund wie folgt:

4.1 Zur Begrifflichkeit „Domain-Information“:

Die anspruchsgemäße Domain-Information wird zur Identifikation einer Domain verwendet. Domain-Information ist insofern von Informationen abzugrenzen, die lediglich ein einzelnes Gerät identifizieren und somit gerätespezifisch seien. Der Senat teilt diese von der Beklagten vertretene Auslegung sowohl hinsichtlich der Unterscheidung zwischen einer Domain-Information und einer gerätespezifischen Information, als auch dahingehend, dass die Domain-Informationen zur

Identifikation der Domain verwendet wird. Zwar wird der Begriff Identifikation nicht wörtlich im Anspruchswortlaut verwendet, jedoch identifizieren beispielsweise ein Domain-Name und ein privates Domain-Passwort die Domain (vgl. Streitpatentschrift, Abs. [0008]). Ein zur Domain hinzugefügtes Gerät kontaktiert einen Schlüsselaussteller („key issuer“), um die Registrierung in die Domain zu vervollständigen. Gemäß Absatz [0021] können auch Kreditkarteninformationen eine Domain-Information darstellen.

Soweit die Klägerin im Gegensatz zur Beklagten implizit die Auffassung vertritt, bereits eine Endgerätekennung entspreche der Domain-Information im Sinne des Streitpatents, greift diese Argumentation zur Überzeugung des Senats nicht durch. Denn eine Endgerätekennung identifiziert lediglich das Gerät selbst und ist gerätespezifisch. Auf die Domain-Information im Detail kommt es dabei nicht an. Vielmehr besteht die gegenüber dem in der Streitpatentschrift genannten Stand der Technik erfindungswesentliche Idee darin, dass die Domain-Informationen über eine Kurzstreckenverbindung übertragen werden. Denn sowohl die Beschreibungseinleitung als auch der Absatz [0021] der Streitpatentschrift sprechen das bekannte Problem an, wonach die Übertragung der Informationen über weite Strecken kompromittiert werden könnte.

Bei den Geräten („domain of devices“; Merkmal 9.1), die bereits Teil der bestehenden Domain sind, kann es sich gemäß Absatz [0012] und [0013] der Streitpatentschrift um Computer, Mobiltelefone oder PDAs, aber auch um Set-Top-Boxen, Autoradios oder netzwerkgebundene MP3-Player handeln. Diese Geräte können geeignet sein, digitalen Inhalt wiederzugeben („renders digital content“).

4.2 Zur Begrifflichkeit „Rechte“ in Zusammenhang mit einem gemeinsamen Konto:

Der dem Nichtigkeitsverfahren zugrundeliegende Anspruchswortlaut betrifft das Hinzufügen von Geräten zu einer bestehenden Domain mit bereits geteilten

Zugriffsberechtigungen. Das gemeinsame Konto („share rights associated with a common account“) ist lediglich insofern von Bedeutung, als dass es die Eigenschaften der Domain beschreibt. Rechte von unterschiedlichen Konten, die ggf. sogar verschiedenen Personen zugeordnet sind, werden nicht in dieser Domain geteilt.

Die „Rechte“ beziehen sich auf die in dem DRM-System verwalteten digitalen Inhalte. Die Nutzung der geschützten digitalen Inhalte oder Werke betrifft gemäß Anspruchswortlaut den Zugriff darauf, und ist nicht auf die in der Streitpatentschrift beschriebene Wiedergabe eines Werks beschränkt. Der angesprochene Fachmann geht vielmehr davon aus, dass eine differenzierte Nutzungsberechtigung in dem zugrundeliegenden DRM-System verwaltet wird. Insofern und in Verbindung mit den Merkmalen 9.3.1 und 9.3.2 gelten für die Nutzung der geschützten digitalen Inhalte durch die anspruchsgemäße Vorrichtung („apparatus“) dieselben Zugriffsbedingungen wie für die anderen Geräte der Domain.

Der Hinzuerwerb weiterer Rechte ist nicht vom Anspruchswortlaut umfasst, denn es geht anspruchsgemäß um das Gerät, wobei die bereits bestehenden Rechte, die auch die anderen Geräte der Domain an den digitalen Inhalten besitzen, auch dem hinzugefügten Gerät eingeräumt werden. Die technische Lehre dazu umfasst, dass ein privater Schlüssel für alle Geräte der Domain ausgegeben wird, was im Gegensatz zu einem individuellen privaten Schlüssel steht, der nur für das neue Gerät („apparatus“) gilt. Die Lehre des Streitpatents führt in diesem Kontext aus, dass die Rechte nicht untereinander weitergegeben werden sollen, da dies zu unsicher sei, sondern ein privater Schlüssel (vom Schlüsselanbieter) ausgegeben wird, der von allen Geräten genutzt werden kann. Um dies zu erreichen, wird die Vorrichtung („apparatus“) in die bestehende Domain aufgenommen, wozu die Vorrichtung entsprechend den Merkmalen 9.1 bis 9.3.2 geeignet sein muss.

4.3 Zur Begrifflichkeit „privater Schlüssel“:

Bei dem privaten Schlüssel handelt es sich um den privaten Schlüssel eines public-private-key Paares gemäß Absatz [0011] der Streitpatentschrift. Der private Schlüssel ist demnach ein kryptographischer Schlüssel (vgl. auch Abs. [0020]), der zum Entschlüsseln des durch den öffentlichen Schlüssel („DRM public key“) verschlüsselten Inhaltsschlüssels benötigt wird (vgl. Abs. [0020], „The rights object contains an encrypted encryption key (content encryption key) needed to render (execute) the digital content. The content encryption key is encrypted with the DRM public key so it can be decrypted only using the DRM private key.“). Der private Schlüssel gilt für alle Geräte der Domain gleichermaßen (vgl. Abs. [0019], „Key issuer 105 then sends equipment 101 the DRM certificate and the DRM private key utilized by the domain.“, Unterstreichung hinzugefügt). Nichts Anderes entnimmt der Fachmann dem Wortlaut des Merkmals 9.3.2 explizit („is utilized by all devices (101) within the domain of devices“).

4.4 Zur Begrifflichkeit „Kurzstreckenverbindung“:

Gemäß Absatz [0013] der Streitpatentschrift fallen unter den anspruchsgemäßen Begriff einer Kurzstreckenverbindung („short range communication“) Funkverbindungen mit kurzer Reichweite (u. a. Bluetooth, 802.11, d. h. WLAN), aber auch physische Kabelverbindungen oder ein Dockingstecker bzw. eine Infrarotkommunikation. Zwar verwendet Merkmal 9.1 lediglich den Begriff „short range link“, jedoch ist klar, dass darunter der in der Streitpatentschrift verwendete Ausdruck „short range communication link“ bzw. „short range communication channel“ zu verstehen ist (vgl. Fig. 1 Bezugszeichen 108 i. V. m. Abs. [0009] – [0010], [0013]). Das Gerät soll sich gemäß Absatz [0008] zumindest bei der Registrierung bevorzugt in der Nähe einer vorhandenen Domain befinden (… „preferably are in close proximity.“). Dies betrifft die Abgrenzung zu einer großräumigen Verbindung wie dem Internet (vgl. auch Fig. 1), was in der Beschreibungseinleitung als nachteilig beschrieben wird (vgl. Abs. [0004]; „remotely register“).

4.5 Zum Patentanspruch 9 als Ganzes:

Die beanspruchte Vorrichtung („apparatus“; Merkmal 9) weist drei räumlich-körperliche Hauptkomponenten auf:

- Eine Kommunikationsschaltung („communication circuitry“), die geeignet ist, über eine Kurzstreckenverbindung von einem (anderen) Gerät („device“) Domain-Informationen zu empfangen (Merkmal 9.1),
- einen Speicher („storage“), der geeignet ist, Domain-Informationen zu speichern (Merkmal 9.2), und
- eine Logikschaltung („logic circuitry“), die geeignet ist, Domain-Informationen bereitzustellen (Merkmal 9.3).

Funktional wirken die Komponenten in der Weise zusammen, dass die Domain-Information von dem o. g. (anderen) Gerät aus einer bestehenden Domain von Geräten empfangen wird. Dabei ist allen Geräten der Domain gemeinsam, dass sie Rechte für den Zugriff auf geschützte digitale Inhalte eines DRM-Systems teilen, wobei die Rechte einem gemeinsamen Konto („common account“) zugeordnet sind (Merkmal 9.1). Gemäß Merkmal 9.2 ist der Speicher der beanspruchten Vorrichtung geeignet, die o. g. empfangene Domain-Information zu speichern. Das Gerät („apparatus“) gemäß Patentanspruch 9 weist die oben genannten räumlich-körperlichen und weitere funktionale Eigenschaften auf. Gemäß Beschreibung, Absatz [0019], sind zwar die beiden Anwendungsfälle des Hinzufügens des Geräts zu einer bestehenden Domain sowie des Eröffnens einer neuen Domain ausgebildet. Die Eigenschaft, gemäß Merkmal 9.1 Informationen aus einer bestehenden Domain zu empfangen, beschränkt jedoch das beanspruchte Gerät darauf, dass es geeignet sein muss, zu der bestehenden Domain hinzugefügt zu werden. Das Gerät kann insofern nicht das erste Gerät der Domain sein, da es für das erste Gerät kein weiteres Gerät der bestehenden Domain gibt, von dem es anspruchsgemäß die Domain-Information empfangen könnte.

Der Logikschaltkreis (Merkmal 9.3) ist funktional dazu geeignet, die o. g. Domain-Informationen einem externen Schlüsselaussteller bereitzustellen. Was der Schlüsselaussteller mit den Domain-Informationen bewirkt (hier: Erzeugen eines privaten Schlüssels oder Abrufen eines bekannten Schlüssels aus der Datenbank, vgl. Streitpatentschrift, Abs. [0019]) beschränkt die beanspruchte Vorrichtung nicht. Jedoch muss die Vorrichtung eingerichtet sein, um mit dem so generierten privaten Schlüssel die von allen Geräten der Domain geteilten Rechte an den geschützten digitalen Inhalten eines DRM-Systems und somit diese selbst nutzbar zu machen (Merkmale 9.3.1 und 9.3.2).

4.6 Das Verfahren gemäß Patentanspruch 1 betrifft die mit den gleichen Begrifflichkeiten beanspruchten und im Wesentlichen inhaltsgleichen Verfahrensschritte, wobei das Hinzufügen eines Geräts zu einer bestehenden Domain und das Einräumen der für die Domain bestehenden Rechte nunmehr mit Anspruch 1, Merkmal 1 explizit (als funktionelles Merkmal) beansprucht wird (dort: „a method for registering a new device as part of a domain of devices …“, Unterstreichung hinzugefügt). Im Übrigen versteht der Fachmann den Patentanspruch 1 entsprechend dem Patentanspruch 9.

II. Zu den Nichtigkeitsgründen

Weder der geltend gemachte Nichtigkeitsgrund der unzulässigen Erweiterung gegenüber den ursprünglichen eingereichten Unterlagen noch der geltend gemachte Nichtigkeitsgrund der mangelnden Patentfähigkeit liegen vor.

1. Zum Nichtigkeitsgrund der unzulässigen Erweiterung

Der Gegenstand des Streitpatents geht nicht über den Inhalt der Patentanmeldung in ihrer ursprünglich eingereichten Fassung hinaus (Art. II § 6 Abs. 1 Nr. 3 IntPatÜG i. V. m. Art. 138 Abs. 1 Buchst c) EPÜ).

Die Vorrichtung gemäß dem erteilten Patentanspruch 9 ist mit sämtlichen Merkmalen in der ursprünglich eingereichten Fassung (Offenlegungsschrift WO 2004/051916 A1, NK3) offenbart.

Die NK3 offenbart eine Vorrichtung gemäß Merkmal 9 (vgl. u. a. NK3, S. 2, Z. 20 ff., auch NK3, Anspruch 10) mit Merkmal 9.2 (vgl. z. B. NK3, Anspruch 10, aber auch NK3, Fig. 2, Bz. 211 i. V. m. NK3, S. 7, Z. 27 ff.).

Die Frage der ursprünglichen Offenbarung der Merkmale 9.1 und 9.3 steht zwischen den Parteien in Streit hinsichtlich der Teilmerkmerkmale „a domain of devices, which share rights associated with a common account“ (dt.: [Domain aus Vorrichtungen], die Rechte in Zusammenhang mit einem gemeinsamen Konto teilen) und „a key issuer which is separate from the domain of devices“ (dt.: [Schlüsselaussteller], der unabhängig von der Vorrichtungsdomain ist).

Soweit die Klägerin vorgetragen hat, dass hinsichtlich des Merkmals 9.1 an keiner Stelle der ursprünglichen Anmeldung als zur Erfindung gehörig offenbart sei, dass die Geräte einer Domain, die Rechte in Zusammenhang mit einem gemeinsamen Konto teilten, sondern vielmehr ursprünglich offenbart sei, dass jedes Gerät für sich bei einem Rechteaussteller Rechte für den Zugriff auf ein Werk anfordern müsse, greift dies nicht durch. Denn, wie von der Beklagten vorgetragen, findet sich dieses Teilmerkmal in der Offenlegungsschrift NK3, S. 1, Z. 22 - 31 i. V. m. NK3, S. 6, Z. 22 und NK3, Anspruch 3. Dabei ist es entgegen der Auffassung der Klägerin unschädlich, dass NK3, S. 1, Z. 22 - 31, den Stand der Technik beschreibt. Denn die in der Streitpatentschrift und der zugehörigen Anmeldung genannten Erfinder stellen sich die Aufgabe, die aus dem Stand der Technik dargestellten Probleme für

DRM-Systeme, bei denen sich Vorrichtungen Rechte in Zusammenhang mit einem gemeinsamen Konto teilen, zu lösen. Das Teilen der mit einem Account verbundenen Rechte ist jedoch nicht Gegenstand der in der Anmeldung geäußerten Problemstellung, sondern gerade dieses Merkmal wird für die offenbarte Lösung beibehalten und gemäß dem Lösungsansatz um die Kommunikation über die Kurzstreckenverbindung mit einem Gerät der Domain und das Bereitstellen der Domain-Information an den Schlüsselaussteller ergänzt.

Die Klägerin vertritt darüber hinaus die Auffassung, dass nicht ursprünglich offenbart sei, dass der Schlüsselaussteller unabhängig von der Vorrichtungsdomain sei. Aus der Gesamtschau der NK3 geht jedoch hervor, dass der Schlüsselaussteller nicht Teil der Domain ist (vgl. NK3, Fig. 1). Der Schlüsselaussteller 105 („key issuer") ist außerhalb der Domain der Geräte („user equipment") angeordnet (vgl. NK3, S. 3, Z. 4 - 9), weil eine Registrierung innerhalb der Domain als nicht sicher genug angesehen wird und daher ein vertrauenswürdiger Server wie ein Schlüsselaussteller („trusted server"; „i.e. key issuer") beteiligt werden müsse. Auch die NK3, S. 8, Z. 26 – 27, offenbart, dass der Schlüsselaussteller über das Mobilfunknetz oder das Internet erreichbar ist, also im Speziellen nicht Teil der über die Kurzstreckenverbindung erreichbaren Geräte der Domain ist. Die restlichen Merkmale des Patentanspruchs 9 entnimmt der Fachmann darüber hinaus den ursprünglichen Patentansprüchen 10, 12 und teilweise 13.

Auch das Verfahren gemäß Patentanspruch 1 ist durch die o. g. Fundstellen entsprechend offenbart.

2. Zum Nichtigkeitsgrund der fehlenden Patentfähigkeit

Dem Streitpatent in der erteilten Fassung steht der Nichtigkeitsgrund der fehlenden Patentfähigkeit nach Artikel II § 6 Absatz 1 Nr. 1, 2 und 3 IntPatÜG, Art. 138 Abs. 1 Buchst. a) EPÜ i. V. m. Art. 54, 56 EPÜ nicht entgegen. Denn die hiermit unter

Schutz gestellte Lehre erweist sich gegenüber dem im Verfahren entgegengehaltenen Stand der Technik als neu und auf einer erfinderischen Tätigkeit beruhend.

2.1 Der Gegenstand des Patentanspruchs 9 ist neu gegenüber dem Stand der Technik, denn keine der von der Klägerin als neuheitsschädlich bezeichneten Druckschriften D1, D3 und D13 offenbart für sich genommen sämtliche Merkmale des Patentanspruchs 9.

2.1.1 Die Druckschrift US 2002/0166047 A1 (D1) betrifft eine Vorrichtung und ein Verfahren, um Informationen zum Entschlüsseln von Inhalten bereitzustellen (vgl. D1, Abs. [0002]; D1, Abs. [0010]: … „for providing information for decrypting content“ …). Gemäß D1 werden geschützte Inhalte in verschlüsselter Form von einem Inhalteserver („content server 22“) via Internet an einen PC (23) bereitgestellt. Ein Mobilfunktelefon („cellular telephone 26“) repräsentiert einen Benutzer (durch seine Telefonnummer), der zur Nutzung des geschützten Inhalts berechtigt ist. Nach einem Authentifizierungsvorgang lädt der Nutzer von einem Lizenzserver („license server 29“) einen Lizenzschlüssel auf sein Mobilfunktelefon. Der Lizenzschlüssel dekodiert einen Inhaltsschlüssel („content key“), mit dem die verschlüsselten Inhalte auf dem PC entschlüsselt werden und wiedergegeben werden können. Zur Übertragung der Schlüssel und IDs ist das Mobiltelefon über eine USB-Verbindung mit dem PC verbunden.

Gemäß D1 wird ein Lizenzschlüssel („license key“) verwendet, um einen Inhaltsschlüssel („content key“) zu dekodieren, welcher dann in dekodierter Form an den PC gesendet wird (vgl. D1, Abs. [0062]). Gemäß D1, Absatz [0040] (auf S. 4, oben), wird der Inhaltsschlüssel nicht auf dem PC gespeichert, sondern dort direkt vom Wiedergabeprogramm zum Entschlüsseln des Inhalts verwendet („The PC 23 directs the application program for playing back the content not to store a content key for decrypting the content in a storage, thereby protecting the content against illegal attacks.“). Somit befindet sich die Berechtigung zur Nutzung des Inhalts in

Form des Lizenzschlüssels auf dem Mobilfunktelefon. Dies gilt auch für die zweite Ausführungsform, bei der der PC mit dem Lizenzserver kommuniziert (vgl. D1, Abs. [0073] ff. i. V. m. D1, Fig. 6). Zwar wird bei dieser der Lizenzschlüssel vom Lizenzserver an den PC gereicht. Anschließend wird er aber vom PC weiter an das Mobilfunktelefon übermittelt, das dann den Lizenzschlüssel – wie in der ersten Ausführungsform gemäß D1 – verwendet, um den Inhaltsschlüssel zu dekodieren. Der PC teilt somit ohne Mobilfunktelefon keine Rechte am Inhalt.

Die Klägerin sieht in dem PC (23) der D1 die anspruchsgemäße Vorrichtung gemäß Merkmal 9 („apparatus“) und in der USB-Verbindung zwischen dem Mobilfunktelefon (26) und dem PC (23) der D1 eine anspruchsgemäße Kurzstreckenverbindung („short range link“). Sie erkennt in dem Mobilfunktelefon eine Vorrichtung („device“) gemäß Merkmal 9.1, also ein Gerät der Domain. Ferner sieht sie in der Endgerätekennung der D1, d. h. der Telefonnummer des Mobilfunktelefons (26), eine Domain-Information i. S. d. Streitpatents, im Lizenzserver (29) der D1 einen Schlüsselaussteller und in dem Lizenzschlüssel der D1 einen privaten Schlüssel i. S. d. Streitpatents.

Diese Merkmalszuordnung der Klägerin greift nicht durch. Denn der Lizenzschlüssel (alias „private key“) wird ausschließlich vom Mobilfunktelefon genutzt, um den Content-Key zu dekodieren, und nicht vom PC. Insofern bilden PC und Mobilfunktelefon der D1 auch keine Domain. In der D1 findet sich zudem keine Information, die den PC und das Mobilfunktelefon als eine bestehende Domain kennzeichnet (d. h. kein gemeinsamer Name, kein gemeinsames Passwort, keine gemeinsame Bezahlmethode), somit fehlt der D1 auch die anspruchsgemäße Domain-Information. Die D1 offenbart daher weder, dass der PC (alias „apparatus“) eine solche Domain-Information empfangen könnte, noch, dass der PC sie speichern könnte, und auch nicht, dass sie vom PC für einen Schlüsselanbieter bereitgestellt werden könnte.

Zwar ist es gemäß D1, Absatz [0063], auch möglich, dass der Nutzer sein Mobilfunktelefon mit einem anderen Gerät oder PC als dem PC (23) verbindet, jedoch offenbart die D1 nicht, dass der fremde PC und der PC (23) Geräte einer Domain sind. Vielmehr deutet der Kontext der D1 darauf hin, dass die beiden PCs nicht in einer Domain sind, denn bei dem anderen PC handelt es sich um das Gerät eines Dritten, das nicht lizensiert ist. Der mittels Mobilfunktelefon autorisierte Nutzer kann dieses Gerät eines Dritten lediglich zur Wiedergabe seiner mittels Lizenzschlüssel lizensierten Musik verwenden.

Eine Kommunikationsschaltung, ein Speicher und eine Logikschaltung für sich genommen sind somit aus der D1 bekannt, denn der PC (23) weist einen Kommunikationsschaltkreis (USB-Schnittstelle) und üblicherweise einen Speicher sowie eine Logikschaltung (üblicherweise eine CPU) auf. Jedoch fehlt das funktionale Zusammenwirken über die Domain-Information. Hinsichtlich des Patentanspruchs 9 fehlt der D1 zumindest die Domain-Information i. S. d. Streitpatents, d. h. zumindest Merkmal 9.3 lehrt die D1 nicht.

2.1.2 Die Druckschrift GB 2 367 925 A (D3) betrifft die Verwaltung digitaler Rechte (digital rights management), wobei ein sogenanntes „node locking“ verwendet wird. Gemäß D3 wird auf einem Gerät, beispielsweise einem Mobiltelefon, eine von einem Server ausgestellte Zugangsberechtigung für die Nutzung von digitalen Inhalten bereitgestellt. Das Mobiltelefon kann dabei mit verschiedenen Endgeräten verbunden werden, auf denen die digitalen Inhalte dargestellt werden können, beispielsweise mit einem PC. Die Verbindung zwischen Mobiltelefon und PC kann dabei drahtlos oder mittels Kabel ausgestaltet sein.

Die D3 geht von einem bekannten, herkömmlichen „node-locking“-Verfahren aus (vgl. D3, Fig. 2 mit Beschreibung), bei dem während der Übertragung der Inhalte vom Server entsprechende Rechte für die Nutzung der Inhalte mit einer geräteabhängigen und unter Verwendung von gerätespezifischen Eigenschaften

berechneten Knotenkennung („pseudo- or semi-unique node identifier obtained or calculated from characteristics of consumer device 106.“) gesperrt („locked“) und die Inhalte in gesperrter Form auf dem Gerät gespeichert werden (vgl. D3, S. 5, Z. 20 ff.). Die Nutzung der gesperrten Inhalte erfordert einen speziellen Klienten und wird freigegeben, wenn die damit (zurück-)berechnete Knotenkennung mit der gerätespezifischen Knotenkennung übereinstimmt. Die Idee der D3 besteht darin, dass eine Kopie der gesperrten Inhalte auf einem fremden Gerät mit hoher Wahrscheinlichkeit zu einer anderen als der gerätespezifischen Knotenkennung führt und daher unbenutzbar bleibt (vgl. D3, S. 5, Z. 25 ff.). Gemäß D3 ist es nachteilig, dass der Benutzer die Inhalte nur auf einem Gerät nutzen kann (vgl. D3, S. 6, Z. 6 ff.). Die D3 stellt daher ein erweitertes „node-locking“-Verfahren („extend the concept of node locking“; vgl. D3, S. 6, Z. 17 ff.) bereit.

Die offenbarte Lehre der D3 ändert an dem bekannten, herkömmlichen „node-locking“-Verfahren, dass die Knotenkennung nicht an das Benutzerendgerät selbst (also das Gerät, auf dem die Inhalte nutzbar sind) gebunden ist, sondern an ein zusätzliches mobiles Gerät (Mobiltelefon 302 oder Smartcard) übertragen wird, das mit dem Benutzergerät verbunden werden muss. Somit befinden sich zwar die gesperrten Inhalte auf dem Benutzergerät, sie können aber nur entsperrt werden, wenn das zusätzliche mobile Gerät mit dem Benutzergerät verbunden ist (vgl. D3, S. 11, Z. 32 – S. 12, Z. 8).

Die D3 basiert somit auf einem gerätespezifischen Konzept, da für die Wiedergabe der geschützten digitalen Inhalte immer das mobile Gerät verwendet werden muss. Ein domainbasiertes DRM-System offenbart die D3 daher nicht. Somit fehlen zumindest das Merkmal 9.1 unter dem Aspekt, dass das Gerät geeignet sein muss, die Domain-Information einer bestehenden Domain zu empfangen, sowie das Merkmal 9.3 unter dem Aspekt, dass das Gerät eine Logikschaltung aufweisen muss, die geeignet ist, die Domain-Information einem Schlüsselanbieter bereitzustellen.

2.1.3 Die Veröffentlichung von Nokia (D13) betrifft Kopierschutz- und Managementtechnologien für das Digitalfernsehen (DVB) und ist Teil des Standardisierungsprozesses für DVB.

Das Kapitel 4 der D13 beschreibt die Architektur eines „Consumer Domain Models“, wobei autorisierte Geräte in Grenzgeräte („border devices“) und Nichtgrenzgeräte („non-border devices“) unterschieden werden. Das Grenzgerät befindet sich zwar beim Endkunden, ist jedoch mit dem Serviceprovider eng verbunden und verantwortlich für die Domainregistrierung, wozu es ein spezielles Modul („DRM terminating module“) aufweist. Das Public-Private-Schlüsselpaar und das Ausstellerzertifikat sind im Grenzgerät werksseitig vorinstalliert (vgl. D13, S. 40, oben: „Device public/private key pair and digital certificate obtained by device manufacturer from certificate authority are pre-installed in border device at factory.“). Auch für die Nichtgrenzgeräte sind ein Public-Private-Schlüsselpaar und ein Ausstellerzertifikat werksseitig vorinstalliert (vgl. D13, S. 41 Mitte). Das Hinzufügen eines Nichtgrenzgeräts zu einer Domain erfolgt stets über das Grenzgerät.

Die Klägerin hat vorgetragen, die in der D13 genannte „Domain-ID“ stelle eine Domain-Information i. S. d. Streitpatents dar und verweist dazu insbesondere auf die D13, S. 41 und S. 48, woraus der Fachmann entnehme, dass die Domain-ID der D13 vom Grenzgerät an ein Nichtgrenzgerät übertragen werde und dass das Quellgerät („source device“) der D13 auch die Domain-ID zugewiesen bekomme.

Im Ergebnis teilt der Senat diese Auffassung nicht, denn die Domain-ID ist für jedes Grenzgerät spezifisch (vgl. D13, S. 40, Ziff. 2: „Border device ... and forwards the request with its own domain ID to service provider ...“), da jedes Grenzgerät eine eigene gerätespezifische Domain-ID gespeichert hat, die es bereits bei seiner eigenen Registrierung zusammen mit dem symmetrischen Schlüssel vom Content-Provider bzw. Serviceprovider zugewiesen bekommen hat (vgl. D13, S. 39 – 40, „3.

Service provider returns the domain ID and domain symmetric key to the border device over the secured communication channel.“).

Die Verteilung des digitalen Inhalts kann über eine USB-Verbindung oder eine IR-Schnittstelle von dem Speichergerät zu einem mobilen Gerät erfolgen (vgl. D13, S. 60). Die D13, Seite 48, betrifft die Verteilung von Inhalten innerhalb einer autorisierten Domain („content copying within same domain“), wobei zwischen Quellgerät („source device“) und Zielgerät („target device“) unterschieden wird. Mit dem Hinzufügen eines Geräts, wobei eine Domain-Information zumindest eines bereits vorhandenen Geräts verwendet wird, steht diese Fundstelle allerdings nicht in Verbindung. Somit offenbart D13, Seite 48, nicht und weist auch nicht darauf hin, dass die Domain-ID eine Domain-Information i. S. d. Streitpatents sein könnte.

Zutreffend hat die Beklagte hingegen vorgetragen, dass das Grenzgerät einen symmetrischen Schlüssel an das Nicht-Grenzgerät sendet, welcher in einem gesicherten Speicherbereich abgelegt wird (vgl. D13, S. 42, Ziff. 5: „5. Border device sends the domain ID and domain symmetric key to the non-border device, which in turn saves the domain symmetric key into local tamper-resistant storage.“) und der anspruchsgemäße, auf einer Domain-Information basierende private Schlüssel eines separaten Schlüsselausstellers somit von der D13 nicht offenbart wird. Insoweit beschreibt die D13, Seiten 41 und 42, ein Verfahren zum Beitritt eines Geräts zu einer autorisierten Domain („Authorized Domain Joining“). Die D13 sieht dabei vor, dass nach einer Anforderung („domain joining request“) des Nicht-Grenzgeräts an das Grenzgerät das Grenzgerät die Anforderung angereichert mit seiner Domain-ID an den Schlüsselaussteller / Serviceprovider weiterleitet (vgl. D13, S. 41, Schritte 1 und 2), dass der Serviceprovider (vgl. D13, S. 41, Schritt 3) ein hinzugefügtes Gerät registriert, eine Bestätigung („approval“; vgl. D13, S. 41, Schritt 4) an das Grenzgerät sendet und erst dann das Grenzgerät (und nicht der Serviceprovider bzw. der Schlüsselaussteller) den von der Beklagten zitierten Schritt 5 mit Übertragen des symmetrischen Schlüssels (und nicht des

anspruchsgemäßen privaten Schlüssels) sowie der Domain-ID an das hinzugefügte Nicht-Grenzgerät ausführt. Das Merkmal 9.3 fehlt deshalb.

Zur Überzeugung des Senats wird zum Erstellen des Inhaltsschlüssels durch das Grenzgerät in der D13 auf den Seiten 25 und 26 nicht offenbart, dass die Domain-ID der D13 eine Domain-Information i. S. d. Streitpatents darstellt. Denn der von der Klägerin hierzu zitierten Stelle der D13, zweiter Absatz, drittes bis fünftes Aufzählungszeichen, lässt sich zwar entnehmen, dass ein Inhaltsschlüssel als Funktion eines Anfangsschlüssels („content key seed“) und des symmetrischen Schlüssels des Grenzgeräts („the domain symmetric key of the border device“) erzeugt wird, und im Falle einer Erneuerung eines Coupons die originale Domain-ID des Grenzgeräts verwendet wird, die bei Bedarf in anderen Geräten gesichert ist („can be backed up by subsequent devices separate from the voucher“). Jedoch betrifft dies nur die Erstellung einer Inhaltskennung („content ID“). Eine anspruchsgemäße Domain-Information, die die Basis für die Erstellung eines privaten Schlüssels bildet, ist damit nicht offenbart. Insbesondere handelt es sich beim „Content Key“ offensichtlich ebenfalls um einen symmetrischen und nicht um einen anspruchsgemäßen privaten (asymmetrischen) Schlüssel (vgl. D13, S. 24, Tabelle 4). Darüber hinaus wird der „Content Key“ auch nicht anspruchsgemäß immer von allen Vorrichtungen innerhalb der Domain verwendet, sondern gemäß der D13, Seiten 29 und 30, Tabelle 7 i. V. m. Kapitel 4.11.2, in Abhängigkeit von Benutzerzuständen und den jeweils durchgeführten Operationen („The proposed CPCM architecture recognizes that, depending on the original usage state of the content and the operation to be performed, there may be different requirements for content key encryption.“; Merkmal 9.3.2 fehlt gleichermaßen).

Die Lehre D13 offenbart somit nicht die Merkmalskombination 9.1 mit 9.3, 9.3.1 und 9.3.2, da keine Domain-Information für einen Schlüsselaussteller bereitgestellt wird. Stattdessen ist der Schlüssel werksseitig vorinstalliert und die Domain-Information kommt vom Schlüsselaussteller selbst. Insbesondere beschreibt die D13 keinen von einem separaten Schlüsselaussteller erstellten, privaten (asymmetrischen)

Schlüssel auf Basis von Domain-Informationen, der in der Kommunikationsschaltung verwendet wird.

2.2 Hinsichtlich der Neuheit gegenüber dem Stand der Technik gemäß D1, D3 oder D13 gilt für den nebengeordneten Patentanspruch 1 Entsprechendes.

2.3 Der Gegenstand des Patentanspruchs 9 beruht sowohl gegenüber dem Offenbarungsgehalt der Druckschrift D2 in Kombination mit einer der Druckschriften D4 oder D5 oder dem Fachwissen (dokumentiert in den Druckschriften D6, D7, D8 und D14) als auch gegenüber dem Offenbarungsgehalt der Druckschrift D13 in Verbindung mit dem Fachwissen (dokumentiert durch die D11) auf einer erfinderischen Tätigkeit.

2.3.1 Die Druckschrift US 2002/0157002 A1 (D2) ist als Stand der Technik im Absatz [0006] der Streitpatentschrift genannt. Sie betrifft Systeme zur Verwaltung für den sicheren Zugriff auf digitale Inhalte (D2, Abs. [0001]: „… content management systems for securely accessing digital content.“). Die Lehre der D2 stellt einen komfortablen Weg für Kunden bereit, um auf digitale Inhalte zugreifen zu können, wobei Inhalt und Privatsphäre geschützt werden, indem ein domainbasiertes DRM-System anstelle eines herkömmlichen kopierbasierten DRM verwendet wird (vgl. D2, Abs. [0027]). Gemäß der D2 ist der Zugriff auf eine begrenzte Anzahl von Geräten innerhalb einer Domain beschränkt („restricted“), und die verschiedenen Geräte („user device (UD)“) einer Domain teilen sich einen gemeinsamen kryptographischen Schlüssel, der der Domain zugeordnet ist („associated with the domain“). Dabei muss der Benutzer sich nur einmalig mit dem Problem der Sicherheit auseinandersetzen („contend“), wenn er ein Gerät der Domain hinzufügen oder entfernen möchte (vgl. D2, Abs. [0027]). Für das Hinzufügen oder Entfernen eines Geräts in bzw. von der Domain sieht die D2 eine Domaininstanz („domain authority“) vor, die u. a. bei der Registrierung die

Legitimation des Gerätes prüft (vgl. D2, Abs. [0029]), indem ein Domainname und ein Domainpasswort abgefragt werden, welche der Benutzer über ein Benutzerinterface (UI) beispielsweise mittels einer Webseite im Internet eingeben muss (vgl. D2, Abs. [0068]). Insofern offenbart die D2 die Grundidee der domainbasierten Rechteverwaltung, wobei ein Schlüsselaussteller (hier: „domain authority“) bei Bedarf einen Schlüssel zum Entschlüsseln geschützter digitaler Inhalte bereitstellt (vgl. D2, Abs. [0069]).

Zwar verfügen Benutzergeräte wie beispielsweise Mobiltelefone über eine Kommunikationsschnittstelle mit kurzer Reichweite, diese wird jedoch ausschließlich zur Verbindung ins Internet bzw. zur Übertragung von Inhalten zu vertrauenswürdigen Geräten verwendet (vgl. D2, Abs. [0028], [0062], [0081], Unteranspruch 2). Die D2 offenbart somit nicht, dass die Domain-Informationen (z. B. Domainname und Domainkennwort) über eine Kurzstreckenverbindung von einem bereits in der Domain befindlichen Benutzergerät übertragen werden. Vielmehr muss der Benutzer nach der Lehre der D2 die Domain-Information stets manuell über das Internet auf einer Webseite des Schlüsselanbieters eingeben (vgl. D2, Abs. [0067] – [0070]).

Die Lehre der D2 ist in der Streitpatentschrift gewürdigt. Die Streitpatentschrift befasst sich mit der Aufgabe, die beiden essenziellen Nachteile der Lehre der D2 zu überwinden: erstens, dass die Daten für jedes Gerät einzeln eingegeben werden müssen, und zweitens, dass eine Fernbereichsübertragung den Schutz der digitalen Inhalte gefährden könnte. Für eine Kombination der D2 mit der D4 und dem Ziel, die anspruchsgemäße Kurzstrecken-Verbindung zur Übertragung der Domain-Information von einem benachbarten Gerät der Domain hinzuzufügen, fehlt zur Überzeugung des Senats für den Fachmann jegliche Veranlassung.

Die Argumentation der Klägerin, wonach die D2 die Art der Übertragung nicht anspreche und der Fachmann daher, ohne selbst erfinderisch tätig zu werden, in der D4 nach einer Lösung suchen und dabei die Kurzstrecken-Verbindung finden

und auf die Lehre der D2 anwenden werde, überzeugt nicht. Denn es fehlt eine tragfähige Verknüpfung zwischen den beiden Druckschriften für dieses Vorgehen des Fachmanns. Zwar beschreibt die D4 in der Einleitung, dass Musik aus dem Internet auf einen Host heruntergeladen werden kann und dass Benutzerprofile auf dem Host gespeichert werden können, welche für MP3-Anwendungen verwendet werden (vgl. D4, Abs. [0002] - [0006]). Die Profile stehen einem portablen Gerät jedoch nicht zur Verfügung (vgl. D4, Abs. [0007]). Gleichfalls fehlt in der D4 ein Hinweis darauf, dass die Nutzerprofile zwischen einem Host und einem portablen Gerät geteilt werden können, wobei der Host und das portable Gerät das Profil über eine drahtgebundene oder ein drahtlose IR-Schnittstelle übertragen (vgl. D4, Abs. [0014] ff.), also über eine Kurzstrecken-Verbindung i. S. d. Streitpatents. Darüber hinaus stellt das Nutzerprofil gemäß D4 keine Domain-Information i. S. d. Streitpatents dar.

Etwas Anderes ergibt sich auch nicht aus der Argumentation der Klägerin zur Verwendung einer Kurzstreckenübertragung als technologische Leistung des Streitpatents im Vergleich zur der Lehre der D2. Die Schrift D2 offenbare, so die Klägerin sinngemäß, den Aufruf einer Website, wobei es Probleme mit dem Passwortmanagement gebe, was die Lehre der D4 durch ein Passwortmanagement über Kurzstrecke löse. Wie die Beklagte zu Recht ausgeführt hat, beschäftigt sich die Lehre der D4 jedoch mit der Synchronisation von Nutzerprofilen, wozu ein Login erforderlich ist (vgl. D4, Abs. [0020]). Domain-Informationen von bestehenden Geräten überträgt die Lehre der D4 nicht über Kurzstrecke.

Zur Überzeugung des Senats hätte der Fachmann die Schrift D2 auch nicht mit der Entgegenhaltung D5 kombiniert. Denn die D5 betrifft ein Verfahren zum Setzen von WLAN-Parametern, indem ein direkter Kontakt oder eine Nahbereichsverbindung zwischen Kommunikationsgeräten hergestellt wird (vgl. D5, Titel; Abs. [0006]). Die D5 befasst sich mit dem Problem, dass Konfigurationen, die die Authentifikation und kryptographische Information betreffen, herkömmlich händisch durchgeführt werden müssen, was unsicher und kompliziert sei. Die Klägerin hat sinngemäß

vorgetragen, der Fachmann entnehme der D5, eine Kurzstecken-Verbindung dann vorzusehen, wenn vertrauliche Daten übertragen, aber nicht händisch eingegeben werden sollen. Jedoch besteht das Problem, dass der Benutzer nach der Lehre der D2 eine unsichere Übertragung der Domain-Daten zu befürchten hat, nicht a priori, da der Benutzer die Daten manuell in das Gerät eingibt. Ein Problem könnte erst dann entstehen, wenn die manuelle Eingabe ersetzt werden soll. Aber dazu gibt die D2 dem Fachmann keinen Anlass. Denn obwohl das Gerät der D2 auch eine Bluetooth-Schnittstelle mit kurzer Sendereichweite aufweisen kann, werden gemäß der D2 die Domain-Informationen am Gerät selbst (händisch) eingeben. Warum der Fachmann die Lehre der D2 dazu hätte verlassen und auf die Lehre der D5 hätte zugreifen sollen, ergibt sich auch aus dem Vortrag der Klägerin nicht.

Gleiches gilt ausgehend von der D2 unter Verwendung des Fachwissens für die gegenseitige Authentifikation zweier Geräte.

2.3.2 Ausgehend von der D13 in Verbindung mit dem Fachwissen (dokumentiert durch die D11) gelangt der Fachmann ebenfalls nicht in naheliegender Weise zum Gegenstand des Patentanspruchs 9. Die Klägerin hat dazu sinngemäß vorgetragen, dass der symmetrische Inhaltsschlüssel („content key“) der D13 den Fachmann dazu veranlasst hätte, sich über die Verwendung von Schlüsseln Gedanken zu machen. Er hätte dann unter Abwägung der Vor- und Nachteile der aus der D11 bekannten Schlüssel den symmetrischen Schlüssel der D13 durch das im Streitpatent verwendete, asymmetrische Public-Private-Schlüsselpaar ersetzt. Dies überzeugt nicht, denn das Fachwissen gemäß der D11 zeigt gerade, dass symmetrische Schlüssel nicht ohne Weiteres durch asymmetrische Schlüssel ersetzt werden können. Bei Verwendung der asymmetrischen Verschlüsselung ist u. a. nachteilig, dass sie um mehrere Größenordnungen langsamer als symmetrische Verschlüsselungsverfahren ist (vgl. D11, S. 32, (iv)). Die Lehre der D13, insbesondere die von der Beklagten zitierte Fundstelle D13, Seite 28, die explizit eine symmetrische Verschlüsselung als Voraussetzung für die Kopiervorgänge der D13 anspricht, hätte der Fachmann daher nicht verlassen. Die

Lehre der D13 offenbart keinerlei Nachteile, für deren Überwindung der Fachmann eine demgegenüber deutlich langsamere, asymmetrische Verschlüsselung in Kauf genommen hätte.

Darüber hinaus hat die Klägerin mit Verweis auf die D2, Absatz [0069], vorgetragen, dass die D2 offenbare, der Fachmann könne statt eines symmetrischen Schlüssels auch einen privaten Schlüssel („private key“) verwenden. Daher sei nahegelegt, den symmetrischen Schlüssel der D13 durch einen privaten Schlüssel zu ersetzen. Diese Argumentation überzeugt nicht. Zwar waren dem Fachmann dem Grunde nach sowohl symmetrische als auch asymmetrische Verschlüsselungsmethoden bekannt; der Fachmann hatte jedoch keinen Anlass, die Lehre der D13 zu verlassen. Auf die obigen Ausführungen zur Zusammenschau der D13 mit der D11 bzw. mit dem Wissen des Fachmanns wird Bezug genommen.

2.4 Gleiches gilt für den Gegenstand des Patentanspruchs 1, der das Verfahren zum Hinzufügen einer Vorrichtung gemäß Patentanspruch 9 zu einer Domain betrifft. Die Patentfähigkeit des beanspruchten Verfahrens wird durch den vorgetragenen Stand der Technik nicht in Frage gestellt.

2.5 Somit erweisen sich auch die auf die Patentansprüche 1 bzw. 9 rückbezogenen Unteransprüche 2 bis 8 bzw. 10 bis 13 als rechtsbeständig, denn diese betreffen lediglich Ausführungsformen der sie tragenden, gegenüber dem vorgelegten Stand der Technik patentfähigen, unabhängigen Patentansprüche 1 und 9.

III. Nebenentscheidungen

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. Rechtsmittelbelehrung

Gegen dieses Urteil ist das Rechtsmittel der Berufung gegeben.

Die Berufung ist innerhalb eines Monats nach Zustellung des in vollständiger Form abgefassten Urteils, spätestens aber innerhalb eines Monats nach Ablauf von fünf Monaten nach Verkündung, durch einen in der Bundesrepublik Deutschland zugelassenen Rechtsanwalt oder Patentanwalt als Bevollmächtigten schriftlich oder in elektronischer Form beim Bundesgerichtshof, Herrenstr. 45 a, 76133 Karlsruhe, einzulegen.

Dr. Schnurr Heimen Bieringer Dr. Ball Christoph