LG München I, Endurteil v. 21.04.2021 – 21 O 16260/20

Titel:

Keine schutzbereichsbeschränkende Wirkung von Zweckangaben bei verfahrensbezogenen Merkmalen in Vorrichtungsanspruch

Normenkette:

PatG § 9, § 139

Leitsätze:

1. Der Aufnahme von Zweck-, Wirkungs- und Funktionsangaben in den Patentanspruch kommt im Regelfall keine schutzbereichsbeschränkende Wirkung zu; das gilt auch, wenn in einem Vorrichtungsanspruch zugleich verfahrensbezogene Merkmale in Bezug genommen sind. Auf diesen Fall sind die zu Zweck-, Wirkungs- und Funktionsangaben entwickelten Rechtsprechungsgrundsätze entsprechend anzuwenden. Daher ist eine in räumlich-körperlicher Hinsicht anspruchsgemäß gestaltete Vorrichtung grundsätzlich unabhängig davon geschützt, in welchem Funktions- und Wirkungszusammenhang diese verwendet wird. (Rn. 65) (redaktioneller Leitsatz)

2. Beinhaltet ein Vorrichtungsanspruch einen bestimmten Funktions- und Wirkungszusammenhang voraussetzende Verfahrensschritte, muss die entsprechende Vorrichtung gerade in dem definierten Funktions- und Wirkungszusammenhang geeignet sein, die patentgemäß vorausgesetzten Verfahrensschritte in entsprechend funktionsgemäßer Weise durchzuführen. (Rn. 66) (redaktioneller Leitsatz)

Schlagworte:

Patent, Erfindung, Patentanspruch, Fachmann, Vorrichtung, Klagepatent, Domain, Auslegung, Patentverletzung, Verletzung, Technik, Nutzung, Unterlassung, Verwendung, Stand der Technik, technische Lehre, Kosten des Rechtsstreits

Fundstelle:

GRUR-RS 2021, 45514

Tenor

1. Die Klage wird abgewiesen.

2. Die Klägerin trägt die Kosten des Rechtsstreits. Das Urteil ist gegen Zahlung einer Sicherheit in Höhe von 110% des zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand

1
Die Klägerin nimmt die Beklagte wegen behaupteter wortsinngemäßer Verletzung des deutschen Teils des Europäischen Patents EP 1 579 621 B1 betreffend ein domaingestütztes, digitales Rechtemanagementsystem mit leichter und sicherer Geräteregistrierung auf Unterlassung und Rückruf aus den Vertriebswegen in Anspruch.

2
Die Klägerin ist ein USamerikanischer, weltweit tätiger Technologiekonzern, der sich auf internetbezogene Dienstleistungen und Produkte spezialisiert hat. Über die bekannte Suchmaschine „XX“ und das von ihr für mobile Endgeräte entwickelte Betriebssystem „ZZ“ hinaus entwickelt und vermarktet die Klägerin insbesondere Online-Werbetechnologien, Dienstleistungen im Bereich Cloud-Computing und damit in Zusammenhang stehende Software und Hardware wie Smartphones, intelligente Lautsprecher und WLAN-Router.

3
Die Klägerin ist im Register des Deutschen Patent- und Markenamtes eingetragene Inhaberin des deutschen Teils des Europäischen Patents EP 1 579 621 B1 (im Folgenden: EP‘621 oder Klagepatent; Anlagen K-B 1 und K-B 2). Der Hinweis auf die Patenterteilung wurde im europäischen Patentregister am

23.07.2014 veröffentlicht. Beim Deutschen Patent- und Markenamt wird der deutsche Teil des Klagepatents unter dem Aktenzeichen 603 46 535.8 geführt.

4
Der deutsche Teil des Klagepatents steht in Kraft. Über eine von der Beklagten mit Schriftsatz vom 06.11.2020 gegen den deutschen Teil des Klagepatents zum Bundespatentgericht erhobene Nichtigkeitsklage (Anlage EIP B4) ist bislang noch nicht entschieden.

5
Seinem Gegenstand nach betrifft das Klagepatent im Wesentlichen die Verwaltung digitaler Rechte („digital rights management“, DRM), insbesondere ein domainbasiertes System zur Verwaltung digitaler Rechte für eine einfache und sichere Geräteregistrierung.

6
Der mit der Klage allein geltend gemachte Vorrichtungsanspruch 9 lautet in der englischen Verfahrenssprache wie folgt:

„An apparatus (101) comprising:

communication circuitry (213) for receiving, over a short range link (108), domain information (209) from a device (101) 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 (100);

storage (211) for storing the domain information (209); and logic circuitry (210) for providing the domain information (209) to a key issuer (105) which is separate from the domain of devices, causing the key issuer (105) to issue a private key (206) for use in accessing protected digital content (204) to the apparatus, wherein the private key (206) is based on the domain information (209) and is utilized by all devices (101) within the domain of devices.“

7
In deutscher Übersetzung lautet der geltend gemachte Vorrichtungsanspruch 9 wie folgt:

„Gerät, das Folgendes umfasst:

einen Kommunikationskreis (213) zum Empfangen, über eine Kurzstrecken-Verbindung (108), von Domain-Informationen (209) von einer Vorrichtung (101), 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 (100);

einen Speicher (211) zum Speichern der Domain-Informationen (209); und einen Logikkreis (210) zur Bereitstellung der Domain-Informationen (209) für einen Schlüsselaussteller (105), der unabhängig von der Vorrichtungsdomain ist, wodurch der Schlüsselaussteller (105) einen privaten Schlüssel (206) zur Verwendung bei Zugriff auf geschützten digitalen Inhalt (204) für das Gerät ausstellt, wobei der private Schlüssel (206) auf den DomainInformationen (209) basiert und von allen Vorrichtungen (101) innerhalb der Vorrichtungsdomain verwendet wird.“

8
Bei der Beklagten handelt es sich gleichfalls um einen USamerikanischen Technologiekonzern, der auf die Entwicklung und Vermarktung drahtloser Audiosysteme und sogenannter Multi-Room-Audiosysteme spezialisiert ist, die eine gleichzeitige Wiedergabe von Audio-Inhalten in mehreren Räumen eines Haushalts ermöglichen.

9
Zu den von der Beklagten über ihre Tochtergesellschaft YY Europe B. V. in Deutschland angebotenen und vertriebenen Produkten zählen unter anderem die mit der vorliegenden Klage angegriffenen Lautsprecher der Marke „YY“, die als sogenanntes „YY Home Sound System“ zum drahtlosen Streamen von Musik in der Lage sind, insbesondere die Modelle … .

10
Die Klägerin ist der Auffassung, dass es sich bei den angegriffenen Lautsprechern des „YY Home Sound Systems“ um Musikabspielgeräte handelt, welche sämtliche technischen Merkmale des geltend gemachten Vorrichtungsanspruchs 9 in wortsinngemäßer Weise verwirklichen. Insbesondere verfügten die

angegriffenen Lautsprecher über eine WLAN-Schnittstelle und seien damit in der Lage, über eine gemäß Abs. [0013] der Klagepatentschrift patentgemäße Kurzstrecken-Verbindung Domain-Informationen zu empfangen. Dass sich die in einer Domain zu verbindenden Geräte in räumlicher Nähe darüber hinaus befinden müssten, die eine physische Kontrolle durch den Nutzer erlaube, sei dem Anspruchswortlaut nicht zu entnehmen. Dies könne in den geltend gemachten Hauptanspruch auch deswegen nicht in beschränkender Weise hineingelesen werden, weil Unteranspruch 12 anderenfalls keinen eigenständigen Anwendungsbereich mehr hätte.

11
Zu den anspruchsgemäß vorausgesetzten Domain-Informationen zähle die in einem „YY Home Sound System“ verwendete, sogenannte „Household-ID“. Als „Household“ werde ein Satz von Wiedergabegeräten (sog. „players“) innerhalb des gleichen Netzwerks eines YY-Accounts bezeichnet. Die „Household-ID“ diene dabei der Individualisierung und Identifizierung eines Haushalts. Im Falle der Erweiterung eines solchen Haushalts um weitere Geräte würde den Letzteren die identische „Household-ID“ von einem Gerät aus dem Haushalt zugeteilt.

12
Sobald neuer geschützter Inhalt wie etwa ein neuer Musikdienst über ein dem bestehenden Geräteverbund neu hinzugefügtes Gerät erworben werde, würde die „Household-ID“ in patentgemäßer Weise als Teil eines Authentifizierungsprozesses bei einem externen Inhalteanbieter verwendet. Der Schutzbereich des Klagepatents sei nicht auf die Hinzufügung einer neuen Vorrichtung zu einem bestehenden Verbund an Vorrichtungen zur Nutzung bereits vorhandener Inhalte beschränkt. Die insoweit von der Beklagten vertretene, gegenteilige Ansicht schränke den Wortlaut des geltend gemachten Vorrichtungsanspruchs unzulässig ein und beschränke den Schutzbereich des Klagepatents zu Unrecht auf ein einzelnes Ausführungsbeispiel. Der angesprochene, relevante Fachmann verstehe den geltend gemachten Patentanspruch vielmehr so, dass alle Vorrichtungen auf ein gemeinsames Konto zugreifen können und an Rechten, die mit diesem Konto verbunden sind, teilhaben. Weder der Umfang der Rechte noch die Art des Zugriffs auf den geschützten digitalen Inhalt seien eingeschränkt.

13
Daher dürfe das Teilmerkmal „Rechte“ nicht auf den Begriff der „Rechteobjekte“ beschränkt werden.

14
Patentgemäß sei nicht vorausgesetzt, dass Domain-Informationen von einer bereits in der Gruppe eingerichteten Vorrichtung und damit einem anderen Player empfangen würden. Entscheidend sei allein, dass die Domain-Informationen von einer Vorrichtung stammen, die innerhalb einer Domain aus Vorrichtungen besteht, ohne dass es aber diese Vorrichtung oder auch nur die Domain sein muss, die die Informationen versendet. Das Wort „von“ („from“) beziehe sich nicht auf das Empfangen, sondern auf die Domain-Informationen. Patentgemäß müsse es sich daher um Informationen handeln, welche die Domain aus Vorrichtungen und nicht nur ein individuelles Gerät identifizieren. Selbst wenn man der Auslegung der Beklagten folgte, wonach die „Household-ID“ als Domaininformation von einem Gerät aus einer bestimmten Domain an den neu hinzuzufügenden YY-Player gesendet werden müsste, wäre eine Patentverletzung zu bejahen. Denn auch bei dem YY-Controller handele es sich um eine anspruchsgemäße Vorrichtung.

15
Ein anspruchsgemäß vorausgesetzter Speicher sei in den angegriffenen Ausführungsformen als Standard-Hardware-Komponente zudem in Form eines Flash-Speichers enthalten.

16
Weiter enthielten die angegriffenen Ausführungsformen einen patentgemäßen Logikschaltkreis. In den fraglichen Lautsprechern sei ein Mikroprozessor verbaut, der als Logikschaltung fungiere und dazu beitrage, dass Domain-Informationen in Gestalt der „Household-ID“ externen Anbietern von Musikstreaming-Diensten wie „Spotify“, „Apple Music“ oder „Deezer“ als anspruchsgemäßen Schlüsselausstellern bereitgestellt würden. Im Falle der als patentverletzend angegriffenen Aufnahme eines neuen Musikdienstes würde der Diensteanbieter den angegriffenen Ausführungsformen einen sogenannten „Authentifizierungs-Token“ und einen sogenannten „Private Key“ übermitteln, bei denen es sich um patentgemäße private Schlüssel handele. Ein solcher setze gerade nicht die Verwendung zum Entschlüsseln von digitalem Inhalt voraus. Der Anspruchswortlaut setze lediglich voraus, dass der private Schlüssel „zur Verwendung bei Zugriff auf

geschützten digitalen Inhalt“ ausgestellt werde. Insoweit genüge aber die Verwendung im Rahmen der Authentifizierung des Nutzers gegenüber dem externen Musikdienst.

17
Ein patentgemäßer privater Schlüssel sei nicht auf eine in der Beschreibung des Klagepatents genannte kryptographische Ausführungsform beschränkt. Die Beschreibung gemäß Abs. [0011] der Klagepatentschrift betreffe lediglich ein besonderes Ausführungsbeispiel. Entgegen der Beklagten definiere Abs. [0011] nicht den anspruchsgemäßen privaten Schlüssel, der beim Zugriff auf geschützten digitalen Inhalt verwendet wird. Entscheidend sei der Wortlaut des Anspruchs 9, der eine Beschränkung auf die Kryptographie-Technik nicht voraussetze. Ein privater Schlüssel sei daher jede Abfolge von Buchstaben/Ziffern, die geheim bleiben und nicht mit beliebigen externen Dritten geteilt werden soll. Bezugspunkt eines privaten Schlüssels seien überdies die Domaininformationen und nicht ein bestimmter digitaler Inhalt. Der private Schlüssel müsse nur „zur Verwendung bei Zugriff auf geschützten digitalen Inhalt“ und nicht „zur Entschlüsselung“ für das Gerät ausgestellt werden. Dagegen enthalte der Anspruchswortlaut keine Konkretisierung dahingehend, welchen Gegenstand die mit einem gemeinsamen Konto verbundenen Rechte haben.

18
Damit ein Nutzer, der bei einem externen Dienst registriert ist, seine jeweiligen Daten für diesen Dienst nicht bei jedem Aufruf erneut eingeben muss, würde der „Authentifizierungs-Token“ (auch: „AuthToken“) verwendet, der den von einem Nutzer gewünschten Musikdienst mit einem YY-Haushalt verbinde und bei Aufruf des Dienstes zur Authentifizierung verwendet werde. Im Rahmen der Registrierung würde ein YYGerät hierzu den Befehl getDeviceAuthToken an den externen Musikdienst senden, wobei die „Houshold-ID“ mit übersandt werde. Sobald der externe Dienst den Befehl empfange, erstelle er den „AuthToken“ sowie den „Private Key“ und sende diese sodann als Antwort an das anfragende YY-Gerät. Der „Private Key“ würde dabei dazu verwendet, über die Funktion „Refresh-Token“ den „AuthToken“ nach dessen zeitlichem Ablauf zu erneuern. Sowohl bei dem „AuthToken“ als auch dem „Private Key“ handele es sich um eine Reihe an Buchstaben/Ziffern in der Länge von bis zu 2048 Zeichen. Diese Zeichenfolge werde von den angegriffenen Ausführungsformen sowie von den externen Dienste-Anbietern vertraulich behandelt. Selbst wenn man daher einen kryptographischen Schlüssel für patentgemäß notwendig erachten sollte, müsste daher eine Verletzung bejaht werden. Denn bei dem „AuthToken“ und dem „Private Key“ handele es sich bereits deswegen um kryptographische Schlüssel, weil diese zum Zweck der Authentifizierung einer Vorrichtung und damit zu einem auch von der Kryptographie verfolgten Zweck verwendet würden.

19
Ob der private Schlüssel zum Zeitpunkt des Empfangs der Domaininformationen bereits existiere oder erst im Zuge des Erhalts der Domaininformationen erteilt wird, sei für eine patentgemäße Ausführungsform unerheblich. Daher falle auch die Erzeugung eines neuen privaten Schlüssels im Falle der Hinzufügung eines neuen Musikdienstes über ein einem bestehenden Geräteverbund neu hinzugefügtes YY-Gerät in den Anwendungsbereich des Klagepatents. Die Klage erfasse gerade die von der Klägerin als patentverletzend angegriffene Konstellation, in der bereits ein Musikdienst für den fraglichen Haushalt eingerichtet ist und von der neu hinzugefügten angegriffenen Ausführungsform ein weiterer Musikdienst eingerichtet wird. Wenn mittels eines neu hinzugefügten YY-Players ein neuer Musikdienst (z. B. Spotify) hinzugefügt werde und mit der fraglichen Domain bereits andere Musikdienste (z. B. Deezer, Amazon Music) verbunden sind, sei das Klagepatent verletzt. Denn in diesem Fall kontaktiere der neu hinzugefügte YY-Player, gesteuert durch den YY-Controller, den neu hinzuzufügenden, externen Musikdienst, der seinerseits den patentgemäßen privaten Schlüssel in Form des „Authentifizierungs-Tokens“ sowie des „Private Key“ ausstelle, die sodann von der angegriffenen Ausführungsform empfangen werde.

20
Auch beim Erneuern des „AuthToken“ mittels des „Private key“ (sogenannter „RefreshToken“) für einen bereits eingerichteten Musikdienst sende der Musikdienst als externer Schlüsselaussteller an die angegriffene Ausführungsform einen neuen „AuthToken“ und damit einen klagepatentgemäßen privaten Schlüssel.

21

Eine Aussetzung ist nach Auffassung der Klägerin nicht angezeigt. Das Klagepatent sei rechtsbeständig. Von dem seitens der Beklagten vorgelegten Stand der Technik grenze sich die technische Lehre des Klagepatents insbesondere deswegen hinreichend ab, weil die dem Fachmann bekannten Dokumente keine erfindungsgemäße Domain an Vorrichtungen und lediglich gerätespezifische Kennungen, nicht aber domainspezifische Kennungen offenbarten.

22
Die Klägerin b e a n t r a g t:

I. Die Beklagte wird verurteilt,

1. es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzu setzenden Ordnungsgeldes bis zu 250.000,00 € - ersatzweise Ordnungshaft - oder einer Ordnungshaft bis zu sechs Monaten, im Falle wiederholter Zuwiderhandlung bis zu insgesamt zwei Jahren, wobei die Ordnungshaft an den gesetzlichen Vertretern der Beklagten zu vollziehen ist, zu unterlassen:

Geräte in der Bundesrepublik Deutschland anzubieten, in den Verkehr zu bringen, zu gebrauchen oder zu den genannten Zwecken einzuführen oder zu besitzen,

die Folgendes umfassen:

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;

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, wobei der private Schlüssel auf den Domain-Informationen basiert und von allen Vorrichtungen innerhalb der Vorrichtungsdomain verwendet wird.

(EP 1 579 621 B1, Anspruch 9, unmittelbare Verletzung)

2. die unter Ziffer I.1. bezeichneten, in Verkehr gebrachten und im Besitz Dritter befindlichen Erzeugnisse aus den Vertriebswegen zurückzurufen,

indem diejenigen Dritten, denen durch die Beklagte oder mit deren Zustimmung Besitz an den Erzeugnissen eingeräumt wurde, unter Hinweis darauf, dass die Kammer mit dem hiesigen Urteil auf eine Verletzung des Klagepatents erkannt hat, ernsthaft aufgefordert werden, die Erzeugnisse an die Beklagte zurückzugeben und den Dritten für den Fall der Rückgabe der Erzeugnisse eine Rückzahlung des gegebenenfalls bereits bezahlten Kaufpreises sowie die Übernahme der Kosten der Rückgabe zugesagt wird und endgültig zu entfernen, indem die Beklagte die erfolgreich zurückgerufenen Erzeugnisse wieder an sich nimmt.

23
Die Beklagte b e a n t r a g t:

die Klage abzuweisen;

hilfsweise, den Rechtsstreit bis zur rechtskräftigen Entscheidung über die gegen das Klagepatent vor dem Bundespatentgericht erhobene Nichtigkeitsklage der YY Europe B. V. vom 6. November 2020 auszusetzen.

24
Die Beklagte ist der Meinung, dass die angegriffenen Ausführungsformen das Klagepatent nicht verletzen. In ihrer Verletzungsargumentation vermenge die Klägerin das Hinzufügen eines YY-Players zu einem YY-Haushalt und das Hinzufügen eines externen Musikdienstes. Hierbei handele es sich um zwei voneinander unabhängige Prozesse. Die beim erstmaligen Einrichten eines Musikdienstes stattfindende externe Kommunikation einer angegriffenen Ausführungsform mit dem fraglichen Diensteanbieter falle gerade nicht in den Schutzbereich des Klagepatents. Das Klagepatent sei vielmehr beschränkt auf die Hinzufügung eines YY-Players zu einer bestehenden Gruppe von YY-Playern mit einem bereits eingerichteten Musikdienst. Denn nur in einem solchen Szenario würde eine patentgemäße Domain aus Vorrichtungen existieren. Würde indes ein YY-Player zu einem bestehenden Verbund an YY-Playern hinzugefügt, erhalte

dieser den „AuthToken“ und den „Private Key“ nicht von dem externen Musikdienstanbieter, sondern von einem in dem Verbund bereits eingerichteten Player. Damit werde die patentgemäß in funktionaler Hinsicht vorausgesetzte Verbesserung der Sicherheit eines DRM durch Einsatz eines externen Schlüsselausstellers bei der Geräteregistrierung nicht verwirklicht.

25
Eine Verletzung des Klagepatents sei auch deswegen ausgeschlossen, weil ein zu einem YY-Household hinzugefügter YY-Player die „Household-ID“ von dem YYController und nicht von einem anderen Player empfange. Patentgemäß sei vorausgesetzt, dass Domain-Informationen von einer bereits in der Gruppe eingerichteten Vorrichtung und damit einem anderen Player empfangen würden. Bei dem YYController, von dem die YY-Player die „Household-ID“ empfingen, handele es sich nicht um eine patentgemäße Vorrichtung.

26
Einem YY-System hinzugefügte Vorrichtungen würden die Authentifizierungsinformationen eines Musikdienstes von einem in dem Verbund bereits registrierten Player erhalten. In dem Moment, in dem ein YY-Player einer Domain hinzugefügt wird, habe dieser noch keine Rechte erhalten und könne daher nicht als Vorrichtung im Sinne des Klagepatents fungieren. Insoweit fehle es an der Existenz bzw. dem Teilen von Rechten im Zusammenhang mit einem gemeinsamen Konto, wobei es sich bei anspruchsgemäßen Rechten um die digitale Beschreibung der kryptografischen Berechtigungen und Befähigung zum Zugriff auf kryptografisch geschützten Inhalt handele.

27
Patentgemäß sei überdies weiter erforderlich, dass die Verbindungsmittel zwischen einem neu hinzugefügten Gerät und einem in der Domain bereits bestehenden Gerät über eine Kommunikationsverbindung realisiert wird, die den physischen Abstand zwischen den Geräten dahingehend beschränkt, dass der Nutzer die Geräte physisch kontrollieren kann. Die von den YY-Geräten vorgesehene WLAN-Verbindung erfülle diese Voraussetzung nicht.

28
Die angegriffenen Ausführungsformen verfügen nach Ansicht der Beklagten zudem nicht über einen patentgemäßen Logikkreis. Auch insoweit sei zu berücksichtigen, dass das Klagepatent auf das Szenario des Hinzufügens eines Geräts zu einer bestehenden Domain aus Vorrichtungen beschränkt sei. Die von der Klägerin als Verletzung vorgetragene manuelle Einrichtung eines Musikdienstes falle nicht in den Anwendungsbereich des geltend gemachten Anspruchs. In einem YY-Household würde der „AuthToken“ zwischen den registrierten YY-Playern geteilt. Dies steht der Beklagten zu Folge in direktem Widerspruch zu der technischen Lehre des Klagepatents, die auf dem zentralen Gedanken eines von der Domain unabhängigen externen Schlüsselausstellers beruht und ein Teilen von Authentifizierungsinformationen durch Vorrichtungen innerhalb der Domain aus Vorrichtungen entsprechend der patentgemäßen Lösung gerade verhindern will.

29
Zudem müsse es sich bei dem patentgemäß vorausgesetzten privaten Schlüssel um einen kryptographischen Schlüssel handeln. Dieser müsse dem Zweck des Entschlüsselns von digitalem Inhalt dienen. Aus Abs. [0011] der Klagepatentschrift ergebe sich ausdrücklich, dass das Klagepatent die Verwendung eines privaten Schlüssels als Gegenstück zu einem öffentlichen Schlüssels betreffend den Bereich der public key-Kryptographie voraussetze. Auch der relevante Fachmann verstehe den Begriff des privaten Schlüssels im kryptographischen Sinne. Dies werde der Beklagten zufolge über die von ihr vorgelegten Gutachten der Sachverständigen W1. und F. hinaus etwa durch in Auszügen vorgelegte Fachliteratur bestätigt. Dagegen würde der „AuthToken“ ebenso wie der „Private Key“ in einem YY-System nicht wie anspruchsgemäß vorausgesetzt zur Entschlüsselung von digitalem Inhalt verwendet. Bei dem „AuthToken“ handele es sich vielmehr um eine Art „Mitgliedschaftskarte“, die ein Musikdienst einem YY-Player ausstelle, nachdem sich der Nutzer zunächst unter Angabe seines Namens und Passworts über den YY-Controller bei dem Musikdienst angemeldet hat. Bei späterem Abruf des Musikdienstes müsse sich der Nutzer dann nicht mehr mit seinem Benutzernamen und Passwort anmelden, sondern könne sich schlicht mit dem „AuthToken“ identifizieren. Der „AuthToken“ werde daher lediglich wie ein Passwort zum Zwecke der Authentifizierung verwendet. Bei dem im Rahmen eines YY-Systems ausgestellten „Private Key“

handele es sich ebenfalls nicht um einen patentgemäßen privaten Schlüssel. Der „Private Key“ werde nur benötigt, um einen neuen „AuthToken“, etwa im Falle dessen zeitlichen Ablaufs, anzufordern.

30
Auch ein patentgemäßer Logikkreis setze voraus, dass das angegriffene Gerät bei einem bereits eingerichteten Musikdienst einen privaten Schlüssel anfordere. Dies sei bei einem YY-System hinzugefügten Geräten nicht der Fall, weil diese den „AuthToken“ von den im Verbund bereits registrierten Geräten erhielten.

31
Bei Hinzufügen eines neuen Musikdienstes würde der „AuthToken“ zwar bei dem externen Diensteanbieter angefordert. Allerdings würde der Token zu diesem Zeitpunkt gerade noch nicht von den anderen Playern in dem bestehenden YY-System verwendet. Die Erzeugung eines neuen Schlüssels falle aber nicht in den Schutzbereich des Klagepatents. Dieses setze vielmehr voraus, dass einem neu zu registrierenden Gerät ein bereits existierender privater Schlüssel ausgestellt wird.

32
Die nach Behauptung der Klägerin in einem YY-Player vorgesehene Möglichkeit der Wiedergabe verschlüsselter Inhalte habe nichts mit der dem Klagepatent entsprechend vorgesehenen Verwendung eines privaten Schlüssels zu tun. Im Gegensatz zu der patentgemäßen Lösung verfügten YY-Player über einen individuellen, gerätespezifischen und damit nicht domainbezogenen privaten Schlüssel. Jeder YY-Player erzeuge ein individuelles Geräte-Zertifikat, das einen mit dem privaten Schlüssel korrespondierenden, öffentlichen Schlüssel enthalte. Das Geräte-Zertifikat würde an einen Musikdienst gesendet, woraufhin der jeweilige YY-Player von dem Musikdienst einen gerätespezifischen „Session-Token“ erhalte, der für die jeweilige Wiedergabe gültig sei.

33
Soweit die Beklagte die Aussetzung des Verletzungsrechtsstreits hilfsweise begehrt, nimmt sie auf ihre im Rahmen der vor dem Bundespatentgericht anhängigen Nichtigkeitsklage vorgelegten, dem relevanten Fachmann nach ihrer Behauptung aus dem Stand der Technik bekannten Dokumente Bezug. Insbesondere das als Entgegenhaltung D1 vorgelegte Dokument US 2002/0166047 A1 nehme die technische Lehre des Klagepatents in neuheitsschädlicher Weise vorweg. Dabei werde in dessen Abs. [0041] auch das Teilmerkmal des Empfangs von Domain-Informationen über eine Kurzstreckenverbindung offenbart. Zudem offenbare der als Entgegenhaltung D13 vorgelegte „Proposal for DVB Content Protection & Copy Management Technologies Version 1.0“ des Unternehmens Nokia sämtliche Merkmale der klagepatentgemäßen Lehre.

34
Am 21.04.2021 hat die Kammer zur Sache verhandelt. Im Anschluss an die mündliche Verhandlung argumentierte die Klägerin in ihrem nicht nachgelassenen Schriftsatz vom 28.05.2021 erstmalig, dass die Kennungen „AuthToken“ und „Private key“ in einen kryptographischen Algorithmus Eingang fänden. Die angegriffenen Ausführungsformen würden diese Kennungen bei Anfragen nach geschütztem digitalen Inhalt an den Musikdienst in Kopfzeilen („Header“) mitsenden. Dabei folge das Einfügen der Kennungen in den Header und die entsprechende Authentifizierung einer formal festgelegten Vorgehensweise, nach der eine definierte Aufgabe (Authentifizierung) gemäß einem strukturierten Schema (Einfügen der Schlüssel in den Header und Abgleich der Schlüssel beim Musikdienst) gelöst würde. Ohne die Kenntnis des Algorithmus könnte dessen Ergebnis in Form der Bestätigung, dass eine Nachricht von einem autorisierten Gerät gesendet wurde, nicht errechnet werden.

35
Zur Ergänzung des Tatbestandes wird auf die zwischen den Parteivertretern gewechselten Schriftsätze nebst Anlagen sowie das Protokoll zur mündlichen Verhandlung vom 21.04.2021 verwiesen.

Entscheidungsgründe

36
Die Klage ist zulässig, in der Sache jedoch unbegründet. Der Klägerin stehen die geltend gemachten Ansprüche nicht zu. Auf der Grundlage der Ausführungen der Klägerin vermag die Kammer eine Verletzung des Klagepatents letztlich nicht zu bejahen.

37
I. 1. Das Klagepatent betrifft ein domaingestütztes digitales Rechtemanagement system mit leichter und sicherer Geräteregistrierung. Digitale Rechtemanagementsysteme waren im Prioritätszeitpunkt dem Grunde nach bereits bekannt. Diese basierten auf der Erkenntnis des Problems, dass digitale Inhalte wie Musik, Spiele, Filme, Bilder und Bücher auf einfache Weise kopiert werden können. Ihrem Sinn und Zweck nach dienen digitale Rechtemanagementsysteme daher gemäß Abs. [0002] der Klagepatentschrift dazu, Sicherheitsmaßnahmen zur Bekämpfung von Produktpiraterie vorzusehen, um so eine angemessene Vergütung von Inhabern digitaler Inhalte sicherzustellen. Entsprechende Sicherungsmaßnahmen sollten, wie dem Fachmann bereits im Prioritätszeitpunkt bekannt war, durch manipulationssichere elektronische Geräte umgesetzt werden.

38
Zu den im Prioritätszeitpunkt bekannten digitalen Rechtemanagementsystemen zählt das Klagepatent das Teilen digitaler Inhalte innerhalb einer Domain an Geräten. Ein solcher Geräteverbund kann beispielsweise eine einheitliche Zahlungsmethode oder eine übereinstimmende Kontonummer verwenden. Bezahlt sodann ein Nutzer für die einmalige Nutzung eines bestimmten Werkes wie etwa eines Films unter Verwendung der domainspezifischen Kontodaten, gilt das Gerät als zu der fraglichen Domain gehörig autorisiert und kann das gewünschte Werk sodann nutzen. Allerdings kann in einem solchen Fall nur ein Gerät auf die gewünschten Inhalte zugreifen. Sobald ein Zugriff über ein Gerät erfolgt, ist ein Zugriff über die weiteren Geräte aus der jeweiligen Domain ausgeschlossen (Abs. [0003] der Klagepatentschrift).

39
Das Klagepatent erkennt ein solches Vorgehen als prinzipiell vorteilhaft an, weist indes auf zwei sich hieraus ergebende Problemstellungen hin (Abs. [0004] und [0021] der Klagepatentschrift): Zum einen mussten im Stand der Technik alle Geräte einzeln registriert werden, was das Klagepatent als für den Nutzer aufwändig kritisiert. Zum anderen ergibt sich ein Sicherheitsrisiko, wenn Nutzer Geräte per Fernzugriff über weite Distanz in einer Domain registrieren.

40
Als dem Fachmann aus dem Stand der Technik bekannte Lösungsansätze verweist das Klagepatent in dessen Abs. [0005] auf den Standardisierungsvorschlag „IBM Response to DVB-CPT Call for Proposal for Content Protection & Copy Management: xCP Cluster Protocol“ vom 19.10.2001. Hierin wird ein Rechtemanagementsystem beschrieben, das Nutzern den nahtlosen Zugang zu digitalen Inhalten inner- und außerhalb ihres Zuhauses bei gleichzeitigem Schutz der Rechte der Inhalteanbieter ermöglicht. Dazu bilden die in einem solchen Heimnetzwerk verbundenen Geräte ein einheitliches Cluster innerhalb einer verschlüsselten Domain. In diesem Cluster gelten alle Geräte als gleichberechtigt, auch wenn diese jeweils spezifische Funktionen erfüllen. Dabei können bestimmte mit Authorisierungsfunktion ausgestattete Geräte einzelne Geräte in das Cluster aufnehmen, wobei sie entweder selbständig oder stellvertretend für ein externes Authorisierungszentrum agieren.

41
In dem dem Fachmann im Prioritätszeitpunkt ebenfalls bereits bekannten USamerikanischen Anmeldedokument US 2002/157002 wird ein domainbasiertes digitales Rechtemanagementsystem beschrieben (Abs. [0006] der Klagepatentschrift). Einer Domain sind dabei ein oder mehrere Geräte zugeordnet, die einen von der Domain verwendeten, gemeinsamen kryptographischen Schlüssel teilen. Registrierung und Abmeldung eines Gerätes erfolgt über eine zuständige Domainstelle („domain authority“) in Verbindung mit einem in dem Gerät verbauten DRM-Modul.

42
Entsprechende, aus dem Stand der Technik bekannte digitale Rechtemanagementsysteme stellen unter dem Gesichtspunkt der Nutzerfreundlichkeit eine vorteilhafte Weiterentwicklung dar. Denn sowohl die Clusterbasierte als auch die Domainbasierte Geräteregistrierung ermöglichen es dem Nutzer im Umfeld eines digitalen Rechtemanagementsystems, Geräte in vereinfachter Weise zu registrieren, da nutzerseitig anstelle der für jedes zu verwendende Gerät einzugebenden, gerätespezifischen Informationen lediglich eine domainspezifische Registrierung erfolgen muss. Als weiter nachteilhaft bezeichnet das Klagepatent indes den nutzerseitig bestehenden Aufwand, jedes Gerät unter Eingabe der domainspezifischen Informationen in der jeweiligen Domain registrieren zu müssen (Abs. [0021] der Klagepatentschrift). Zudem kritisiert das Klagepatent den Stand der Technik unter Sicherheitsgesichtspunkten, weil so auch Geräte,

über die der Nutzer keine unmittelbare physische Kontrolle hat, in einfacher Weise zur gemeinsamen Rechtenutzung registriert werden können (Abs. [0008] der Klagepatentschrift). Dahingehende Sicherheitsbedenken bestehen dem Klagepatent insbesondere bei einer über das Internet oder per EMail erfolgenden Geräteregistrierung (Abs. [0031] der Klagepatentschrift).

43
2. An diesen Stand der Technik knüpft das Klagepatent gemäß Abs. [0008] der Klagepatentschrift an, indem ein Verfahren sowie eine Vorrichtung für ein digitales Rechtemanagementsystem offenbart wird, welches eine zugleich einfache, weil domainbasierte, und sichere Registrierung von Geräten ermöglicht. Dabei ist es dem Klagepatent zufolge vorzugswürdig, wenn sich die zu registrierende Vorrichtung in unmittelbarer Nähe zu den in der Domain bereits vorhandenen Vorrichtungen befindet.

44
Eine weitere Vereinfachung der Geräteregistrierung will das Klagepatent vor dem Hintergrund erreichen, als es für Nutzer beschwerlich ist, einmal festgelegte Domaininformationen wie den Domainnamen und das Domainpasswort zu erinnern und erneut einzugeben, wenn neue Geräte zu einer bestehenden DRM-Domain hinzugefügt werden. Gemäß Abs. [0009] der Klagepatentschrift wird es in zwei Konstellationen als in besonderem Maße schwierig bezeichnet, Geräte zu registrieren: Zum einen, nachdem seit der Registrierung eines ersten Gerätes längere Zeit verstrichen ist und zum anderen, wenn es um die Registrierung von Geräten mit eingeschränkter Benutzeroberfläche geht. Eine vereinfachte Geräteregistrierung sieht gemäß Abs. [0010] daher vor, dass die relevanten DRM-Informationen von einem in der bestehenden Domain bereits registrierten Gerät empfangen werden.

45
An dieser vereinfachten Registrierung durch Empfang der DRM-Informationen von einem bereits in einer Domain registrierten Gerät kritisiert das Klagepatent indes, dass hierdurch digitale Inhalte nicht ausreichend geschützt sind (Abs. [0010]). Als Maßnahme zur Verbesserung der Sicherheit schlägt das Klagepatent daher den Einsatz eines Schlüsselausstellers vor, um die Geräteregistrierung abschließen zu können. Dieser kann gemäß Abs. [0010] der Klagepatentschrift die Geräteregistrierung aktiv durchsetzen und so die Sicherheit erhöhen. Weiter soll die Sicherheit dadurch erhöht werden, dass das neu zu registrierende Geräte DRM-Informationen nur über eine Kurzstreckenverbindung von der bestehenden Domain empfangen kann (Abs. [0010]).

46
Der angesprochene Fachmann entnimmt der Klagepatentschrift den Abs. [0008] bis [0010] und gleichfalls den entsprechenden Beschreibungsstellen in Abs. [0022] und [0023] sowie Abs. [0031] und [0032] der Klagepatentschrift daher, dass die Sicherheit digitaler Inhalte zum einen dadurch geschützt werden soll, dass Domaininformationen über eine Kurzstreckenverbindung empfangen werden und zum anderen ein Schlüsselaussteller eingesetzt wird. Die Bedeutung des Einsatzes eines Schlüsselausstellers erkennt der Fachmann dabei darin, dass die Geräte anderenfalls - d.h. wenn ein Schlüsselaussteller nicht eingesetzt würde - private DRM-Schlüssel teilen und DRMZertifikate ausstellen müssten (Abs. [0032] des Klagepatentschrift).

47
3. Vor diesem Hintergrund und unter Berücksichtigung des dem Klagepatent zu Grunde liegenden Standes der Technik stellt sich das Klagepatent die Aufgabe, ein domainbasiertes, digitales Rechtemanagementsystem anzubieten, welches die Hinzufügung neuer Geräte auf einfache und zugleich sichere Weise ermöglicht.

48
Zur Lösung dieser Aufgabe schlägt das Klagepatent gemäß dem mit der Klage geltend gemachten Vorrichtungsanspruch 9 ein Gerät vor, das mit einem Kommunikationsschaltkreis, einem Speicher und einem Logikschaltkreis über drei zentrale Bestandteile verfügt. Im Einzelnen lässt sich der geltend gemachte Vorrichtungsanspruch wie nachfolgend dargestellt gliedern. Die Kammer nimmt dabei Bezug auf die Merkmalsgliederung der Klägerin, da sich diese unmittelbar auf den für die Auslegung primär maßgeblichen Anspruchswortlaut stützt:

9 Gerät, das Folgendes umfasst:

9.1 einen Kommunikationskreis (213) zum Empfangen, über eine Kurzstrecken-Verbindung (108), von Domain-Informationen (209) von einer Vorrichtung (101), 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 (100);

9.2 einen Speicher (211) zum Speichern der Domain-Informationen (209); und

9.3 einen Logikkreis (210) zur Bereitstellung der Domain-Informationen (209) für einen Schlüsselaussteller (105), der unabhängig von der Vorrichtungsdomain ist, wodurch der Schlüsselaussteller (105) einen privaten Schlüssel (206) zur Verwendung bei Zugriff auf geschützten digitalen Inhalt (204) für das Gerät ausstellt,

9.3.1 wobei der private Schlüssel (206) auf den Domain-Informationen (209) basiert und

9.3.2 von allen Vorrichtungen (101) innerhalb der Vorrichtungsdomain verwendet wird.

49

4. Der geltend gemachte Anspruch lehrt damit ein sich im Wesentlichen aus drei Bestandteilen zusammensetzendes Gerät, über welches im Rahmen eines digitalen Rechtemanagementsystems auf digitale Inhalte wie Musik, Filme, Bücher o.ä. zugegriffen wird. Die einzelnen Bestandteile einer anspruchsgemäßen Vorrichtung werden in funktionaler Hinsicht jeweils näher beschrieben. Figur 1 des Klagepatents veranschaulicht die Rolle einer anspruchsgemäßen Vorrichtung (101) im Rahmen eines klagepatentgemäßen digitalen Rechtemanagementsystems (100):

50

Als anspruchsgemäße Vorrichtung (101) zur Nutzung digitaler Inhalte eines Rechteinhabers (103) kommen u.a. insbesondere Computer und Mobiltelefone in Betracht, die etwa über einen darin verbauten MP3-Player Musik abspielen können (Abs. [0012] der Klagepatentschrift). Weitere Bestandteile eines erfindungsgemäßen Rechtemanagementsystems sind ein Schlüsselaussteller (105), ein Netzwerk (107) sowie eine Kurzstrecken-Verbindung (108). Die Kommunikation zwischen einer anspruchsgemäßen Vorrichtung und dem Rechteinhaber (103) erfolgt dabei über das Netzwerk (107), bei dem es sich patentgemäß beispielsweise um ein Mobilfunknetz, ein lokales Netzwerk (LAN) oder ein Wide Area Network (WAN) handeln kann (Abs. [0016] der Klagepatentschrift). Die seitens des Nutzers verwendeten Vorrichtungen kommunizieren dagegen anspruchsgemäß über eine Kurzstrecken-Verbindung (108) miteinander, um auf Grund der damit verbundenen physischen Nähe der Geräte und der damit einhergehenden, besseren Kontrollierbarkeit die Gefahr von Hackerangriffen zu verringern (Abs. [0010], [0013] und [0022] der Klagepatentschrift).

51

Eine weitere Verbesserung der Sicherheit eines Rechtemanagementsystems soll dem Klagepatent zu Folge über den Einsatz des Schlüsselausstellers (105) erreicht werden. Gemäß Abs. [0014] der Klagepatentschrift handelt es sich bei dem Schlüsselaussteller um eine Anwendung, die eine authentifizierte Kommunikation mit Benutzergeräten ermöglicht und diesen ein DRM-Zertifikat sowie einen privaten DRM-Schlüssel zur Verfügung stellt. Eine authentifizierte Kommunikation erfolgt auf der Grundlage eines sogenannten Challenge-Response Protokolls, über das ein von dem Gerätehersteller installiertes Gerätezertifikat (207) und die Domaininformationen (209) ausgetauscht werden. Das auf dieser Grundlage sodann von dem Schlüsselaussteller ausgestellte DRM-Zertifikat (202) beinhaltet neben der gerätespezifischen Kennung wie etwa einer der Vorrichtung spezifisch zugewiesenen Serien- oder Modellnummer einen öffentlichen DRM-Schlüssel und eine von dem Schlüsselaussteller hergestellte, digitale Signatur (Abs. [0015] der Klagepatentschrift). Der dem öffentlichen DRMSchlüssel entsprechende private DRM-Schlüssel (206) wird sicher in dem Speicher (211) der Vorrichtung (101) abgelegt. Figur 2 des Klagepatents illustriert die im geltend gemachten Patentanspruch beschriebenen drei Bestandteile einer patentgemäßen Vorrichtung (101) wie folgt:

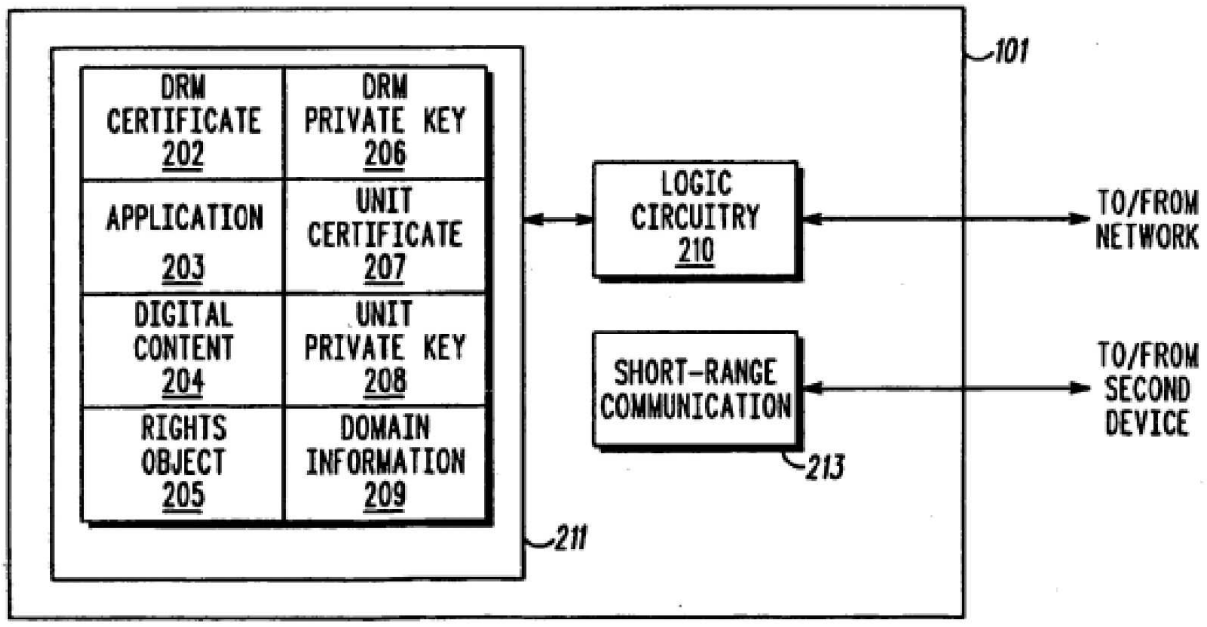

FIG. 2

52
5. Näher erläuterungsbedürftig sind die zwischen den Parteien umstrittenen Merk malsgruppen 9.1 und 9.3. Von zentraler Bedeutung sind dabei aus Sicht der Kammer die folgenden, zwischen den Parteien streitig diskutierten Fragen:

- Zum Ersten die Frage, ob die in den angegriffenen Ausführungsformen vorhandene WLAN-Schnittstelle den Aufbau einer patentgemäßen Kurzstreckenverbindung ermöglicht (Merkmalsgruppe 9.1);

- Zum Zweiten die Frage, ob der geltend gemachte Patentanspruch auch das Ausstellen eines neuen Schlüssels für neue digitale Inhalte, die für eine bestehende Domain über ein dieser neu hinzugefügtes Gerät hinzuerworben wurden, erfasst (Merkmalsgruppe 9.3); und

- Zum Dritten die Frage, wie ein patentgemäßer privater Schlüssel ausgestaltet sein muss, insbesondere, ob ein solcher kryptographischer Natur sein muss (Merkmalsgruppe 9.3).

53
a. In rechtlicher Hinsicht gilt für die Auslegung folgender Maßstab:

54
aa. Ziel der Auslegung des geltend gemachten Patentanspruchs ist es, dessen Sinngehalt aus Sicht des von dem streitgegenständlichen Patent angesprochenen Durchschnittsfachmanns im Prioritätszeitpunkt zu ermitteln. Nach Ansicht der Kammer ist relevanter Fachmann vorliegend ein Universitätsabsolvent (Diplom oder Master) der Fachrichtung Informatik mit Kenntnissen auf dem Gebiet der Kryptographie und mehrjähriger Berufserfahrung im Bereich der Entwicklung digitaler Rechtemanagementsysteme (vgl. BPatG Beschluss vom 24.10.2017, Az. 23 W (pat) 24/17, BeckRS 2017, 133838).

55
Maßgeblich für die Bestimmung des relevanten Fachmanns ist der technische Gegenstand des streitgegenständlichen Patents. Das Klagepatent betrifft ein computergestütztes und damit typischerweise von Absolventen der Fachrichtung Informatik entwickeltes, digitales Rechtemanagementsystem (vgl. etwa Abs. [0012] und [0021] der Klagepatentschrift), das in einem - wie ausgeführt - zentralen Aspekt auf dem Einsatz eines Schlüsselausstellers beruht. Seinem Abs. [0011] zufolge ist die technische Lehre des Klagepatents vor dem Hintergrund bestimmter, ausdrücklich genannter Erkenntnissen aus dem Bereich der Kryptographie zu verstehen.

56
bb. Grundlage der aus Sicht des Fachmanns vorzunehmenden Auslegung ist primär der Offenbarungsgehalt der Patentansprüche und ergänzend - im Sinne einer Auslegungshilfe - der Offenbarungsgehalt der Patentschrift, soweit dieser in den Patentansprüchen Niederschlag gefunden hat.

Die Patentschrift ist dabei maßgebend für das Verstehen der Erfindung. Sie legt den Inhalt der darin verwendeten Begriffe fest und stellt damit gleichsam ihr eigenes Lexikon dar (st. Rspr.; statt vieler: BGH, GRUR 1999, 909, 912 - Spannschraube).

57
Die zur Ermittlung des Offenbarungsgehalts eines Patentanspruchs notwendige Auslegung dient dazu, die technische Lehre des Klagepatents zu erfassen, wie sie aus fachmännischer Sicht - d.h. unter Berücksichtigung des Vorverständnisses, das sich aus dem Fachwissen und Fachkönnen des von der Erfindung angesprochenen Fachmanns ergibt - mit dem Wortlaut des Anspruchs zum Ausdruck gebracht wird. Entscheidend ist damit eine funktionale Auslegung der Schutzansprüche und der darin verwendeten Begriffe, um deren technischen Sinn unter Berücksichtigung von Aufgabe und Lösung, wie sie sich objektiv aus dem Klagepatent ergeben, zu bestimmen (BGH, BeckRS 2015, 19864, Rn. 16 - Luftkappensystem). Maßgeblich sind insoweit der Sinngehalt eines Patentanspruchs in seiner Gesamtheit und der Beitrag, den die einzelnen Merkmale zum Leistungsergebnis der geschützten Erfindung beitragen. Aus der Funktion der einzelnen Merkmale im Kontext des Patentanspruchs ist abzuleiten, welches technische Problem diese Merkmale für sich und in ihrer Gesamtheit tatsächlich lösen (BGH, a.a.O.; GRUR 2012, 1124, 1126, Rn. 27 - Polymerschaum). Der Patentanspruch bildet eine Einheit, so dass die technischen Merkmale nicht rein isoliert betrachtet und unabhängig voneinander ausgelegt werden dürfen (BGH, GRUR 2011, 129, 131, Rn. 29 - Fentanyl-TTS). Daher gilt es, im Rahmen der Auslegung die patentierte Erfindung einheitlich zu erfassen (BGH, GRUR 2004, 1023, 1025 - Bodenseitige Vereinzelungseinrichtung). Die Patentschrift ist folglich in einem sinnvollen Zusammenhang zu lesen und ihr Gesamtinhalt im Zweifel so zu verstehen, dass sich Widersprüche nicht ergeben (BGH, BeckRS 2015, 13347, Rn. 22 - Kreuzgestänge; GRUR 2015, 159, 161, Rn. 31 - Zugriffsrechte; GRUR 2011, 701, 703, Rn. 24 - Okklusionsvorrichtung).

58
Ergeben sich indes unauflösbare Widersprüche zwischen der technischen Lehre der Beschreibung und der technischen Lehre der Schutzansprüche, ist der Patentanspruch maßgeblich (BGH, BeckRS 2015, 13347, Rn. 22 - Kreuzgestänge; GRUR 2011, 701, 703, Rn. 23 a.E. - Okklusionsvorrichtung). Im Rahmen der Auslegung dürfen Beschreibung und Zeichnungen zudem weder zu einer inhaltlichen Erweiterung noch zu einer sachlichen Einengung des durch den Wortsinn des Patentanspruchs festgelegten Schutzgegenstandes führen (BGH, GRUR 2011, 701, 703, Rn. 23 a.E. - Okklusionsvorrichtung; GRUR 2010, 602, 605, Rn. 27 - Gelenkanordnung). Soweit sich indes die Beschreibung als Erläuterung des Gegenstands des Patentanspruchs lesen lässt, ist sie zur Bestimmung des Schutzbereichs eines Patents zu berücksichtigen (BGH, GRUR 2011, 701, 703, Rn. 23 a.E. - Okklusionsvorrichtung).

59
Als übergreifenden Gesichtspunkt hat die Auslegung schließlich neben dem Gesichtspunkt eines angemessenen Schutzes der erfinderischen Leistung das gleichgewichtig danebenstehende Gebot der Rechtssicherheit zu beachten (BGH, GRUR 2007, 1059, 1062, Rn. 25 - Zerfallszeitmessgerät; vgl. auch GRUR 2004, 1023, 1025 - Bodenseitige Vereinzelungseinrichtung).

60
b. Vor diesem Hintergrund ist nach Auffassung der Kammer die Frage, ob eine WLAN-Schnittstelle den Aufbau einer anspruchsgemäßen Kurzstreckenverbindung im Sinne von Merkmalsgruppe 9.1 ermöglicht, im Ergebnis zu bejahen. Gemäß Abs. [0013] der Klagepatentschrift handelt es sich bei WLANVerbindungen um Kurzstreckenverbindungen im Sinne des Klagepatents. Dem angesprochenen Fachmann ist dabei bewusst, dass es sich bei dem Kürzel „802.11“ um die Bezeichnung der von der Standardisierungsorganisation IEEE verwalteten WLAN-Standardspezifikation handelt.

61
Die Argumentation der Beklagten, wonach der zuständige Patentprüfer im Erteilungsverfahren vor dem Europäischen Patentamt gemäß dem als Anlage EIP B4-NK6 vorgelegten E-Mail vom 06.03.2012 zu erkennen gegeben habe, dass WLAN als Kurzstreckenverbindung nicht in Betracht komme, greift aus Sicht der Kammer nicht durch. Dabei kann dahinstehen, ob die im Rahmen des Erteilungsverfahrens erfolgte Äußerung des Prüfers überhaupt als zulässiges Auslegungsmittel in Betracht kommt (für eine Berücksichtigung als einem technischen Fachlexikon vergleichbares Mittel etwa OLG Düsseldorf, GRUR-RS 2016, 11229; für eine indizielle Berücksichtigung zur Bestätigung der auf andere Gesichtspunkte gestützten Auslegung BGH, GRUR 2016, 921, Rn. 40 - Pemetrexed).

62
Das Schreiben des Prüfers vom 03.04.2012 lässt bereits seinem Inhalt nach keinen hinreichend sicheren Schluss zu, dass WLAN-Verbindungen explizit als Kurzstreckenverbindungen ausgeschlossen sind. Das Schreiben diente vielmehr als Hinweis darauf, dass die angemeldete, patentgemäße Lehre nach Ansicht des zuständigen Prüfers weder neu noch erfinderisch ist. Neuheit und erfinderische Tätigkeit könnten nur bejaht werden, wenn die Verwendung einer Kurzstreckenverbindung in den Anspruch aufgenommen würde. Lediglich am Rande wird in dem Schreiben zugleich erwähnt, dass mit dem Verwenden von „wireless LAN, Internet, etc." kein Beitrag zur Erhöhung der Sicherheit geleistet würde. Dennoch definiert das Klagepatent dann aber in Abs. [0013] seiner schlussendlich erteilten Fassung die Verwendung von WLAN als patentgemäße Kurzstreckenverbindung. Insoweit muss es nach Ansicht der Kammer daher für die Frage der Patentverletzung bei dem Grundsatz verbleiben, dass das Patent als sein eigenes Lexikon die Bedeutung der anspruchsgemäß vorausgesetzten technischen Merkmale festlegt (BGH, GRUR 1999, 909, 912 - Spannschraube).

63
c. Die Frage, ob der geltend gemachte Patentanspruch auch das Ausstellen eines neuen Schlüssels für neue digitale Inhalte erfasst, die für eine bestehende Domain über ein dieser neu hinzugefügtes Gerät hinzuerworben wurden, ist hingegen nach Ansicht der Kammer zu verneinen. Merkmalsgruppe 9.3 setzt voraus, dass der externe Schlüsselaussteller dem zu einer bestehenden Domain neu hinzutretenden Gerät einen privaten Schlüssel für bereits vorhandene digitale Inhalte ausstellt. Die oben zusammengefassten Auslegungsmaßstäbe zu Grunde gelegt ist der Schutzbereich des geltend gemachten Patentanspruchs der Überzeugung der Kammer nach auf den Funktions- und Wirkungszusammenhang der Hinzufügung einer neuen Vorrichtung zu einer bestehenden Domain zur Nutzung bereits vorhandener Inhalte beschränkt. Ein anspruchsgemäßes Gerät im Sinne des geltend gemachten Vorrichtungsanspruchs 9 muss daher so eingerichtet und programmiert sein, dass die patentgemäß vorausgesetzten Merkmale gerade auch in diesem spezifischen Funktions- und Wirkungszusammenhang verwirklicht werden. Der angesprochene Fachmann versteht die dem Vorrichtungsanspruch 9 zu Grunde liegende technische Lehre dahingehend, dass diesem eine einheitliche Erfindung zu Grunde liegt, deren wesentlicher erfinderischer Gedanke darin besteht, für den Fall eines Hinzufügens eines zusätzlichen Gerätes zu einem bestehenden Verbund an Geräten eine einfache und zugleich sichere Möglichkeit der Geräteregistrierung bereitzustellen, um gerade auch über dieses neu hinzutretende Gerät bereits bestehende Inhalte nutzen zu können. Dieses Verständnis ist im Wortlaut des geltend gemachten Vorrichtungsanspruchs 9 angelegt (nachfolgend lit. aa.), wird durch die Beschreibung bestätigt (nachfolgend lit. bb.) und entspricht nicht zuletzt der objektiven Aufgabe des Klagepatents (nachfolgend lit. cc.). Vor diesem Hintergrund machen die angegriffenen Ausführungsformen von der erfindungsgemäßen Lehre keinen Gebrauch. Die Klägerin hat nicht dargelegt, dass die angegriffenen Ausführungsformen in dem patentgemäß vorausgesetzten Zweck- und Wirkungszusammenhang der Verwendung einer neuen Vorrichtung zur Nutzung vorhandener digitaler Inhalte den privaten Schlüssel von dem externen Schlüsselaussteller erhalten (nachfolgend lit. dd.).

64
aa. Gemäß Merkmalsgruppe 9.3 setzt ein anspruchsgemäß ausgestaltetes Gerät einen Logikkreis voraus, der aus Sicht des angesprochenen Fachmanns geeignet sein muss, die im Anspruchswortlaut ausdrücklich genannten Funktionen zu erfüllen. Insbesondere muss der Logikkreis die über den Kommunikationskreis gemäß Merkmalsgruppe 9.1 erhaltenen Domain-Informationen einem externen Schlüsselaussteller weiterleiten, der sodann der neu zu registrierenden Vorrichtung einen in der entsprechenden Domain bereits verwendeten privaten Schlüssel zur Nutzung vorhandener Inhalte ausstellt.

65
(1) Im Ausgangspunkt zu Recht weist die Klägerin in diesem Zusammenhang darauf hin, dass bei einem wie hier geltend gemachten Sachpatent der Aufnahme von Zweck-, Wirkungs- und Funktionsangaben in den Patentanspruch im Regelfall keine schutzbereichsbeschränkende Wirkung zukommt, so dass es sich bei der Prüfung der Patentverletzung grundsätzlich erübrigt, Erwägungen darüber anzustellen, ob identisch vorhandene Merkmale demselben Zweck dienen und dieselbe Wirkung und Funktion haben wie diejenigen des Klagepatents, wenn eine Ausführungsform von den Merkmalen eines Vorrichtungsanspruchs in deren räumlichkörperlicher Ausgestaltung identisch Gebrauch macht (BGH, GRUR 2009, 837, 838, Rn. 15 - Bauschalungsstütze; BGH, GRUR 2006, 570, 573, Rn. 21 - extracoronales Geschiebe; BGH, GRUR 1991, 436, 441 - Befestigungsvorrichtung II). Gleiches gilt nach Ansicht der Kammer, wenn wie im Rahmen des

vorliegenden Vorrichtungsanspruchs zugleich verfahrensbezogene Merkmale in Bezug genommen sind. Auf diesen Fall sind die zu Zweck-, Wirkungs- und Funktionsangaben entwickelten Rechtsprechungsgrundsätze entsprechend anzuwenden. Daher ist im Grundsatz davon auszugehen, dass eine in räumlichkörperlicher Hinsicht anspruchsgemäß gestaltete Vorrichtung unabhängig davon geschützt ist, in welchem Funktions- und Wirkungszusammenhang diese verwendet wird (vgl. Loth in Fitzner/Lutz/Bodewig, BeckOK Patentrecht, 19. Edition, Stand 15.01.2021, Rn. 290).

66
Keine hinlängliche Berücksichtigung findet in der von der Klägerin vertretenen Auslegung indes, dass - wie sich aus der zu Zweck-, Wirkungs- und Funktionsangaben entwickelten Rechtsprechung weiter ergibt - der durch das Klagepatent geschützte Gegenstand so ausgebildet sein muss, dass er für den im Anspruch angegebenen Zweck verwendbar ist bzw. die im Anspruch angegebene Funktion erfüllen kann (BGH, BeckRS 2008, 15268, Rn. 17 - Tintenpatrone; BGH, GRUR 2009, 837, 838, Rn. 15 - Bauschalungsstütze; BGH, BeckRS 2010, 00634, Rn. 12 - Hundefutterbeutel). Fordert der Patentanspruch die Eignung der geschützten Vorrichtung, einen bestimmten Vorgang ausführen zu können, und benennt er weiter ein Mittel, über das diese Eignung erreicht werden soll, ist der Patentanspruch im Zweifel dahin auszulegen, dass das Mittel dazu vorgesehen ist und dementsprechend geeignet sein muss, an dem Vorgang, wenn er ausgeführt wird, in erheblicher Weise mitzuwirken (BGH, GRUR 2020, 159, 161, Rn. 18 - Lenkergetriebe). Im Patentanspruch enthaltene Zweck-, Wirkungs- oder Funktionsangaben sind daher nicht schlechthin bedeutungslos. Sie können vielmehr als Bestandteile des Patentanspruchs an dessen Aufgabe teilnehmen, den geschützten Gegenstand zu bestimmen und damit zugleich zu begrenzen, wenn sie das Vorrichtungselement, auf das sie sich beziehen, als ein solches definieren, das so ausgebildet sein muss, dass es die betreffende Funktion erfüllen kann (BGH, GRUR 2018, 395, 397, Rn. 18 - Wasserdichter Lederschuh; BGH, GRUR 2012, 475, 476 - Elektronenstrahltherapiesystem; BGH, GRUR 2006, 923, 925, Rn. 15 - Luftabscheider für Milchsammelanlage). Übertragen auf einen Vorrichtungsanspruch, der einen bestimmten Funktions- und Wirkungszusammenhang voraussetzende Verfahrensschritte beinhaltet, bedeutet dies, dass die Vorrichtung gerade in dem definierten Funktions- und Wirkungszusammenhang geeignet sein muss, die patentgemäß vorausgesetzten Verfahrensschritte auch in entsprechend funktionsgemäßer Weise durchzuführen.

67
Die Kammer vermag der Klägerin vor diesem Hintergrund nicht zu folgen, wenn sie maßgeblich aus der Eigenart des geltend gemachten Anspruchs als Vorrichtungsanspruch ableiten möchte, dass es für eine patentgemäße Ausführungsform nicht darauf ankommen soll, ob diese so gestaltet, d.h. im vorliegenden technischen Kontext so programmiert ist, im Falle der Verwendung zur Nutzung bereits erworbener digitaler Inhalte den in der bestehenden Vorrichtungsdomain des Nutzers bereits genutzten privaten Schlüssel von dem externen Schlüsselaussteller zu erhalten. Vielmehr ergibt die Auslegung, dass die Reichweite des Schutzanspruchs durch den Zweck- und Wirkungszusammenhang der Hinzufügung einer neuen Vorrichtung zur Nutzung auch von bestehenden Inhalten begrenzt ist.

68
(2) Ausgehend vom Anspruchswortlaut gibt die Merkmalsgruppe 9.3 in funktionaler Hinsicht vor, dass der vorausgesetzte Logikkreis dazu dient, einem unabhängig von der Vorrichtungsdomain bestehenden, externen Schlüsselaussteller Domain-Informationen bereitzustellen. Die Bereitstellung der Domain-Informationen ist weiter durch eine dahingehende Wirkungsangabe definiert, dass hierdurch der Schlüsselaussteller dazu veranlasst wird, einen privaten Schlüssel zur Verwendung bei Zugriff auf geschützten digitalen Inhalt für das Gerät auszustellen. Dabei muss der von dem externen Schlüsselaussteller dem Gerät ausgestellte private Schlüssel gerade auf den Domain-Informationen, die das Gerät gemäß Merkmalsgruppe 9.1 von einem in der Domain bereits vorhandenen Vorrichtung erhalten hat, basieren und von allen Vorrichtungen innerhalb der Vorrichtungsdomain verwendet werden.

69
Die höchstrichterlichen Vorgaben zufolge gebotene, einheitliche Betrachtung der patentgemäßen Lehre bedingt hierbei, dass vorliegend im Rahmen der Merkmalsgruppe 9.3 kein anderes Szenario als in Merkmalsgruppe 9.1 beansprucht sein kann. In beiden Merkmalsgruppen ist vorausgesetzt, dass die jeweils entscheidenden Informationen und Daten (gemäß Merkmal 9.1 die Domain-Informationen und gemäß Merkmal 9.3 der auf Grund dieser DomainInformationen ausgestellte private Schlüssel) der Zwecksetzung der Verwendung bei Zugriff auf geschützten digitalen Inhalt dienen. Setzt aber Merkmalsgruppe 9.1 sowohl

eine bestehende Domain, auf welche sich die Domain-Informationen beziehen müssen, als auch ein in der Domain erfolgendes Teilen von Rechten in Zusammenhang mit einem gemeinsamen Konto voraus, kann im Rahmen von Merkmalsgruppe 9.3 nichts anderes gelten.

70
Merkmalsgruppe 9.1 setzt dem Anspruchswortlaut nach ausdrücklich voraus, dass das anspruchsgemäße Gerät einen Kommunikationskreis aufweist, der dazu dient, Domain-Informationen zu empfangen, die sich auf eine Vorrichtung beziehen, die innerhalb einer Domain aus Vorrichtungen und damit einer Mehrzahl an Vorrichtungen besteht. Unabhängig von der zwischen den Parteien streitig diskutierten Frage, ob das Klagepatent zwingend einen unmittelbar von einer Vorrichtung aus der fraglichen Domain ausgehenden Sendvorgang voraussetzt, ist dem Anspruchswortlaut nach daher jedenfalls entscheidend, dass bereits eine Vorrichtungsdomain besteht. Damit geht das Klagepatent in Anspruch 9 aber davon aus, dass das patentgemäße Gerät einer bestehenden Vorrichtungsdomain hinzugefügt wird und dementsprechend für eben dieses Szenario so programmiert sein muss, um die anspruchsgemäß vorausgesetzten Funktionen erfüllen zu können.

71
Darüber hinaus setzt Merkmalsgruppe 9.1 voraus, dass die bereits vorhandenen Vorrichtungen Rechte in Zusammenhang mit einem gemeinsamen Konto teilen. Dies versteht der Fachmann in dem Sinne, dass bereits gemeinsam genutzte Inhalte in der Domain vorhanden sind. Denn klagepatentgemäße „Rechte“ beziehen sich gerade auf die in einem digitalen Rechtemanagementsystem verwalteten digitalen Inhalte. Das in Zusammenhang mit einem gemeinsamen Konto verlangte Teilen von Rechten ist dabei in der deutschen ebenso wie in der als Verfahrenssprache maßgeblichen englischen Sprachfassung nicht als Funktionsvorgabe formuliert, sondern wird vielmehr - wie die auch insoweit im Indikativ erfolgte Formulierung zeigt - als bestehend vorausgesetzt.

72
Was damit letztlich von einem patentgemäßen Gerät zunächst empfangen und sodann dem externen Schlüsselaussteller als Grundlage der Ausstellung eines patentgemäßen privaten Schlüssels zur Verfügung gestellt werden muss, ist in den für die Zwecke der Auslegung einheitlich zu lesenden Merkmalsgruppen 9.3 und 9.1 bereits im Anspruchswortlaut definiert. In beiden Fällen geht es um Domain-Informationen betreffend eine bestehende Domain, in der bereits bestimmte digitale Inhalte genutzt werden.

73
bb. Dass hingegen der Hinzuerwerb neuer digitaler Inhalte und ein hierfür neu ausgestellter privater Schlüssel nicht patentgemäß ist, ergibt sich für den angesprochenen Fachmann aus der aus der Beschreibung ersichtlichen funktionalen Zielsetzung der patentgemäßen, technischen Lehre.

74
(1) Abs. [0010] der Klagepatentschrift weist darauf hin, dass die Erholung von Domain-Informationen von einer bereits in der Vorrichtungsdomain existierenden Vorrichtung unter Sicherheitsgesichtspunkten nicht ausreicht, das neue Gerät in der entsprechenden Domain zu registrieren. Vielmehr heißt es dort ausdrücklich:

[0010] (…) Security is greatly enhanced if the new device then needs to send this DRM information to a trusted server (i.e., a key issuer) to complete its enrollment into the domain. With this approach, the key issuer can actively enforce domain enrollment and help improve security (…).

Zu Deutsch:

[0010](…) Die Sicherheit wird signifikant erhöht, wenn die neue Vorrichtung die DRM-Information dann an einen vertrauenswürdigen Server (d.h. einem Schlüsselaussteller) sendet, um ihre Registrierung in der Domain abzuschließen. Auf diese Weise kann der Schlüsselaussteller die Registrierung in einer Domain aktiv durchsetzen und dazu beitragen, die Sicherheit zu verbessern. □…□ Diese funktionale Zielsetzung der erfindungsgemäßen Lehre setzt gerade voraus, dass ein digitales Rechtemanagementsystem eine Absicherung über den externen Schlüsselaussteller hinsichtlich sämtlicher Geräteregistrierungen, d.h. sowohl bei der Erstregistrierung als auch bei Folgeregistrierungen, ermöglicht. Der Zweck einer Erhöhung der Sicherheit würde hingegen nicht, jedenfalls nicht in patentgemäßer Weise erfüllt, wenn lediglich bei der Erstregistrierung eines Gerätes für einen neuen Musikdienst ein externer Schlüsselaussteller eingesetzt würde. Anderenfalls würde gerade der mit Blick auf die Rechtenutzung kritische Bereich des Hinzufügens

zusätzlicher Geräte angesichts des hierdurch erweiterten Risikos unerlaubter Zugriffe auf geschützte Inhalte nicht erfasst.

□2□

Dass patentgemäß ein neues Gerät einen privaten Schlüssel für bestehende Inhalte von dem externen Schlüsselaussteller und gerade nicht im Wege des Teilens von bereits in der Domain registrierten Geräten erhalten muss, verdeutlicht überdies Abs. [0032] der Klagepatentschrift, der ausdrücklich wie folgt lautet:

[0032] □…□ If all subsequent enrollments into the family of devices are forced to use shortrange communication for enrollment, the newly added device are forced to be in direct physical control of the user, resulting in more secure DRM system. Additionally, the use of the key issuer 105 greatly improves security. For example, if a key issuer were not used then devices would need to share their DRM private keys and issue DRM certificates. Hackers would have an easier time breaching the security of such a system since they have physical access to their devices and can tamper with the hardware to try and create false DRM certificates. □…□

Zu Deutsch: [0032]□…□ Wenn alle nachfolgenden Registrierungen in die Familie an Geräten für die Registrierung zwingend eine Kurzstreckenverbindung nutzen, befindet sich das neu hinzugefügte Gerät gezwungenermaßen unter der physischen Kontrolle des Nutzers, was ein sichereres DRM-System zur Folge hat. Weiter erhöht der Einsatz eines Schlüsselausstellers 105 signifikant die Sicherheit. Würde, beispielsweise, ein Schlüsselaussteller nicht eingesetzt, dann müssten die Geräte ihre privaten DRM-Schlüssel teilen und DRM-Zertifikate ausstellen. Hacker hätten so leichteres Spiel, die Sicherheit eines solchen Systems zu brechen, da sie physischen Zugang zu ihren Geräten haben und versuchen können, die Hardware zu manipulieren und gefälschte DRM-Zertifikate zu erstellen (…).

75
Schriftbildliche Hervorhebungen hinzugefügt.

76
Aus dieser Beschreibungsstelle erkennt der angesprochene Fachmann, dass das Teilen der privaten Schlüssel durch die Geräte innerhalb einer Domain gerade vermieden werden soll. Gerade um dies zu vermeiden, sieht das Klagepatent den Einsatz eines externen Schlüsselausstellers als wortlautgemäß zwingenden Bestandteil eines anspruchsgemäß ausgestalteten Gerätes vor. Daher kann eine neue Vorrichtung, die nur bei der Erstregistrierung eines neuen Musikdienstes den privaten Schlüssel von einem externen Schlüsselaussteller erhält, nicht aber im Falle der Registrierung in einer bestehenden Domain zur Nutzung der dort bereits vorhandenen Inhalte auch nicht als bloß schlechtere und nur in geringerem Maße zur Sicherheit digitaler Inhalte beitragende Ausführungsform eines anspruchsgemäßen Gerätes betrachtet werden. Vielmehr handelt es sich bei einer neu hinzugefügten Vorrichtung, die so eingerichtet ist, dass sie die notwendigen Kennungen für bestehende Inhalte von den bereits im Domainverbund registrierten Geräten und nicht von dem externen Schlüsselaussteller erhält, um ein außerhalb des Schutzbereichs des Klagepatents liegendes Aliud.

77
(3) Dieses Verständnis sieht der Fachmann in Abs. [0008], [0009] und [0010] des Klagepatents bestätigt. Denn hiernach geht es der technischen Lehre des Klagepatents gerade darum, einem Nutzer eine vereinfachte und zugleich sichere Geräteregistrierung zu ermöglichen, nachdem zumindest für ein erstes Gerät Domaininformationen bestimmt worden sind. Der Fachmann erkennt überdies aus der Systematik der Patentbeschreibung, dass in Abs. [0008] bis [0011] die grundlegende Funktionsweise der streitgegenständlichen technischen Lehre dargestellt wird, bevor ab Abs. [0012] eine Beschreibung anhand der Figuren 1 bis 4 des Klagepatents erfolgt.

78
Dabei verkennt die Kammer nicht, dass Abs. [0008] in dessen Satz 2 von einer bevorzugten Ausführungsform spricht und dem Grunde nach - worauf die Klägerin insoweit zutreffend hinweist - gilt, dass die Auslegung eines Patents dessen Schutzbereich nicht auf ein bestimmtes Ausführungsbeispiel beschränken und dadurch hinter dem Wortlaut des geltend gemachten Anspruchs zurückbleiben darf □ BGH, GRUR 2004, 1023, 1024 - Bodenseitige Vereinzelungsvorrichtung□. Denn wie ausgeführt bleibt die Auslegung bereits nicht hinter dem Anspruchswortlaut zurück. Vielmehr entspricht die Festlegung des von der Klägerin geltend gemachten Anspruchs auf den Funktions- und Wirkungszusammenhang der Nutzung

bestehender digitaler Inhalte über das zu einem Verbund an Vorrichtungen neu hinzutretendes Gerät dem Wortsinn des Anspruchs ebenso wie dem funktionalen Sinn und Zweck der technischen Lehre des Klagepatents sowie dessen Beschreibung.

79
Dazu kommt, dass die Beschreibung in Abs. [0008] zwar im Zusammenhang mit dem Hinzufügen neuer Geräte zu einer bestehenden Domain von einer bevorzugten Ausführungsform spricht. Tatsächlich versteht der angesprochene Fachmann jedoch das Hinzufügen neuer Geräte zu einer bestehenden Domain nicht als bevorzugte Ausführungsform einer im Übrigen weiter zu verstehenden allgemeineren technischen Lehre, sondern erkennt hierin die eigentliche, dem Klagepatent zu Grunde liegende, objektive Aufgabenstellung. Soweit Abs. [0008] von einer bevorzugten Ausführungsform spricht, entnimmt der Fachmann bereits der Formulierung „by obtaining domain information □…□ from devices already in the domain that preferably are in close proximity“, zu Deutsch: „indem Domain-Informationen □…□ von bereits in der Domain befindlichen Geräten empfangen werden, die sich bevorzugter Weise in unmittelbarer Nähe befinden“, dass sich die als bevorzugt bezeichnete Ausgestaltung einer erfindungsgemäßen Vorrichtung gerade nicht auf das Hinzufügen eines neuen Gerätes zu einem bestehenden Domainverbund, sondern auf die unmittelbare Nähe zu einem anderen, in dem Domainverbund bereits befindlichen Gerät bezieht. Die Erholung des privaten Schlüssels von dem externen Schlüsselaussteller seitens der zu einem bestehenden Domainverbund neu hinzugefügten Vorrichtung lehrt Abs. [0008] der Klagepatentschrift dagegen als unabdingbare Voraussetzung, um die Geräteregistrierung als solche abschließen und digitale Inhalte nutzen zu können. Abs. [0009] der Klagepatentschrift bestätigt die dem Klagepatent zu Grunde liegende Aufgabenstellung, indem auf die Schwierigkeiten bei der Geräteregistrierung zusätzlicher Vorrichtungen hingewiesen wird, nachdem bereits eine Domain geschaffen wurde. Für eben dieses in Abs. [0009] nochmals ausdrücklich bestätigte Szenario der Hinzufügung einer neuen Vorrichtung zu einem bestehenden Domainverbund, lehrt Abs. [0010] sodann, dass die Sicherheit digitaler Inhalte erheblich verbessert werden kann, wenn die neu hinzukommende Vorrichtung vor der Registrierung in der bestehenden Domain den externen Schlüsselaussteller kontaktiert.

80
Gleiches gilt mit Blick auf Abs. [0022] der Klagepatentschrift. Nachdem zunächst in Abs. [0021] die im Stand der Technik bestehenden technischen Probleme einer möglicherweise beschwerlichen Geräteregistrierung sowie möglicher Sicherheitsbedenken im Falle einer via Fernzugriff erfolgenden Geräteregistrierung wiederholt wurden, zeigen Zeilen 50/53 der Spalte 6 des Klagepatents als vorteilhafte Lösung auf, Geräte nur über eine Kurzstreckenverbindung in einer bereits bestehenden Domain zu registrieren. Zur Begründung verweist die Patentschrift darauf, dass eine mit einem bereits registrierten Gerät aufgebaute Kurzstreckenverbindung Gelegenheiten für mögliche Eindringlinge in die fragliche Domain verringern könnte. Vor diesem Hintergrund schlägt Abs. [0022] der Klagepatentschrift sodann vor, dass in der bevorzugten Ausführungsform neue Geräte einer bestehenden Domain hinzugefügt werden, indem Domain-Informationen von bereits in der Domain registrierten Vorrichtungen empfangen werden, welche sich bevorzugterweise in unmittelbarer Nähe befinden. Auch insoweit gilt daher, dass die grundlegende Aufgabenstellung darin liegt, ein neues Gerät einer bestehenden Domain hinzuzufügen, was in bevorzugter Weise dadurch geschieht, dass entsprechende Domain-Informationen über eine Kurzstreckenverbindung empfangen werden.

81
(4) Nichts anderes ergibt sich entgegen der Klägerin aus Abs. [0019] der Klagepatentschrift. Demzufolge kann der Schlüsselaussteller aus den von dem neuen Gerät erhaltenen Domain-Informationen erkennen, ob dieses einer neuen oder einer bereits bestehenden Domain hinzugefügt wird. Für beide Konstellationen lehrt die Beschreibung sodann Folgendes:

[0019] (…) Key issuer then creates a DRM certificate that contains all necessary information (e.g., the DRM public key, serial number, model number etc.) for equipment 101 to obtain rights to digital content from rights issuer 103. Key issuer 105 then send equipment 101 the DRM certificat and the DRM private key utilized by the domain.

Zu Deutsch: [0019](…) Der Schlüsselaussteller erstellt dann ein DRM-Zertifikat, das alle notwendigen Informationen (z.B. den öffentlichen DRM-Schlüssel, Seriennummer, Modellnummer usw.) für die Vorrichtung 101 enthält, um die Rechte an digitalem Inhalt von dem Rechteinhaber 103 zu erhalten. Der

Schlüsselaussteller 105 sendet der Vorrichtung 101 dann das DRM-Zertifikat und den von der Domain verwendeten, öffentlichen DRM-Schlüssel.

82
Die Lesart der Klägerin, dass diese Passage der Beschreibung ausschließlich auf die Begründung einer neuen Domain zu beziehen sei, ist nach Ansicht der Kammer nicht zutreffend. Der angesprochene Fachmann wird die Beschreibung vielmehr dahin verstehen, dass der Schlüsselaussteller in Abhängigkeit von der jeweiligen Domainaktion (Hinzufügung des Geräts zu einer neuen oder zu einer bestehenden Domain) entweder ein neues Paar an öffentlichem/privatem DRMSchlüssel erstellt oder - im Falle der Hinzufügung zu einer bestehenden Domain - das in einer Datenbank bereits hinterlegte Schlüsselpaar heranzieht. Für beide Fälle und damit gerade auch für den Fall des Hinzufügens zu einer bestehenden Domain lehrt Abs. [0019], dass der nächste Schritt seitens des externen Schlüsselaussteller darin besteht, ein für das neu hinzugefügte Gerät spezifisches DRM-Zertifikat herzustellen und diesem zuzusenden.

83
Dies bedeutet indes nicht, dass der Erhalt eines neuen privaten Schlüssels von dem externen Schlüsselaussteller im Falle der Hinzufügung neuer digitaler Inhalte die Voraussetzungen der Merkmalsgruppe 9.3 des Klagepatents verwirklicht. Denn wie die im Lichte der funktionalen Zielsetzung des Klagepatents gebotene Auslegung ergeben hat, muss das neu hinzugefügte Geräte gerade für die Nutzung bereits vorhandener Inhalte den entsprechenden privaten Schlüssel von einem externen Schlüsselaussteller erhalten. Dass dies auch im Falle des Hinzufügens neuer digitaler Inhalte zu erfolgen hat, steht dem nicht entgegen, sondern entspricht allein der Tatsache, dass erfindungsgemäß ein einheitliches digitales Rechtemanagement offenbart ist, in dem über die aktive Rolle des externen Schlüsselausstellers bei der Geräteregistrierung ein einheitlicher Schutzstandard gewährleistet und ein bloßes Teilen der Rechte unter den in der Domain vorhandenen Vorrichtungen als nicht hinreichend sicher vermieden werden soll.

84
cc. Dass ein patentgemäßes Gerät bei dessen Registrierung in einem digitalen Rechtemanagementsystem einen privaten Schlüssel auch für bestehende digitale Inhalte von dem externen Schlüsselaussteller erhalten muss, ergibt sich darüber hinaus in Abgrenzung zu dem in der Patentschrift in Abs. [0005] genannten Stand der Technik. Demzufolge war auf der Grundlage des von IBM im Rahmen der DVB-CPT Standardisierungsdiskussion vorgeschlagenen „xCP Cluster“-Protokolls ein digitales Rechtemanagementsystem vorgesehen, in dessen Rahmen innerhalb eines Geräteclusters vorhandene Geräte in gleichberechtigter Weise andere, hinzutretende Geräte autorisieren und diesen so Zugang zu bestehenden Rechten erlauben können. Eine solche Informationsgewinnung von Geräten aus dem Kreise der eigenen Domain bezeichnet Abs. [0010] der Klagepatentschrift indes als nicht hinreichend sicher, um ein neues Gerät in der Domain zu registrieren. Vielmehr ist es das ausdrückliche, technischfunktionale Ziel der erfindungsgemäßen Lehre, einen externen Schlüsselaussteller einzuschalten, über den ein neu hinzutretendes Gerät einen privaten Schlüssel erhält, um sich in der bestehenden Domain zu registrieren. Ein Teilen des privaten Schlüssels innerhalb einer Domain erachtet die erfindungsgemäße Lehre gemäß Abs. [0032] der Klagepatentschrift dagegen explizit als nachteilig.

85
Letztlich entspricht es daher gerade der objektiven Aufgabe des Klagepatents, ein zur Nutzung bereits vorhandener digitaler Inhalte neu erworbenes Gerät so auszugestalten, dass über den Einsatz eines externen Schlüsselausstellers für sämtliche Inhalte eine hinreichende Kontrolle erfolgt, ob in der fraglichen Domain die notwendigen Nutzungsrechte tatsächlich vorhanden sind.

86
Im Falle des erstmaligen Hinzufügens digitaler Inhalte liegt es hingegen in der Natur der Sache, dass das fragliche Gerät die zur Nutzung notwendigen Informationen und Schlüssel von dem Musikdienstanbieter als aus Sicht der Klägerin patentgemäßem Schlüsselaussteller erhält. Der Erhalt eines privaten Schlüssels von einem externen Schlüsselaussteller zur Nutzung neuer digitaler Inhalte entsprach damit im Prioritätszeitpunkt dem Stand der Technik.

87
dd. Diese Auslegung zu Grunde gelegt, kann eine Verwirklichung der Merkmalsgruppe 9.3 durch die angegriffenen Ausführungsformen im Ergebnis nicht bejaht werden. Die Klägerin hat für ihre Verletzungsargumentation die Funktionsweise der angegriffenen Ausführungsformen nicht in dem

patentgemäßen Funktions- und Wirkungszusammenhang der Hinzufügung einer neuen Vorrichtung zur Nutzung in einer Domain vorhandener digitaler Inhalte dargelegt.

88
(1) Die Klägerin geht - insoweit im Einklang mit der seitens der Kammer vertretenen Auslegung - davon aus, dass eine patentgemäße Ausführungsform ein neu zu einer bestehenden Vorrichtungsdomain hinzutretendes Gerät voraussetzt (Seite 32 der Klageschrift vom 12.06.2020 sowie Seiten 14 und 21 der Replik vom 19.02.2021, Bl. 212, 219 d. Akte). Letztlich entspricht dies im Wege der Auslegung gefundene Ergebnis auch der von der ursprünglichen Patentanmelderin M LLC im Rahmen des Erteilungsverfahrens vertretenen Sichtweise, die damit das im Wege der Auslegung gefundene Ergebnis letztlich bestätigt (vgl. BGH, GRUR 2016, 921, Rn. 40 - Pemetrexed). In dem Schreiben an das Europäische Patentamt vom 22.12.2011 (Anlage EIP B4-NK7) hat die Anmelderin ausdrücklich darauf abgestellt, dass die zentralen patentgemäßen Schritte des Empfangs von Domain-Informationen, der Bereitstellung dieser Domain-Informationen an einen externen Schlüsselaussteller und dem Erhalt eines privaten Schlüssels von dem Schlüsselaussteller seitens eines neuen Geräts ausgeführt werden müssen („Thus, the claimed invention performs the following steps at a new device (…) By requiring the new device to send the domain information to a trusted key issuer (…)“).

89
(2) Setzt eine patentgemäße Ausführungsform aber voraus, die anspruchsgemäß vorausgesetzten Schritte als neu zu einer Domain an Vorrichtungen hinzugefügtes Gerät ausführen zu können, kann - soweit die Klägerin die Funktion Refresh-Token gleichfalls als patentverletzend angreift - das Erneuern des „AuthToken“ über den „Private Key“ bereits im Ansatz die Voraussetzungen der Merkmalsgruppen 9.3 und 9.1 nicht erfüllen (so aber die Klägerin auf Seite 24 der Replik vom 19.02.2021, Bl. 222 d. Akte). Denn die Erneuerung des „AuthToken“ dient gerade nicht dem auch der Klägerin zufolge als patentgemäßer Funktions- und Wirkungszusammenhang vorausgesetzten Hinzufügen eines neuen Geräts zu einer bestehenden Vorrichtungsdomain. Vielmehr wird lediglich für ein bereits registriertes Gerät ein neuer „AuthToken“ erholt.

90
(3) Im Übrigen hat die Klägerin den ihrer Verletzungssubsumtion zu Grunde gelegten Sachvortrag auf den Funktions- und Wirkungszusammenhang beschränkt, bei dem über einen zusätzlich zu bereits bei dem Nutzer vorhandenen Geräten erworbenen YY-Lautsprecher ein neuer Musikdienst freigeschaltet wird (siehe etwa Seite 43 der Klage vom 12.06.2020 sowie Seite 23/24 der Replik vom 19.02.2021, Bl. 221/222 d. Akte). Nur für diesen Fall der Hinzufügung eines neuen Musikdienstes führt die Klägerin aus, dass die angegriffenen YY-Geräte eine Zugangskennung in Gestalt des „AuthToken“ und des „Private Key“ von einem externen Schlüsselaussteller erhalten.

91
In dem hingegen maßgeblichen, patentgemäßen Funktions- und Wirkungszusammenhang der Hinzufügung einer neuen Vorrichtung zur Nutzung vorhandener Inhalte erhält die neu hinzugefügte Vorrichtung die zur Nutzung entsprechender Inhalte erforderlichen Kennungen von den im Domainverbund bereits registrierten Geräten und gerade nicht - was patentgemäß notwendig wäre - von dem externen Schlüsselaussteller. Vielmehr - und dies stellt auch die Klägerin selbst nicht in Frage - erhalten die angegriffenen Ausführungsformen ihre Zugangskennung bei Hinzufügung einer bestehenden Vorrichtungsdomain zur Nutzung bereits vorhandener Inhalte von anderen Geräten aus dem YYHaushalt. Ein solches Teilen von Zugangskennungen will das Klagepatent jedoch, wie insbesondere Abs. [0032] zeigt, gerade vermeiden. Stattdessen sieht das Klagepatent gemäß dessen Abs. [0010] eine aktive Rolle des externen Schlüsselausstellers bei der Geräteregistrierung vor.

92
Dem kann die Klägerin nicht mit Erfolg entgegenhalten, dass mit Blick auf die Eigenart des geltend gemachten Anspruchs als Vorrichtungsanspruch die Eignung der angegriffenen Ausführungsformen genüge, im Rahmen eines patentgemäßen Funktions- und Wirkungszusammenhangs verwendet zu werden (vgl. BGH, GRUR 2006, 570, 573, Rn. 21 - extracoronales Geschiebe), was nach Ansicht der Klägerin dadurch belegt sei, dass ja im Falle der Hinzufügung eines neuen Musikdienstes die Kennungen „AuthToken“ und „Private Key“ von dem externen Schlüsselaussteller erhalten würden. Zwar steht damit fest, dass die angegriffenen Ausführungsformen in dem Funktions- und Wirkungszusammenhang der

Hinzufügung neuer Inhalte (etwa eines neuen Musikdienstes wie „Spotify“ zusätzlich zu dem bereits genutzten Dienst „Apple Music“) die vermeintlichen privaten Schlüssel bezüglich des neu hinzugefügten Dienstes (im hier gewählten Beispiel: „Spotify“) von dem externen Schlüsselaussteller erhalten. Allerdings handelt es sich hierbei nicht um den wie dargelegten, zwingend vorausgesetzten patentgemäßen Funktions- und Wirkungszusammenhang, der - wie ausgeführt - gerade eine neue Vorrichtung zur Nutzung vorhandener Inhalte betrifft. Für den patentgemäß vorausgesetzten Funktions- und Wirkungszusammenhang fehlt es aber bereits an einem entsprechenden Tatsachenvortrag der Klägerseite, so dass eine Verletzung hier nicht bejaht werden kann. Auf Grund des insoweit unwidersprochen gebliebenen Vortrags der Beklagten ist vielmehr davon auszugehen, dass die einem Domainverbund hinzugefügten, angegriffenen YY-Geräte die zur Nutzung bereits vorhandenen Inhalte erforderlichen Kennungen von den bereits in dem jeweiligen Geräteverbund vorhandenen Geräten erhalten. Daher fehlt es bei dieser, von den angegriffenen Ausführungsformen gewählten Lösung jedoch an dem patentgemäß als wesentlicher Schritt zur Verbesserung der Sicherheit digitaler Inhalte vorgesehenen Einsatz eines externen Schlüsselausstellers.

93
Nichts anderes ergibt sich entgegen der auf Seiten der Beklagten im Rahmen der mündlichen Verhandlung geäußerten Ansicht aus dem Urteil der Kammer vom 23.10.2020, Az. 21 O 11384/20. Die Kammer kam hier unter Anwendung der zu Wirkungs- und Funktionsangaben entwickelten und der Auslegung auch im vorliegenden Verfahren zu Grunde gelegten Rechtsprechungsgrundsätze zu dem Ergebnis, dass ein patentgemäßes Benutzerendgerät in der Lage sein musste, einen Kernnetzwerkelementbezeichner zu speichern und in anspruchsgemäßer Weise zu senden, wohingegen die Auswahl und Verbindung nach der Lehre des dortigen Klagepatents netzwerkseitig unter Auswertung des von dem Benutzerendgerät übersandten Kernnetzwerkelementbezeichners erfolgen sollte. Insoweit unterscheiden sich die Sachverhaltskonstellationen grundlegend. Denn anders als in der dem Urteil vom 23.10.2020 zu Grunde liegenden Konstellation kommt es dem hiesigen Klagepatent dessen funktionellen Vorgaben nach gerade darauf an, dass die Übermittlung des hier patentgemäßen Informationselements von einem bestimmten Sender (hier: dem externen Schlüsselaussteller) zu einem bestimmten Zweck (hier: der Nutzung vorhandener digitaler Inhalte) erfolgt.

94
d. Darüber hinaus kommt die Kammer bei Anwendung der oben dargelegten Aus legungsgrundsätze zu dem Ergebnis, dass ein gemäß Merkmalsgruppe 9.3 vorausgesetzter privater Schlüssel kryptographischer Natur sein muss. Der angesprochene Fachmann erkennt aus der Klagepatentschrift, dass ein patentgemäßer privater Schlüssel von einer technischen Lehre aus dem Bereich der Kryptographie Gebrauch machen muss (nachfolgend lit. aa.). Dass es sich bei den von den angegriffenen YY-Geräten empfangenen Kennungen „AuthToken“ und „Private Key“ um einen kryptographischen Schlüssel handelt, kann auf der Grundlage des von der Klägerin erfolgten Sachvortrages nicht bejaht werden (nachfolgend lit. bb.).

95
aa. Ausgehend vom Anspruchswortlaut der Merkmalsgruppe 9.3 muss der patentgemäß vorgesehene Logikkreis den Schlüsselaussteller dazu veranlassen, dem fraglichen Gerät, welches die Domain-Informationen an den Schlüsselaussteller gesendet hat, einen privaten Schlüssel zur Verwendung bei Zugriff auf geschützten digitalen Inhalt auszustellen.

96
(1) Ausgehend vom Anspruchswortlaut unter Berücksichtigung des in ständiger höchstrichterlicher Rechtsprechung bestätigten Grundsatzes, wonach eine Patentschrift ihr eigenes Lexikon darstellt (BGH, GRUR 1999, 909, 912 - Spannschraube) steht aus Sicht der Kammer fest, dass es sich bei einem patentgemäßen privaten Schlüssel um einen kryptographischen Schlüssel handeln muss.

97
Dabei ist im vorliegenden Fall im besonderen Maße zu bedenken, dass die schlichte, begriffliche Übereinstimmung hinsichtlich der in den angegriffenen Ausführungsformen verwendeten Kennungen (insbesondere mit Blick auf den in YY-Geräten neben dem „AuthToken“ verwendeten „Private Key“) nicht zu der voreiligen Annahme eines patentgemäßen privaten Schlüssels (in der englischen Sprachfassung: „private key“) verleiten darf. Entscheidend ist vielmehr, wie der angesprochene Fachmann das patentgemäß

vorgesehene Merkmal „privater Schlüssel“ versteht. Die insoweit entscheidende Antwort ergibt sich aus Abs. [0011] der Klagepatentschrift. Demzufolge ist der private Schlüssel als Gegenstück zu einem im Rahmen der Public-Key Kryptographie verwendeten öffentlichen Schlüssel definiert. Dort heißt es ausdrücklich:

[0011] Prior to describing the DRM system in accordance with the preferred embodiment of the present invention the following definitions are provided to set the necessary background.

- Public-Key Cryptography - Cryptographic technique that uses a pair of keys, a public and a private key. The private key is used for either decrypting data or generating digital signatures and the public key is used for either encrypting data or verifying digital signatures. □…□

Zu Deutsch: [0011] Bevor das DRM-System in Übereinstimmung mit der bevorzugten Ausführungsform der vorliegenden Erfindung beschrieben wird, werden die nachfolgenden Definitionen dargelegt, um den notwendigen Hintergrund darzustellen.

- Public-Key Kryptographie - Kryptographische Technik, die ein Schlüsselpaar verwendet, einen öffentlichen und einen privaten Schlüssel. Der private Schlüssel wird verwendet, um entweder Daten zu entschlüsseln oder digitale Signaturen zu generieren und der öffentliche Schlüssel wird verwendet, um entweder Daten zu verschlüsseln oder digitale Signaturen zu verifizieren. □…□ Die Argumentation der Klägerin, dass hier nicht der anspruchsgemäß vorausgesetzte private Schlüssel, sondern die Public-Key Kryptographie erläutert werde, kann bereits dem klaren Wortlaut der vorgenannten Beschreibungsstelle nach keinen Erfolg haben. Der - im Rahmen der Beschreibung durch Kursivdruck gesondert hervorgehobene - Terminus „private key“ wird seiner Funktion nach explizit dahingehend beschrieben, dass es sich um ein Mittel zur Entschlüsselung von Daten oder der Erstellung einer digitalen Signatur handelt.

98
Gleichfalls als nicht durchgreifend erachtet die Kammer das Argument der Klägerin, wonach sich die Definition in Abs. [0011] nur auf ein besonderes Ausführungsbeispiel beziehe. Auch insoweit steht bereits der Beschreibungswortlaut entgegen. Ausdrücklich heißt es dort, dass der notwendige Hintergrund dargestellt wird. Dem angesprochenen Fachmann ist damit klar, dass den hier erläuterten Begrifflichkeiten allgemeine Bedeutung für die patentgemäße technische Lehre zukommt.

99
(2□ Die gebotene einheitliche Betrachtung der klagepatentgemäßen technischen Lehre zeigt vielmehr, dass die Verwendung des anspruchsgemäß vorausgesetzten privaten Schlüssels ausgehend von der in Abs. [0011] vorgegebenen allgemeinen Begriffsdefinition ausschließlich zur Entschlüsselung von Daten oder der Erstellung digitaler Signaturen gelehrt wird. So sieht etwa Abs. [0029] der Klagepatentschrift vor, dass eine Vorrichtung zur Nutzung digitalen Inhalts auf den privaten Schlüssel zugreifen muss und diesen zum Entschlüsseln des zur Verschlüsselung des Inhalts verwendeten Schlüssels verwendet („(…) and uses it [DRM private key 206] to decrypt the content encryption key from rights object 205“). Gleiches folgt aus Abs. [0020] der Klagepatentschrift. Dagegen können nicht kryptographische Ausgestaltung des privaten Schlüssels der Beschreibung gerade nicht entnommen werden.

100
Dem kann die Klägerin nicht mit Erfolg entgegenhalten, dass Abs. [0020] nur ein in Unteranspruch 13 gesondert unter Schutz gestelltes Ausführungsbeispiel betreffe. Abs. [0020] der Klagepatentschrift illustriert vielmehr die kryptographische Absicherung patentgemäßer digitaler Rechtemanagementsysteme. Der Fachmann entnimmt Abs. [0020], dass die in einem klagepatentgemäßen digitalen Rechtemanagementsystem vorhandenen Rechteobjekte diesem nach Erhalt eines DRM-Zertifikats zur Verfügung gestellt worden sein mussten, auf dessen Grundlage der Rechteinhaber einer an einem digitalen Rechtemanagement beteiligten Vorrichtung das digital signierte und einen den digitalen Inhalt verschlüsselnden Verschlüsselungsschlüssel beinhaltende Rechteobjekt übersendet haben muss. Dabei weiß der Fachmann aus Abs. [0015] des Klagepatents, dass es sich bei den Rechteobjekten um die Lizenzen zur Nutzung digitaler Inhalte handelt. Die Rechteobjekte im Sinne des Klagepatents stellen damit die eigentliche, rechtliche Grundlage für digitale Rechtemanagementsysteme dar, aus denen sich Umfang und Reichweite der einem Nutzer zustehenden Befugnisse ergeben. Unter dem Gesichtspunkt der Sicherheit dem zu Grunde liegender digitaler Inhalte lehrt das Klagepatent in Abs. [0020] die als besonders vorteilhaft erachtete Lösung, einen privaten Schlüssel zur Entschlüsselung eines zweiten

Verschlüsselungsschlüssels zu verwenden, um so den gewünschten digitalen Inhalt zu entschlüsseln. Folglich wird hier aus Sicht des angesprochenen Fachmanns eine zusätzliche Verschlüsselungsmöglichkeit gelehrt.

101
Die Kammer teilt vor diesem Hintergrund zwar die Auffassung der Klägerin insoweit, als Abs. [0020] der Klagepatentschrift die gemäß Unteranspruch 13 gesondert beanspruchte Verwendung eines Verschlüsselungsschlüssels zur Entschlüsselung digitalen Inhalts zum Gegenstand hat. Allerdings belegt dies mit Blick auf die relevante Auslegung des technischen Merkmals „privater Schlüssel“ gerade weiter, dass es sich bei einem solchen um einen kryptographischen Schlüssel handeln muss. Denn gemäß Unteranspruch 13 kann der private Schlüssel - so dessen ausdrücklicher Anspruchswortlaut - zur Entschlüsselung eines „zweiten Verschlüsselungsschlüssel“ verwendet werden. Wird aber - wie ausgeführt - der private Schlüssel explizit im Sinne einer zusätzlichen Verschlüsselungsmöglichkeit ausdrücklich „zur Entschlüsselung“ und damit auf kryptographische Art und Weise eingesetzt, steht für den angesprochenen Fachmann fest, dass es sich bei einem privaten Schlüssel im Sinne der patentgemäßen Lehre um einen kryptographischen Schlüssel handeln muss.

102
Mit Blick auf das in dem zu Grunde liegenden Hauptanspruch wortlautgleich beinhaltete Merkmal kann nichts anderes gelten. Vielmehr widerspräche es der gebotenen einheitlichen Betrachtung der patentgemäßen Lehre, wenn man einen privaten Schlüssel gemäß Unteranspruch 13 im Sinne eines kryptographischen Schlüssels verstehen, zugleich aber das jeweils mit derselben Bezugsziffer 206 gekennzeichnete, identische Merkmal des privaten Schlüssel gemäß Hauptanspruch 9 dem allgemeinsprachlichen Begriffsverständnis folgend im Sinne einer beliebig wählbaren, geheim zu haltenden alphanumerischen Zeichenfolge auslegen wollte. Dies führt auch nicht zu einer hinter dem Wortlaut des Hauptanspruchs zurückbleibenden, diesen lediglich um in einem Unteranspruch enthaltene Merkmale ergänzenden und deswegen unzulässigen Auslegung (vgl. BGH, Urt. v. 29.07.2014, Az. X ZR 5/13, BeckRS 2014, 17436, Rn. 18; OLG Düsseldorf, GRUR-RS 2021, 12120, Rn. 55 - Behandlungsmaschine). Vielmehr kann - wie der BGH bereits ausdrücklich entschieden hat - die Ermittlung des Sinngehalts eines Unteranspruchs grundsätzlich zur richtigen Auslegung des Hauptanspruchs beitragen (BGH, GRUR 2016, 1031, 1033, Rn. 15 - Wärmetauscher). Dies gilt insbesondere, wenn wie vorliegend kein additives Merkmal, sondern ein in sämtlichen Ansprüchen genanntes und als solches einheitlich bezeichnetes Merkmal auszulegen ist. Dagegen würde die Interpretation der Klägerin unter Berücksichtigung von Unteranspruch 13 im Ergebnis zu einem unzulässigen, gespaltenen Merkmalsverständnis führen.

103
(3) Darüber hinaus erkennt der Fachmann aus Abs. [0033] der Klagepatentschrift, dass ein patentgemäßer privater Schlüssel kryptographischer Natur sein muss.

104
Dem Fachmann wird in Abs. [0033] der Klagepatentschrift offenbart, dass zur Absicherung von digitalen Rechtemanagementsystemen als Alternative zur Verwendung öffentlicher und privater Schlüssel in Public Key-Verschlüsselungssystemen auch symmetrische Schlüsseltechniken oder Broadcast KeyVerschlüsselungstechniken verwendet werden können. Insofern ist der Klägerin zuzugeben, dass die patentgemäße Lehre vor dem Hintergrund des Abs. [0033] der Klagepatentschrift nicht auf die Verwendung eines privaten Schlüssels im Rahmen eines Public Key-Verschlüsselungssystems festgelegt ist. Dem Fachmann ist aber auf Grund seines allgemeinen Fachwissens bekannt, dass es sich sowohl bei symmetrischen Schlüsseltechniken als auch Broadcast Key-Verschlüsselungstechniken um kryptographische Techniken handelt.

105
Hierauf hat die Beklagte in der mündlichen Verhandlung hingewiesen. Die Klägerin ist dem weder in ihrem mündlichen Vortrag noch schriftsätzlich entgegengetreten. Darüber hinaus entspricht der Vortrag der Beklagten in der mündlichen Verhandlung dem fachmännischen Begriffsverständnis. Broadcast KeyVerschlüsselungstechniken beschäftigen sich demzufolge mit der Nutzung kryptographischer Schlüssel zum Schutz bestimmter Inhalte und/oder um auf bestimmte Dienste durch eine Gruppe an Nutzern im Gegensatz zu rein bilateralen Punktzu-Punkt-Kommunikationsverbindungen (vgl. hierzu die Aussage des von der Klägerin im parallelen USamerikanischen Patentverletzungsverfahren benannten Sachverständigen

S1. vom 08.03.2021, United States District Court Northern District of California, Az. 3:20-cv-3845, Anlage K-B 07, Seite 25). Bei symmetrischen Schlüsseltechniken wird eine bestimmte Zeichenfolge mit Hilfe eines zwischen Sender und Empfänger vereinbarten Schlüssels verschlüsselt, so dass nur der Sender und der Empfänger den Inhalt der Nachricht zur Kenntnis nehmen können. Ein insoweit einfaches Beispiel illustriert das dem Fachmann im Prioritätszeitpunkt bekannte Handbuch zur angewandten Kryptographie (Menezes/van Oorschot/Vanstone, „Handbook of Applied Cryptography“, Juni 1996, Anlage B4). Vereinbaren Sender und Empfänger etwa einen Schlüssel „e“, der die in einer Kennung oder Nachricht verwendeten Buchstaben in Gruppen zu jeweils fünf Zeichen aufteilt und die einzelnen Buchstaben in den jeweils drittnächsten Buchstaben des Alphabets umwandelt,

$$e = \begin{pmatrix} A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z \\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z\ A\ B\ C \end{pmatrix}$$

wird beispielsweise die Nachricht „THIS CIPHER IS CERTAINLY NOT SECURE“ verschlüsselt in die Zeichenfolge „WKLVF LSKHU LVFHU WDLQO BQRWV HFXUH“, so dass ein Dritter ohne Kenntnis des Schlüssels zwar die Nachricht als solche sehen, inhaltlich aber ohne den entsprechenden Schlüssel nicht verstehen kann (Menezes/van Oorschot/Vanstone, a.a.O., Seiten 15/16). Dieses Beispiel veranschaulicht zugleich ein Grundprinzip kryptographischer Technik, der es im Wesenskern darum geht, den Inhalt einer Nachricht oder eines Kennwortes für Dritte mittels einer bestimmten Funktion (dem eigentlichen Schlüssel) unkenntlich zu machen und so sicherzustellen, dass nur autorisierte Personen Zugriff auf bestimmte Daten haben.

106
(4) Dass ein anspruchsgemäßer privater Schlüssel nur ein kryptographischer Schlüssel sein kann, entspricht überdies dem Verständnis des relevanten Fachmanns.

107
Das Klagepatent selbst (vgl. etwa Abs. [0011] der Klagepatentschrift) ebenso wie der in Abs. [0005] und Abs. [0006] der Klagepatentschrift zitierte, dem Fachmann im Prioritätszeitpunkt bekannte Stand der Technik basieren auf dem Grundkonzept der Sicherung digitaler Inhalte durch kryptographische Methoden. Überdies zählte die Verwendung kryptographischer Techniken, um digitale Inhalte gegen unerlaubte Nutzungen zu schützen, bereits im Prioritätszeitpunkt zu den insoweit bekannten und üblichen technischen Methoden (vgl. Rosenblatt/Trippe/Mooney, Digital Rights Management, 2002, Anlage EIP B5, Seite 89, wonach zwar nicht alle digitalen Rechtemanagementsysteme Kryptographie nutzen, es sich hierbei aber um die am nächsten mit dem digitalen Rechtemanagement assoziierte Kerntechnologie handelt). Berücksichtigt man dabei, dass der Fachmann gemäß Abs. [0002] der Klagepatentschrift dem grundlegenden Sinn und Zweck eines digitalen Rechtemanagementsystems nach dazu angehalten ist, die Sicherheit der jeweiligen digitalen Inhalte zu verbessern und das Risiko möglicher Produktpiraterie zu verringern, ist davon auszugehen, dass der Fachmann den ihm aus der Kryptographie geläufigen Fachterminus „privater Schlüssel“ gerade im Zusammenhang mit der technischen Lehre des Klagepatents im technischen und nicht lediglich im allgemeinsprachlichen Sinne versteht. Ein gegenteiliges Verständnis stünde nicht zuletzt in Widerspruch zu der patentgemäßen Aufgabe, eine zugleich einfache und sichere Geräteregistrierung in einer bestehenden Domain zu ermöglichen.

108
Dieses vor dem funktionalen Hintergrund der klagepatentgemäßen technischen Lehre ermittele, fachmännische Begriffsverständnis wird sowohl von dem von der Klägerin in dem vor dem US District Court Northern District of California geführten, parallelen USamerikanischen Patentverletzungsverfahren benannten Sachverständigen S1., als auch den von der Beklagten benannten Sachverständigen W1. und F. bestätigt. Auch diesen zufolge setzt das Klagepatent einen kryptographischen Schlüssel voraus. So beantwortete der parteibenannte Sachverständige S1. die Frage, ob ein privater Schlüssel im Zusammenhang des dem hiesigen Klagepatent entsprechenden Patents US 7,899,187 B2 (US‘187) ein kryptographischer Schlüssel ist, mit „Ja“ (Anlage KB 07, Seite 20, Z. 11). Dagegen verneinte der Sachverständige S1. die Frage, ob ein privater Schlüssel klagepatentgemäß ausschließlich zum Entschlüsseln von Daten eingesetzt werden kann, und verwies darauf, dass ein privater Schlüssel beispielsweise auch im Rahmen einer Signatursystems verwendet werden könne. Dies entspricht letztlich dem - wie ausgeführten - Verständnis aus Abs. [0011] der Klagepatentschrift, wonach private Schlüssel neben der Entschlüsselung von Daten auch zur Erstellung digitaler Signaturen verwendet werden können.

Dem von der Beklagten benannten Sachverständige W1. zufolge handelt es sich bei dem Begriff „privater Schlüssel“ um einen im Bereich der Kryptographie geläufigen Fachterminus, das mit Blick auf das dem Klagepatent entsprechende Patent US‘187 ausdrücklich aufgegriffen werde, indem die Verwendung des privaten Schlüssels gerade im Zusammenhang mit der Entschlüsselung von Daten oder der Erstellung digitaler Signaturen verwendet werde (Wickers, Anlage EIP B7, Seiten 40/41). Nach Ansicht des Sachverständigen F. muss ein patentgemäßer privater Schlüssel nicht nur allgemein kryptographischer Natur sein, sondern das Gegenstück zu einem im Rahmen eines Public-Key Kryptographiesystems verwendeten öffentlichen Schlüssels darstellen (F., Anlage EIP B6, Seite 5).

109
Ein Dissens ist daher seitens der im Zusammenhang mit der Auslegung des Klagepatents konsultierten Sachverständigen nur hinsichtlich der konkreten Art der als patentgemäß in Betracht kommenden kryptographischen Techniken auszumachen. Hinsichtlich des fachmännischen Verständnisses, dass ein privater Schlüssel im Sinne des Klagepatents kryptographischer Natur sein muss, besteht indes Einigkeit.

110
bb. Dieses Merkmalsverständnis zu Grunde gelegt machen die angegriffenen Ausführungsformen von dem patentgemäß vorgesehenen Merkmal eines „privaten Schlüssels“ keinen Gebrauch. Die in einem YY-System verwendeten Kennungen „AuthToken“ und „Private Key“ stellen keine privaten Schlüssel im Sinne des Klagepatents dar. Die Klägerin hat nicht hinreichend dargelegt, dass von ihr als vermeintliche private Schlüssel angegriffenen Kennungen kryptographischer Natur sind. Der Vortrag, dass es sich bei den Kennungen „AuthToken“ und „Private Key“ jeweils um eine Reihe von Buchstaben/Ziffern in der Länge von bis zu 2048 Zeichen handele, die geheim bleiben und nicht mit Dritten geteilt werden soll, lässt die Verwendung kryptographischer Techniken nicht erkennen. Vielmehr basiert die von den angegriffenen Ausführungsformen praktizierte Authentifizierung einer Vorrichtung bei dem externen Schlüsselanbieter auf einem reinen, letztlich einem herkömmlichen Passwortsystem vergleichbaren Referenzwerteabgleich.

111
(1) Die Kennungen „AuthToken“ und „Private Key“ können entgegen der Klägerin auch nicht allein aus dem Grund als kryptographische Schlüssel bezeichnet werden, weil diese der Authentifizierung eines Nutzers und damit einem von kryptographischen Techniken verfolgten Zweck dienen. Zwar ist es richtig, dass die Kryptographie als Technikbereich neben der Sicherstellung von Vertraulichkeit und Datenintegrität auch dem Zweck der Authentifizierung dient (vgl. Sherman, Anlage K-B 07; Menezes/van Oorschot/Vanstone, Anlage EIP B4-D11, Seite 4). Allerdings kann nicht per se jede Technik, die auch einem oder mehreren dieser Zielrichtungen dient, allein auf Grund einer gleichgerichteten Zweckrichtung als dieser Technik zugehörig betrachtet werden. Entscheidend ist vielmehr die funktionale Art und Weise, wie dieses Ziel technisch umgesetzt wird. Die hierbei eingesetzten technischen Mittel müssen daher kryptographischer Natur sein. Dies ist vorliegend indes nicht der Fall.

112
(2) Die Beklagte hat - insoweit unwidersprochen - ausgeführt, dass es bei kryptographischen Techniken darum geht, Klartext in Geheimtext umzuwandeln (siehe etwa der im Stand der Technik bekannte und öffentlich verfügbare Aufsatz von Mäki vom 25.05.2000 zum Thema „Security Fundamentals in Adhoc Networking, Anlage EIP B4-D12, Seite 3; Wicker, Anlage EIP B7, Seite 27, Rn. 86), was über das Handbuch von Menezes/van Oorschot/Vanstone hinaus auch in der Stellungnahme des von der Beklagten im USamerikanischen Parallelverfahren benannten Sachverständigen W1. bestätigt wird. Dieser weist auf Seite 26, Rn. 83, als Beispiel gerade auf das unter Ziff. I.4.d.aa.(3) bereits erläuterte und dem Fachmann im Prioritätszeitpunkt aus dem Handbuch von Menezes/van Oorschot/Vanstone geläufige Kryptographiesystem hin. In technischer Hinsicht ist dabei die Verwendung einer mathematischen Funktion von zentraler Bedeutung, welche in digitalen Rechtemanagementsystemen in Form entsprechender Algorithmen umgesetzt werden (Menezes/van Oorschot/Vanstone, Anlage EIP B4-D11, Seite 6; Rosenblatt/Trippe/Mooney, Digital Rights Management, Anlage EIP B5, Seite 90). Dies bestätigt der von der Beklagten benannte Sachverständige W1. (Anlage EIP B7, Seite 26, Rn. 85) wie folgt:

„But the principle remained the same - the system would take plain text as an input, apply an algorithm, and output cryptographically secure text. The only way for a recipient of the secure text to discern its true meaning was to utilize a private key.“

Zu Deutsch:

„Das Prinzip aber blieb gleich - das System würde Klartext als Input aufnehmen, einen Algorithmus anwenden und kryptographisch sicheren Text ausgeben. Der allein mögliche Weg für einen Empfänger des sicheren Texts, dessen wahre Bedeutung zu erkennen, liegt in der Verwendung eines privaten Schlüssels."

113
Dass die Authentifizierung der angegriffenen Ausführungsformen über die Kennungen „AuthToken" und „Private Key" auf der Grundlage kryptographischer Techniken erfolgt, hat die Klägerin indes nicht dargelegt. Insbesondere ist dem Vortrag der Klägerin keinerlei Anhaltspunkt dafür zu entnehmen, ob und gegebenenfalls mit welcher technischen Methode diese Kennungen für Dritte mittels einer bestimmten Funktion unkenntlich gemacht würden, um so sicherzustellen, dass nur autorisierte Personen den gewünschten Zugriff erhalten. Ebenso wenig ist vorgetragen, dass und gegebenenfalls wie in den angegriffenen Ausführungsformen ein kryptographischer Algorithmus Verwendung findet, um in Zusammenhang mit den relevanten Kennungen Klartext in für Dritte nicht erkennbaren Geheimtext umzuwandeln.

114
(3) Soweit die Klägerin in ihrem nicht nachgelassenen Schriftsatz vom 28.05.2021 versucht hat, substantiiert vorzutragen, dass die von den angegriffenen Ausführungsformen verwendeten Kennungen „AuthToken" und „Private key" von einem Zufallsgenerator erzeugt würden und Eingang in einen kryptographischen Algorithmus fänden, ist der insoweit nach Schluss der mündlichen Verhandlung erfolgte Vortrag gemäß § 296a Satz 1 ZPO zurückzuweisen.

115
Die Beklagte hat bereits in der Klageerwiderung vom 03.02.2021 (dort: Seiten 24 ff.) darauf hingewiesen, dass ein patentgemäßer privater Schlüssel kryptographischer Natur sein muss. Dazugehörige Nachweise und Unterlagen hat die Beklagte bereits mit der Klageerwiderung vorgelegt (insbesondere Anlagen EIP B3 sowie EIP B4-D11) und mit der Duplik sowie weiterer Fachliteratur und zwei dieser anliegenden Sachverständigengutachten vertieft (insbesondere Anlagen EIP B5, EIP B6 und EIP B7). Die Klägerin hat sich hingegen bis zur mündlichen Verhandlung auf die Argumentation zurückgezogen, dass ein patentgemäßer Schlüssel nicht zwingend kryptographischer Natur sein müsse. Den Vortrag, wonach für die Authentifizierung einer Vorrichtung bei einem externen Schlüsseldienst die Kennungen „AuthToken" und „Private Key" vorgeblich von einem kryptographischen Algorithmus verarbeitet würden, hätte die Klägerin ohne Weiteres bereits im Vorfeld der mündlichen Verhandlung ausführen können, umso mehr, als selbst der nicht nachgelassene Vortrag mit keinerlei detaillierten technischen Erläuterungen einhergeht. Auf Grund des Bestreitens auf Seiten der Beklagten hätte hierzu bereits vorab der mündlichen Verhandlung erkennbarer Anlass bestanden. Selbst im Rahmen der mündlichen Verhandlung beschränkte sich die Klägerin weiterhin auf ihre Auffassung, wonach es genüge, zur Auslegung des Klagepatents zu argumentieren, dass dieses keinen kryptographischen Schlüssel voraussetze. Einen Antrag auf Schriftsatznachlass hat sie nicht gestellt.

116
Selbst wenn man den nachgeschobene Vortrag zu Gunsten der Klägerin der Sache nach berücksichtigt, ist dieser zumindest in der Sache nicht geeignet, die Behauptung der Verwendung eines kryptographischen Schlüssels darzulegen. Weder die Erzeugung der Kennungen durch einen Zufallsgenerator noch der Hinweis auf die Verarbeitung der Kennungen in einem Algorithmus zur Authentifizierung einer Vorrichtung lässt einen Rückschluss auf einen kryptographischen Algorithmus zu. Dies gilt umso mehr, als sich die verspäteten Ausführungen der Klägerin auf die unsubstantiierte Behauptung beschränken, dass die Kennungen in einer nicht näher bezeichneten Art und Weise in einen nicht näher bezeichneten Header eingefügt werden. Inwieweit hierbei kryptographische Techniken angewendet werden und ein Algorithmus die zur Geräteregistrierung verwendeten Kennungen verschlüsselt, d.h. Klartext in Geheimtext umwandelt, ist nicht ersichtlich.

117
Wie die Auslegung zudem gezeigt hat, müsste der private Schlüssel, um als kryptographisch im Sinne des Klagepatents qualifiziert werden zu können, verwendet werden, um Daten zu entschlüsseln oder digitale Signaturen zu erzeugen (Abs. [0011] der Klagepatentschrift). Auch hierzu enthält der nachgeschobene Vortrag der Klägerin keinerlei Anhaltspunkte.

118

(4) Dem kann die Klägerin nicht unter Verweis auf Seite 46 der Klage entgegenhalten, bereits an dieser Stelle dazu vorgetragen zu haben, dass die von den angegriffenen Ausführungsformen verwendeten Kennungen „AuthToken“ und „Private key“ kryptographische Schlüssel darstellten. Auf Seite 46 der Klage hat die Klägerin auf die von den angegriffenen Ausführungsformen verwendete Funktion „Encrypt content“ hingewiesen. Nachdem der Beklagtenvertreter jedoch in der mündlichen Verhandlung erläutert hatte, dass es hierbei um eine Funktionalität gehe, die es in einem Verbund an YY-Geräten ermögliche, digitale Inhalte zu verschlüsseln und die nichts mit der Verwendung patentgemäßer privater Schlüssel zu tun habe, hat der Klägervertreter ausdrücklich den in der Klage erfolgten Vortrag als missverständlich eingeräumt und sich hiervon distanziert.

119
Ungeachtet dieses widersprüchlichen Vortrages hat die Klägerin die substantiierten Ausführungen der Beklagten zu der auf Seite 46 der Klage angeführten „Encrypt content“-Funktion jedenfalls nicht bestritten. Den Beklagtenvortrag zu Grunde gelegt ist die „Encrypt content“-Funktion somit dahingehend zu verstehen, dass diese gerade nicht den patentgemäßen privaten Schlüssel betrifft, sondern eine gerätespezifische Verschlüsselung mit Blick auf einen bestimmten Mediastream ermöglicht.

120
(5) Wenn die Klägerin schließlich in ihrem Schriftsatz vom 02.06.2021 aus dem von der Beklagten gemäß Anlage EIP B6 vorgelegten Gutachten des Sachverständigen F. herleiten möchte, dass dieser in seinem Gutachten die - vermeintlich patentgemäße - Funktionsweise entsprechender Token zur Authentifizierung (Abgleich mit Referenzwert) erläutert habe, übersieht die Klägerin, dass der Sachverständige einen dahingehenden, Tokenbasierten Vergleich eines Wertefeldes mit einem Referenzwertefeld ausdrücklich als Beispiel einer nichtkryptographischen Form der Authentifizierung aufführt (siehe Anlage EIP B6, Seiten 3/4, Brückenabsatz).

121
cc. Auf die Frage, ob die von den angegriffenen Ausführungsformen zur Authentifizierung bei Musikdiensteanbietern verwendeten, nichtkryptographischen Kennungen „AuthToken“ und „Private Key“ unter dem Gesichtspunkt der äquivalenten Benutzung eine Patentverletzung darstellen können, ist nicht näher einzugehen. Hierzu hat die Klägerin weder vorgetragen noch einen entsprechenden Antrag gestellt.

122
II. Die Nebenentscheidungen über die Kosten sowie die vorläufige Vollstreckbarkeit folgen aus §§ 91 Abs. 1 Satz 1, 709 Satz 1 ZPO.