BUNDESPATENTGERICHT

IM NAMEN DES VOLKES

URTEIL

An Verkündungs Statt
zugestellt am
10. März 2021
…

5 Ni 28/18 (EP)

(Aktenzeichen)

In der Patentnichtigkeitssache

…

ECLI:DE:BPatG:2021:100321U5Ni28.18EP.0

betreffend das europäische Patent 1 404 085
(DE 603 09 647)

hat der 5. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf Grund der mündlichen Verhandlung vom 18. November 2020 durch den Vorsitzenden Richter Voit, die Richterin Martens sowie die Richter Dipl.-Ing. Univ. Albertshofer, Dipl.-Geophys. Univ. Dr. Wollny und Dipl.-Phys. Univ. Bieringer

für Recht erkannt:

I. Das europäische Patent 1 404 085 wird mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland für nichtig erklärt.

II. Die Beklagte trägt die Kosten des Rechtsstreits.

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

T a t b e s t a n d

Die Beklagte ist eingetragene Inhaberin des auch mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland in englischer Verfahrenssprache erteilten europäischen Patents EP 1 404 085 (Streitpatent), das am 29. September 2003 angemeldet wurde und die Priorität von drei US-amerikanischen Anmeldungen in Anspruch nimmt, wobei die älteste Priorität vom 27. September 2002 datiert. Beim Deutschen Patent- und Markenamt wird das Streitpatent unter dem Aktenzeichen DE 603 09 647.6 geführt. Es trägt die Bezeichnung „System and method for securely handling control information“ (System und Verfahren zur gesicherten

Behandlung von Kontrollinformationen) und umfasst 12 Patentansprüche, die alle mit der Nichtigkeitsklage angegriffen sind.

Die nebengeordneten Patentansprüche 1 und 8 lauten nach der Streitpatentschrift EP 1 404 085 B1 wie folgt:

1. A system for securely handling control information, comprising:

An integrated circuit (30) comprising a content processing block (170) and a control processing block (130), the content processing block (170) being coupled to the control processing block (130),
wherein the integrated circuit (30) is operable to receive content and associated control information,
wherein the control processing block (130) is adapted to validate the authenticity of the control information received by the integrated circuit (30), and
wherein the content processing block (170) is adapted to process the content received by the integrated circuit (30) to content output sent from the integrated circuit (30) in accordance with the validated control information;

8. A method for securely handling control information, comprising:

(a) validating (200) the control information;
(b) decoding (210) the validated control information; and
(c) configuring a content processor of an application specific integrated circuit, ASIC based on the decoded control information,

wherein the validating, the decoding and the configuring are performed with the application specific integrated circuit ASIC,
characterized in that
the method further comprises
modifying (250) the control information.

In deutscher Übersetzung nach der Streitpatentschrift (EP 1 404 085 B1) lauten die Patentansprüche 1 und 8:

1. System zum gesicherten Behandeln von Steuerungsinformationen, welches aufweist:

eine integrierte Schaltung (30), die einen Inhaltverarbeitungsblock (170) und
einen Steuerungsverarbeitungsblock (130) aufweist, wobei der Inhaltverarbeitungsblock (170) mit dem Steuerungsverarbeitungsblock (130) gekoppelt ist,
wobei die integrierte Schaltung (30) betreibbar ist, um Inhalt und zugeordnete Steuerungsinformationen zu empfangen,
wobei der Steuerungsverarbeitungsblock (130) dazu ausgelegt ist, die Authentizität der von der integrierten Schaltung (30) empfangenen Steuerungsinformationen zu validieren, und
wobei der Inhaltverarbeitungsblock (170) dazu ausgelegt ist, den von der integrierten Schaltung (30) empfangenen Inhalt in Inhaltsausgänge von der integrierten Schaltung (30) gemäß der validierten Steuerungsinformationen zu verarbeiten;
dadurch gekennzeichnet, dass
die integrierte Schaltung (30) ferner einen Steuerungsmodifizierungsblock (150) aufweist, der dazu ausgelegt ist, die von der integrierten Schaltung (30) empfangenen Steuerungsinformationen zu modifizieren.

8. Verfahren zum gesicherten Behandeln von Steuerungsinformationen, welches umfasst:

(a) Validieren (200) der Steuerungsinformationen;
(b) Decodieren (210) der validierten Steuerungsinformationen; und
(c) Konfigurieren eines Inhaltprozessors einer anwendungsspezifischen integrierten Schaltung, ASIC, auf der Grundlage der decodierten Steuerungsinformationen,

wobei das Validieren, das Decodieren und das Konfigurieren mit der anwendungsspezifischen integrierten Schaltung, ASIC, durchgeführt werden,
dadurch gekennzeichnet, dass
das Verfahren ferner aufweist:

Modifizieren (250) der Steuerungsinformationen.

Wegen der auf Patentanspruch 1 rückbezogenen Unteransprüche 2 bis 7 und der Patentansprüche 9 bis 12, die sich auf den Verfahrensanspruch 8 beziehen, wird auf die Streitpatentschrift Bezug genommen.

Mit ihrer Klage vom 20. November 2018 macht die Klägerin geltend, das Streitpatent sei mangels Patentfähigkeit für nichtig zu erklären, da seine Gegenstände gegenüber dem Stand der Technik nicht neu seien, jedenfalls aber dem Fachmann zum Prioritätszeitpunkt nahegelegen hätten und somit nicht auf einer erfinderischen Tätigkeit beruhten. Mit der Replik vom 12. Mai 2020 hat die Klägerin zudem gerügt, der Gegenstand des Streitpatents gehe über den Offenbarungsgehalt der Ursprungsanmeldung (belegt als Druckschrift NK4) hinaus, da die Aufnahme der Merkmale 1.2c in Anspruch 1 bzw. 8.1d in Anspruch 8 jeweils eine unzulässige Zwischenverallgemeinerung darstellten (vgl. hierzu die Gliederung im Abschnitt II.).

Ihren Vortrag zur fehlenden Patentfähigkeit stützt die Klägerin unter anderem auf folgende Druckschriften:

D1 WO 02 / 056 535 A1
D1a Englische Übersetzung der Druckschrift WO 02 / 056 535 A1 (D1)
D2 EP 1 265 396 A1
D3 WO 00 / 59 150 A2
D4 US 5,796,828 A
D5 EP 0 924 930 A2
D6 WO 02 / 01 326 A2

Die Klägerin beantragt,

> das europäische Patent 1 404 085 (DE 603 09 647) mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland in vollem Umfang für nichtig zu erklären.

Die Beklagte beantragt,

> die Klage nach Maßgabe des Hauptantrags vom 28. August 2020 abzuweisen,
> hilfsweise nach Maßgabe der Hilfsanträge 1 bis 4, überreicht mit Schriftsatz vom 28. August 2020, sowie der Hilfsanträge 5 und 6, überreicht in der mündlichen Verhandlung,
> weiter hilfsweise im Umfang des Anspruchs 1 und der darauf rückbezogenen Ansprüche des Hauptantrags und der Hilfsanträge vom 28. August 2020.

Die Klägerin hält die Nichtigkeitsklagen auch gegenüber den Fassungen aufrecht, mit denen die Beklagte das Streitpatent hilfsweise verteidigt.

In der Fassung nach dem Hauptantrag ist Patentanspruch 1 identisch mit der erteilten Fassung, Patentanspruch 8 lautet wie folgt (Änderung gegenüber der erteilten Fassung farblich und unterstrichen):

8. A method for securely handling control information, comprising:

(a) validating (200) the -authenticity of the control information;
(b) decoding (210) the validated control information; and
(c) configuring a content processor of an application specific integrated circuit, ASIC based on the decoded control information,
wherein the validating, the decoding and the configuring are performed with the application specific integrated circuit ASIC,
characterized in that
the method further comprises modifying (250) the control information.

a) Hilfsantrag 1

In der Fassung nach dem Hilfsantrag 1 lautet der Patentanspruch 1 und der nebengeordnete Patentanspruch 8, gemäß mit Schriftsatz vom 28.08.2020 eingereichter Fassung jeweils wie folgt (Änderungen gegenüber dem Hauptantrag farblich und unterstrichen hervorgehoben):

1. A system for securely handling control information, comprising:

An integrated circuit (30) comprising a content processing block (170) and a control processing block (130), the content processing block (170) being coupled to the control processing block (130), and

an input interface (50) coupled to the integrated circuit (30) and adapted to be coupled to an input connection (100),

wherein the integrated circuit (30) is operable to receive content and associated control information included in frames carried through the input connection (100) from a central content provider,

wherein the control processing block (130) is adapted to validate the authenticity of the control information received by the integrated circuit (30), and

wherein the content processing block (170) is adapted to process the content received by the integrated circuit (30) to content output sent from the integrated circuit (30) in accordance with the validated control information;

characterized in that

the integrated circuit (30) further comprises a control modifying block (150) adapted to modify the control information received by the integrated circuit (30).

8. A method for securely handling control information, comprising:

(~~a~~a) receiving content and control information included in frames carried through an input connection (100) from a central content provider;

(b) validating (200) the authenticity of the control information;

(~~b~~c) decoding (210) the validated control information; and

(~~c~~d) configuring a content processor of an application specific integrated circuit, ASIC based on the decoded control information,

wherein the validating, the decoding and the configuring are performed with the application specific integrated circuit ASIC, wherein the ASIC is coupled through an input interface (50) to the input connection (100),

characterized in that

the method further comprises modifying (250) the control information.

b) Hilfsantrag 2

In der Fassung nach dem Hilfsantrag 2 lautet der Patentanspruch 1 und der nebengeordnete Patentanspruch 7, gemäß mit Schriftsatz vom 28.08.2020

eingereichter Fassung jeweils wie folgt (Änderungen gegenüber dem Hilfsantrag 1 farblich und unter- /durchgestrichen hervorgehoben):

1. A system for securely handling control information, comprising:

An integrated circuit (30) comprising a content processing block (170) and a control processing block (130), the content processing block (170) being coupled to the control processing block (130), and

an input interface (50) coupled to the integrated circuit (30) and adapted to be coupled to an input connection (100),

wherein the integrated circuit (30) is operable to receive content and associated control information included in frames carried through the input connection (100) from a central content provider,

wherein the control processing block (130) is adapted to validate the authenticity of the control information received by the integrated circuit (30), and

wherein the content processing block (170) is adapted to process the content received by the integrated circuit (30) to content output sent from the integrated circuit (30) in accordance with the validated control information;

characterized in that

the integrated circuit (30) further comprises a control modifying block (150) adapted to modify the control information received by the integrated circuit (30) and

the integrated circuit (30) further comprises an authentication application block (160) adapted to authenticate the modified control information.

~~7~~8. A method for securely handling control information, comprising:

(~~a~~a) receiving content and control information included in frames carried through an input connection (100) from a central content provider;

(b) validating (200) the authenticity of the control information;

(~~b~~c) decoding (210) the validated control information; and

(~~c~~d) configuring a content processor of an application specific integrated circuit, ASIC based on the decoded control information,

wherein the validating, the decoding and the configuring are performed with the application specific integrated circuit ASIC, wherein the ASIC is coupled through an input interface (50) to the input connection (100),

characterized in that

the method further comprises modifying (250) the control information and authenticating (260) the modified control information.

c) Hilfsantrag 3

In der Fassung nach dem Hilfsantrag 3 lautet der Patentanspruch 1 und der nebengeordnete Patentanspruch 8, gemäß mit Schriftsatz vom 28.08.2020 eingereichter Fassung jeweils wie folgt (Änderungen gegenüber dem Hauptantrag farblich und unter- /durchgestrichen hervorgehoben):

1. A system for securely handling control information, comprising:

An integrated circuit (30) comprising a content processing block (170) and a control processing block (130), the content processing block (170) being coupled to the control processing block (130),

wherein the integrated circuit (30) is operable to receive content and associated control information,

wherein the control processing block (130) is adapted to validate the authenticity of the control information received by the integrated circuit (30), wherein the control information includes a key that links the control information to source and destination points, and

wherein the content processing block (170) is adapted to process the content received by the integrated circuit (30) to content output sent from the integrated circuit (30) in accordance with the validated control information;

characterized in that

the integrated circuit (30) further comprises a control modifying block (150) adapted to modify the control information received by the integrated circuit (30).

8. A method for securely handling control information, comprising:

(a) validating (200) the authenticity of the control information, wherein the control information includes a key that links the control information to source and destination points;

(b) decoding (210) the validated control information; and

(c) configuring a content processor of an application specific integrated circuit, ASIC based on the decoded control information,

wherein the validating, the decoding and the configuring are performed with the application specific integrated circuit ASIC,

characterized in that

the method further comprises modifying (250) the control information.

d) Hilfsantrag 4

In der Fassung nach dem Hilfsantrag 4 lautet der Patentanspruch 1 und der nebengeordnete Patentanspruch 8, gemäß mit Schriftsatz vom 28.08.2020

eingereichter Fassung jeweils wie folgt (Änderungen gegenüber dem Hauptantrag farblich und unterstrichen hervorgehoben):

1. A system for securely handling control information, comprising:

An integrated circuit (30) comprising a content processing block (170) and a control processing block (130), the content processing block (170) being coupled to the control processing block (130),

wherein the integrated circuit (30) is operable to receive content and associated control information,

wherein the control processing block (130) is adapted to validate the authenticity of the control information received by the integrated circuit (30), wherein validating the authenticity includes authenticating a link between the control information and the associated content to verify that the control information has not been modified and a key that links the control information to the authentication of the source and destination points as well as the means to unlock access to the corresponding content, and

wherein the content processing block (170) is adapted to process the content received by the integrated circuit (30) to content output sent from the integrated circuit (30) in accordance with the validated control information;

characterized in that

the integrated circuit (30) further comprises a control modifying block (150) adapted to modify the control information received by the integrated circuit (30).

8. A method for securely handling control information, comprising:

(a) validating (200) the authenticity of the control information, wherein validating the authenticity includes authenticating a link between the control information and the associated content to verify that the control information has not been modified and a key that links the control information to the authentication of the source and destination points as well as the means to unlock access to the corresponding content;

(b) decoding (210) the validated control information; and

(c) configuring a content processor of an application specific integrated circuit, ASIC based on the decoded control information,

wherein the validating, the decoding and the configuring are performed with the application specific integrated circuit ASIC,

characterized in that

the method further comprises modifying (250) the control information.

e) Hilfsantrag 5

In der Fassung nach dem Hilfsantrag 5, wie er in der mündlichen Verhandlung überreicht worden ist, lautet der Patentanspruch 1 wie folgt (Änderungen zur Fassung gemäß Hauptantrag unterstrichen hervorgehoben):

1. A system for securely handling control information, comprising:

An integrated circuit (30) comprising a content processing block (170) and a control processing block (130), the content processing block (170) being coupled to the control processing block (130),

wherein the integrated circuit (30) is operable to receive content and associated control information,

wherein the control processing block (130) is adapted to validate the authenticity of the control information received by the integrated circuit (30), wherein the control data is validated according to an authentication algorithm in the control processing block (130), wherein the authentication also includes a key that links it to the authentication of the source and destination points and

wherein the content processing block (170) is adapted to process the content received by the integrated circuit (30) to content output sent from the integrated circuit (30) in accordance with the validated control information;

characterized in that

the integrated circuit (30) further comprises a control modifying block (150) adapted to modify the control information received by the integrated circuit (30).

Der nebengeordnete Patentanspruch 8 entspricht dem Patentanspruch 8 gemäß Hauptantrag.

f) Hilfsantrag 6

In der Fassung nach dem Hilfsantrag 6, wie er in der mündlichen Verhandlung überreicht worden ist, lautet der Patentanspruch 1 wie folgt (Änderungen zur Fassung gemäß Hauptantrag unterstrichen hervorgehoben):

1. A system for securely handling control information, comprising:

An integrated circuit (30) comprising a content processing block (170) and a control processing block (130), the content processing block (170) being coupled to the control processing block (130),

wherein the integrated circuit (30) is operable to receive content and associated control information,

wherein the control processing block (130) is adapted to validate the authenticity of the control information received by the integrated circuit (30), wherein the control data is validated according to an authentication algorithm in the control processing block (130), wherein the authentication also includes a key that links it to the authentication of the source and destination points as well as the means to unlock access to the corresponding content and

wherein the content processing block (170) is adapted to process the content received by the integrated circuit (30) to content output sent from the integrated circuit (30) in accordance with the validated control information;

characterized in that

the integrated circuit (30) further comprises a control modifying block (150) adapted to modify the control information received by the integrated circuit (30).

Der Patentanspruch 8 entspricht dem Patentanspruch 8 gemäß Hauptantrag.

Die Beklagte tritt dem Vorbringen der Klägerin in allen Punkten entgegen. Die erstmals in der mündlichen Verhandlung erfolgten Ausführungen der Klägerin zum Begriff „EKB“ stellten ein neues Vorbringen dar, das die Vertagung der mündlichen Verhandlung erfordere, zumindest aber Schriftsatznachlass. Der Gegenstand des

Streitpatents sei patentfähig, denn sein Gegenstand sei gegenüber dem im Verfahren befindlichen Stand der Technik neu und beruhe ausgehend davon auf einer erfinderischen Tätigkeit. Jedenfalls in der Fassung nach einem der Hilfsanträge habe das Streitpatent daher Bestand.

Mit einem Hinweis nach § 83 Abs. 1 PatG vom 3. August 2020 hat der Senat den Parteien die Gesichtspunkte mitgeteilt, die für die Entscheidung voraussichtlich von besonderer Bedeutung sind.

E n t s c h e i d u n g s g r ü n d e

A.

Die Klage ist zulässig und auch begründet. Soweit die Beklagte die erteilte Fassung nicht mehr verteidigt, ist das Streitpatent bereits ohne Sachprüfung für nichtig zu erklären. Es kann in der Fassung nach dem Hauptantrag mangels Patentfähigkeit ebenfalls keinen Bestand haben. Dies gilt darüber hinaus auch für die Fassungen sämtlicher Hilfsanträge, denn diese Gegenstände waren dem Fachmann am maßgeblichen Prioritätstag ausgehend von der Druckschrift D1/D1a bereits bekannt bzw. nahegelegt.

I.

1. Das Streitpatent befasst sich laut Absatz [0002] damit, dass digitale oder analoge Inhalte durch die Verwendung von Steuerungsinformationen wie z. B. Digitale Rechteverwaltung-Steuerungen ("Digital Rights Management"; DRM) und Kopiersteuerungsinformationen ("Copy Control Information"; CCI) gesichert und beschränkt werden könnten. DRM- oder CCl-Steuerungen begleiteten die Inhalte unabhängig davon, ob es sich bei den Inhalten um eine Komponente eines einzelnen Inhalts (z.B. eine Videokomponente) oder um eine Gruppe von

Komponenten (z.B. eine Videokomponente, eine Audiokomponente und eine Datenkomponente), die eine Multimedia-Präsentation bilden, handele.

DRM- und CCl-Steuerungen seien häufig (z.B. über eine kryptografische Verbindung, eine Zeigerstruktur, die auf eine Programmnummer, ein Wasserzeichen usw. hinweist) mit dem Inhalt verknüpft, den sie steuern und der gegen unbefugte Eingriffe geschützt werden müsse. Die Steuerungsinformationen könnten durch eine angewendete Authentifizierung geschützt werden, welche die Verbindung zwischen den Steuerungsinformationen und den zugeordneten Inhalten authentisiere, um zu verifizieren, dass die DRM- und CCl-Steuerungen nicht modifiziert wurden. Bei einer Verarbeitung von DRM- und CCl-Steuerungen in einer herkömmlichen reinen Software-Umgebung seien die Steuerungsinformationen jedoch noch anfälliger gegen unbefugte Eingriffe oder Hacken. Ferner könnten andere Systeme, die Firmensysteme mit bedingtem Zugriff anwenden, versuchen, die Steuerungsinformationen mit bedingtem Zugriff in Hardware zu schützen, die gegen unbefugte Eingriffe immun sei; die gegen unbefugte Eingriffe immune Hardware sei jedoch separat von der eigentlichen lnhaltverarbeitungs-ASIC, was die letztliche Konfiguration der lnhaltverarbeitungs-ASIC für unbefugte Eingriffe durch nicht vertrauenswürdige Parteien zugänglich lasse. Darüber hinaus könne es sein, dass herkömmliche Systeme nicht in der Lage sind, die Steuerungsinformationen auf gesicherte Weise durch eine vertrauenswürdige Partei zu modifizieren. Weitere Einschränkungen und Nachteile von herkömmlichen und traditionellen Lösungsansätzen ergäben sich für den Durchschnittsfachmann aus einem Vergleich solcher Systeme mit Aspekten der vorliegenden Erfindung (Streitpatent, Abs. [0003] und [0004]).

Die als Stand der Technik zitierte Druckschrift US-A-6,055,314 betreffe ein System und ein Verfahren für den gesicherten Kauf und die gesicherte Zustellung von Videoinhaltprogrammen in Verbindung mit Entschlüsselungsfähigkeiten, wogegen die US 2002 / 012 432 A1 eine Rechenvorrichtung mit einem digitalen Rechteverwaltungssystem zeige, wobei ein geschützter digitaler Inhalt auf der Rechenvorrichtung dargestellt werde. Die US-A-6,064,739 zeige einen sicheren Videoinhaltprozessor, der verschlüsselte digitale Videoinformationen empfange, sie

in analoge Informationen für einen Monitor konvertiere und dabei einen unbefugten Zugriff auf die unverschlüsselten intermediären digitalen Daten verhindere (Streitpatent, Abs. [0005] bis [0007).

2. Als Aufgabe wird im Streitpatent genannt, Steuerungsinformationen, die lnhaltsinformationen zugeordnet sind, gemäß der tatsächlichen Verwendung der lnhaltsinformationen zu modifizieren (vgl. Streitpatent, Abs. [0008]). Darunter ist im dort beschriebenen technischen Kontext zu verstehen, dass zumindest Teile einer Steuerungsinformation („control information“) in einem Sytem und/oder Verfahren je nach der Nutzung digitaler Daten (wie z.B. Audio-/Videodateien) durch einen Nutzer gemäß im Vorfeld festgelegter Randbedingungen zu aktualisieren sind. Als Beispiel im Streitpatent dient hierfür die Limitierung von nutzerseitig erstellbaren Kopien digitaler Daten von einer diese Daten zur Verfügung stellenden Einheit, in der die Steuerungsinformation als eine Art Zähler fungiert, der entsprechend der Anzahl bereits erfolgter Kopien zu aktualisieren ist (Streitpatent, Abs. [0042], [0050] und [0051]).

3. Das Streitpatent richtet sich an einen Diplom-Ingenieur der Elektrotechnik oder Nachrichtentechnik, der mehrjährige Erfahrung in der Konzeption und Umsetzung von Sicherheitsmaßnahmen im Rahmen von digitaler Mediendistribution bzw. deren Zurverfügungstellung besitzt, was auch die Berücksichtigung von Fragen digitaler Rechteverwaltung mit einschließt.

II. Zur Fassung nach dem Hauptantrag

Die Fassung nach Hauptantrag ist nicht zur Selbstbeschränkung des erteilten Patents geeignet, da der mit der Klage geltend gemachte Nichtigkeitsgrund der fehlenden Patentfähigkeit nach Art. II §6 Abs. 1 Nr. 1 IntPatÜG, Art. 138 Abs. 1 a) EPÜ i.V.m Art. 52 bis 56 EPÜ gegeben ist.

1. Der Gegenstand der in der Fassung gemäß Hauptantrag verteidigten Patentansprüche 1 und 8 lässt sich jeweils in folgende Merkmale gliedern:

Patentanspruch 1

1.1	A system for securely handling control information, comprising:
1.2	An integrated circuit operable to receive content and associated control information, comprising
1.2a	a control processing block, adapted to validate the authenticity of the control information received by the integrated circuit,
1.2b	a content processing block coupled to the control processing block, adapted to process the content received by the integrated circuit to content output sent from the integrated circuit in accordance with the validated [control] information,
1.2c	a control modifying block adapted to modify the control information received by the integrated circuit.

Patentanspruch 8

8.1	A method for securely handling control information, comprising:
8.1a$_{HP}$	validating the authenticity of the control information;
8.1b	decoding the validated [control] information; and
8.1c	configuring a content processor of an application specific integrated circuit, ASIC, based on the decoded control information,
8.1d	modifying the control information
8.2	wherein the validating, the decoding and the configuring are performed with the application specific integrated circuit ASIC.

2. Der Senat legt den Patentansprüchen 1 und 8 folgendes Verständnis zugrunde:

Zum Systemanspruch 1

Unter einem „System for securely handling control information" ist vor dem technischen Hintergrund, wie er durch das Streitpatent beschrieben ist, eine Ansammlung von mehreren elektronischen Bausteinen und/oder Software-prozeduren zu verstehen, die beispielsweise im Rahmen des Digital Rights Management (DRM) und/oder der Copy Control Information (CCI) geeignet verschaltet bzw. verknüpft Verwendung findet (Streitpatent, Abs. [0002] - [0004]). Bei der so genannten „control information" handelt es sich um sicherheitsrelevante Steuerungsinformation(en), z.B. diejenigen, die mit DRM verbundene (Ab-)Fragen bzw. Steuerungsabläufe betreffen und/oder den Kopierschutz von digitalen Daten im Rahmen von CCI (Merkmal **1.1**).

Allgemein betrachtet realisieren DRM nutzende Systeme eine Zugriffskontrolle auf digitale Inhalte (hier: „content information" / Inhaltsdaten) über kryptografische Verfahren, wobei ein digitaler Inhalt durch Verschlüsselung eindeutig an eine wie auch immer geartete Lizenz gebunden wird. Möchte der Benutzer auf einen per DRM geschützten Inhalt zugreifen, fordert z.B. die DRM-Steuerung eines Gerätes vom Lizenzserver die oder eine zur Wiedergabe notwendige Lizenz an (diese kann auch selbst eine Steuerungsinformation („control information") oder Teil einer solchen sein) oder sucht danach auf dem genutzten Abspielgerät. Werden mit dieser und/oder auch anderen Komponenten Authentizität und/oder Integrität des jeweiligen Wiedergabeprogramms und/oder (in Zusammenhang damit bzw. separat die) des Nutzers verifiziert, werden die Inhalte oft mit einem in der Lizenz enthaltenen Schlüssel entschlüsselt, auf diese Weise lesbar gemacht und an das Wiedergabeprogramm geleitet. Existiert z.B. eine nur einmalige Abspiellizenz für einen konkreten digitalen Film auf einem konkreten Gerät, so muss nach/während dem Abspielen seines digitalen Inhalts auch eine Modifizierung an den diesen Aspekt betreffenden Steuerungsdaten für den Film vorgenommen werden, damit ein erneutes Abspielen softwaretechnisch unterbunden werden kann.

Für das streitpatentgemäße System gelten mit den anschließenden Merkmalen hierfür folgende Vorgaben:

Ein Baustein des streitpatentgemäßen Systems ist ein „integrated circuit" (IC), der einen an diesem anliegenden, nicht weiter bestimmten digitalen Inhalt und diesem Inhalt zugeordnete Steuerungsinformationen empfangen kann und selbst aus (mindestens) drei weiteren Komponenten besteht bzw. drei Softwareprozeduren in sich trägt (Merkmal **1.2**).

Die erste der Komponenten bzw. Prozeduren wird als „control processing block" bezeichnet und dient zu einer streitpatentgemäßen Überprüfung der Echtheit / Validierung der Authentizität („to validate the authenticity“) der vom IC empfangenen Steuerungsinformationen (Merkmal **1.2a**). Was unter einer streitpatentgemäßen Validierung der Authentizität konkret zu subsummieren ist, ist zwischen den Parteien höchst umstritten:

Seitens der Beklagten wird sinngemäß die Meinung vertreten, dass der beanspruchte Wortlaut „to validate the authenticity of the control information“ nach fachmännischer Lesart bedeute, dass die Steuerungsdaten im Streitpatent daraufhin überprüft werden, ob sie von einer dort angegebenen Quelle erstellt wurden. Zwar kann der übliche fachliche Sprachgebrauch Anhaltspunkte für das Verständnis des Fachmanns geben, aber nur, wenn der Inhalt des Streitpatents auf kein abweichendes Verständnis hindeutet (vgl. BGH Urteil vom 7. Juli 2015 X ZR 64/13 - Bitdatenreduktion, Rn. 13). Beim Streitpatent ist dies jedoch – wie die Klägerin zurecht ausführt – der Fall, da in seinem Absatz [0003] eine Definition von „authenticate" (insb.: „The control information may be protected by an applied authentication that authenticates the link between the control information and the associated content to verify that the DRM and the CCI controls have not been modified") gegeben wird. Das Ausführungsbeispiel in den Absätzen [0049] und [0050] i.V.m. der Figur 4 unterstützt diese streitpatentspezifische andere Lesart des Merkmals.

Im Einzelnen wird nämlich im Absatz [0049], Zeilen 43 bis 46, thematisiert, dass die Authentifizierung einen Schlüssel enthalten kann („may"), der sie mit der Authentifizierung der Quell- und Zielpunkte sowie den Mitteln zum Entsperren des Zugriffs auf den entsprechenden Inhalt verknüpft. Die fachübliche Lesart, dass die Quelle Teil der Authentisierung ist, ist somit nicht zwingend erforderlich. Auch das Ausführungsbeispiel in Absatz [0050] in Verbindung mit Figur 4 rechtfertigt eine breitere Lesart. Danach gehört z.B. die mögliche Anzahl von Kopien zu den Steuerungsdaten, bspw., wenn ein Inhalt nur einmal kopiert werden kann, werden die Steuerungsdaten modifiziert (von „one copy permitted“ auf „no more copying permitted“) und anschließend derselbe Authentisierungsalgorithmus wie beim Empfang der Steuerungsdaten auf die modifizierten Steuerungsdaten angewendet. Als Ergebnis wird ein Kontrollwort, ein Authentisierungscode, ein Wasserzeichen oder ähnliches den aktualisierten Steuerungsdaten beigefügt. In Absatz [0051] des Streitpatents werden weitere Datentypen, die - neben der optionalen Quelle und der Anzahl der Kopien - Bestandteil der Steuerungsdaten sein können, genannt („analog component output"; „digital signal output“; „uncompressed"; „compressed", „copy rights"; „output resolution'), die sämtlich unter den Wortlaut des Merkmals 1.2a fallen.
Daher sieht der Senat eine breitere, nicht auf die fachübliche Lesart des Begriffes „to validate the authenticity" beschränkte, Auslegung als geboten an.

Die zweite beanspruchte Komponente bzw. Prozedur wird als „content processing block" bezeichnet und ist mit dem „control processing block" verknüpft. Sie dient zur Verarbeitung des vom IC empfangenen Inhalts - also den eigentlichen Nutzdaten, wie etwa den Audio-/Videodaten eines digitalen Films. Dabei wird mittels der validierten (d.h. nach vorangegangenem Schritt authentizierten) Steuerungsinformationen der Inhalt für die dafür vorgesehenen Ausgänge („content output") aufbereitet (Merkmal **1.2b**).

Die dritte Komponente wird als "modifying block" bezeichnet und hat die Aufgabe, vom IC empfangene Steuerungsinformationen auf nicht weiter festgelegte Weise zu

modifizieren, wie beispielsweise einen Kontrollwert oder Zähler im Rahmen des Kopierschutzes eines Filmes inhaltlich zu ändern, um dadurch sein erneutes Abspielen bei einem weiteren Aufruf zu unterbinden (Merkmal **1.2c**).

Zum nebengeordneten Verfahrensanspruch 8:

Da der mit dem Hauptantrag verteidigte Gegenstand des Patentanspruchs 8 letztlich nur das zum Systemanspruch 1 zugehörige Verfahren darstellt, gilt mit derselben Begründung für die entsprechenden Verfahrensmerkmale das zum Patentanspruch 1 Ausgeführte in analoger Weise.

3. Der Gegenstand des Patentanspruchs 1 nach Hauptantrag ist nicht neu.

Die PCT-Anmeldung WO 02/056 535 A1 (**D1**), die in japanischer Sprache veröffentlicht worden ist - und zu der die Klägerin eine englischsprachige Übersetzung eingereicht hat (**D1a**), welche den folgenden Ausführungen textlich zugrunde gelegt wird - stellt ein System und ein Verfahren vor, das zur Umsetzung einer autorisierten Nutzung digitaler Inhalte (D1a, S. 1, 2. Abs.: „authorized use of content …“) dient, wobei für diesen Inhalt Schutzmaßnahmen festgelegt werden.

Der Schutz beruht u.a. auf der Nutzung, Überprüfung und ggf. notwendigen Anpassung eines so genannten „integrity check value (ICV)“, der Manipulationen an abzuspielenden oder zu nutzenden digitalen Datensätzen aufdecken helfen bzw. verhindern soll (D1a, S. 21, Abs. 3: „Next, an integrity check value (ICV) for preventing data from being falsified is described.“).

a) Der ICV ist hier nicht identisch mit DRM-Daten (oder einem DRM-Wert), welche sich gemäß der PCT-Anmeldung vielmehr aus so genannten „rights data“, „content ID“, und „encrypted content key“ zusammensetzen. Ein ICV ist laut Druckschrift D1/D1a ein unter Verwendung von DRM-Daten generierter Wert, um damit abzuspielende Daten mit einer Sicherheitsinformation zu kennzeichnen (vgl. D1a,

Fig. 12 und 14, „MEDIA 500, 700“) und innerhalb eines Abspielgeräts Überprüfungen dieser Daten in Form eines Vergleichs der in den abzuspielenden Daten und im Abspielgerät vorliegenden ICV-Werte vorzunehmen (vgl. D1a, Fig. 18, „DEVICE 800“, das ein „ENCRYPTION PROCESSING MEANS 810“ als streitpatentgemäßen „integrated circuit“ (IC) zur Verarbeitung von außen am Gerät 800 ankommenden Daten („RECORDING MEDIA 900“) aufweist. Stimmen diese beiden Werte überein, kann die Nutzung derselben im Rahmen weiterer durch die Komponenten 900 und 810 vorgegebener und/oder erzeugter Randbedingungen erfolgen und entsprechend geltender Vorgaben auch eine Aktualisierung von Parametern wie dem ICV-Wert und/oder der DRM-Daten – die letztlich beide als Steuerungsinformationen im Sinne des Streitpatents anzusehen sind – beinhalten (vgl. D1a, Fig. 17 bis 19 i.V.m. S. 43, Abs. 4 – S. 45, Abs. 5; Merkmale **1.1 und 1.2**).

Soweit die Beklagte verneint, dass mit dem „ENCRYPTION PROCESSING MEANS 810“ der Figur 18 der Druckschrift D1/D1a ein IC im streitpatentgemäßen Sinne verbunden ist, greift diese Auffassung nicht durch. Die Beschreibung der Druckschrift D1/D1a lehrt nämlich zum einen, dass selbiges mit dem „ENCRYPTION PROCESSING MEANS 150“ der Figur 1 übereinstimmt (D1a, S. 43 letzt. Abs. bis S. 44, Abs. 1: „… Fig. 18 shows an encryption processing means 810 (corresponding to the encryption processing means 150 in Fig. 1) …“; Unterstreichungen hinzugefügt), und zum anderen ausdrücklich, dass das „ENCRYPTION PROCESSING MEANS 150“ als einzelner Chip in Form eines LSI („Large Scale Integrated Circuit") und damit als integrierte Schaltung (IC) ausgeführt sein kann (D1a, S. 20, Abs. 2).

b) Die Lehre der Druckschrift D1/D1a ist nicht auf die oben genannten Maßnahmen beschränkt, sondern bedarf u.a. im Vorfeld der ICV-Betrachtung einer Reihe weiterer Teilnehmer, Parameter bzw. (Software-)Prozeduren. Insbesondere wird ein so genannter „enabling key block (EKB)“ (zu dessen Struktur vgl. D1a, Fig. 7), ein „enabling key block (EKB) key“, ein „key distribution center KDC“, ein „content key (K_c)“ und ein „encrypted content key $E_{EKB}(K_c)$“ beschrieben. Diese Parameter

sind gemäß den dortigen Figuren 11, 12, 14 und 17 bis 19 mit dem ICV bzw. untereinander und mit dem Freigeben oder Blocken von abspielbaren Daten verknüpft.

Gemäß der Lehre der Druckschrift D1/D1a wird als Grundvoraussetzung einer Mediendistribution zunächst von einem Distributor mittels einer dafür vorgesehenen Einheit ein Datenträger („MEDIA“, vgl. D1a, Fig. 11, rechts unten) erstellt und mit Sicherheitsmerkmalen versehen. Hierfür nutzt der Distributor einen als „authoring device 400“ bezeichneten Baustein (vgl. D1a, Fig. 12, linker Teil; S. 33, Abs. 3 ff.).

Hat dieser Baustein über eine geeignete Schnittstelle Nutzdaten erhalten, die letztlich an einem „user device“ abspielbar sein sollen (D1a, Fig. 11 (für die Struktur) und Fig. 17 (für den Ablauf) i.V.m. S. 32, Abs. 2: „The interface I/F 420 receives externally supplied digital signals representing various types of content such as pictures, sound, and programs, and outputs the signals to the bus 410.“), beschreibt er über eine weitere Schnittstelle („MEDIA I/F 490“) den Datenträger nicht nur mit diesen Nutzdaten in geeigneter Form (D1a, S. 32, Abs. 5, insb.: „Here, the media (recording medium) is, for example, an optical disk such as a DVD or a CD, a magnetooptical disk, a magnetic disk, a magnetic tape, or a digital-data recordable medium such as a semiconductor memory such as a RAM“; Unterstreichung hinzugefügt), sondern auch mit weiteren Daten (D1a, S. 31, vorl. Abs. - S. 33, Abs. 2). Diese weiteren Daten betreffen im Wesentlichen Sicherheits- und Copyrightaspekte.

Wird nun solch ein „MEDIA 500, 900“ (vgl. D1a, Fig. 12 und 18) zum Abspielen von Inhalten mit einem Abspielgerät („DEVICE 800“) verknüpft, werden die auf dem „MEDIA 500, 900“ abgespeicherten Steuerungsinformationen am Abspielgerät mittels der „MEDIA I/F 830“ empfangen und zum „ENCRYPTION PROCESSING MEANS 810“ geleitet, wo sie durch dessen funktionale Einheiten validiert und weiterverarbeitet werden. Dabei wird u.a. der dem abzuspielenden Inhalt zugeordnete DRM-Datensatz aus „MEDIA 500, 900“ ausgelesen (vgl. D1a, Seite

44, Abs. 2). Die ausgelesenen DRM-Daten finden in Folge Eingang in mehrere funktionale Einheiten der integrierten Schaltung (D1a, Fig. 18). Durch die funktionale Einheit „ICV GENERATOR 813“ der integrierten Schaltung (810) wird für die DRM-Daten auf Basis eines dem abzuspielenden Inhalt zugeordneten und ebenfalls ausgelesenen und der Schaltung zur Verfügung gestellten „integrity check value“ (ICV) sowie eines zugehörigen Schlüssels „ICV key“ ein ICV-Vergleichswert („ICV‘“) berechnet (D1a, Fig. 18 i.V.m. S. 44, Abs. 6: „Next, the device generates (S505) a verifying integrity-check value (ICV‘) in an ICV generating means (Calculate ICV) 813 ..., for the DRM data read from the user area …“). In einer weiteren funktionalen Einheit „ICV COMPARISON 814“ der integrierten Schaltung (810) wird der berechnete Vergleichswert ICV‘ dann mit dem ebenfalls aus „MEDIA“ ausgelesenen Wert ICV verglichen, um zu verifizieren, ob der DRM-Datensatz verändert wurde (D1a, Fig. 18 i.V.m. D1a, S. 44, Abs. 7 - bis S. 45, Z. 1: „Next, the generated verifying integrity-check value (ICV‘), and the ICV read from the media in step S502 are compared (S506)"). Stimmen diese beiden Werte überein, wird daraus gefolgert, dass die DRM-Daten (d.h. Steuerungsdaten im Sinne des Streipatents) nicht verändert wurden; in kausaler Konsequenz aus dieser Folgerung wird eine weitergehende Datenverarbeitung von Daten aus „MEDIA“ zugelassen (vgl. D1a, S. 47, Abs. 4: „When ICV = ICV‘ holds, it is determined that the DRM data is not falsified, and the process proceeds to the next step. When ICV = ICV‘ does not hold, it is determined that the DRM data is falsified, and the sequence of the subsequent playback processing flow is stopped and the process ends in a playback process error.“). Somit ist durch die Lehre der Druckschrift D1/D1a eine Validierung/Authentisierung von Steuerungsinformationen im streitpatentlichen Sinne realisiert (Merkmal **1.2a**).

Da in allen Einlassungen der Parteien das Merkmal 1.2a besonders kontrovers diskutiert wurde, sei die Druckschrift D1/D1a im Folgenden rein ergänzend auch gegenüber o.g. fachüblicher Lesart der Begrifflichkeit „to validate the authenticity (of the control information)“ betrachtet. Dazu bedarf es einer eingehenderen Analyse

des bereits eben genannten „enabling key block (EKB)“ (die auch im Rahmen weiterer Merkmale - auch anderer Antragsfassungen – von Bedeutung ist):

Gemäß Figur 12 der Druckschrift D1/D1a werden alle auf „MEDIA“ zu schreibende Daten in einer eine Dreiteilung darstellenden Weise auf dem Datenträger abgelegt und zwar in einem Bereich, der den „enabling key block (EKB)“ enthält, einem zweiten Bereich namens „PROTECTED AREA“ und einem dritten, der „USER AREA“ genannt wird. Der EKB wird dem „authoring device 400“ von einem externen „reliable key distribution center KDC“ für ein „valid user device“ zur Verfügung gestellt (und wie z.B. in den Figuren 4 bis 6 i.V.m. S. 22, letzt. Abs. bis S. 25, Abs. 2 beschrieben umgesetzt). Der EKB wird im „authoring device 400“ nicht weiter verändert und besteht aus mehreren Einzelkomponenten (D1a, S. 32, Abs. 6 – S. 33, Abs. 2, insb.: „… the authoring device receives unencrypted digital content, and a protection for the content, that is, an EKB including EKB keys (e.g., a root key, a key encryption key (KEK)) for use in encryption. The EKB is issued by a reliable key distribution center (KDC). The key distribution center KDC generates an EKB in which, … a root key as an encrypted key of a content key generated by a contents provider is set so as to be decrypted by only a valid user device. Based on information from an entity managed by each device, the key distribution center (KDC) can generate an EKB that can be decrypted by only a valid user device without directly knowing a stored key set of the device. An authoring entity as a contents provider receives rights data which is added to content and which includes use-restriction information such as the number of times copying is performed, and a content identifier (ID), …“; Unterstreichungen hinzugefügt).

Der EKB aus „MEDIA“ ist dergestalt konzipiert, dass er ausschließlich mit einer gültigen Lizenz entschlüsselt werden kann. Er wird somit aus fachmännischer Sicht zur Validierung einer Lizenz beim „user“, respektive auf dem Abspielgerät, verwendet (vgl. D1a, S. 33, Abs. 5, „a. EKB“: „The EKB is an EKB that can be decrypted by only a user having a valid license, that is, a right of valid use of content which is recorded in the media, and is issued by the key distribution center (KDC),

as described above. The EKB is recorded in the user area of media 500.“; Unterstreichungen hinzugefügt).

Der EKB stellt also mit eine Voraussetzung für das Abspielen von Daten beim „user“ dar und ist deshalb auch auf dem „DEVICE 800“ abgelegt, und zwar dort in Form des „DEVICE NODE KEY“, der dem „EKB PROCESSOR 811“ zuliefert, um entsprechend der in Figur 19 im Ablauf dokumentierten Prozedur abzufragen (vgl. auch D1a, S.44, Abs. 4 zu den Schritten „S502“ und „S503“), ob das Abspielgerät berechtigt ist, das „RECORDING MEDIA 900“ der Figur 18 auch abzuspielen (D1a, Fig. 17 bis 19 i.V.m. S. 42, Abs. 2, insb.: „The EKB is updated in cases such as device revocation … and is provided with a version number whenever updating is performed. In data-recordable media, the latest EKB version number is recorded in the user area since a content record using an EKB having an old version is revoked. Accordingly, the device executes comparison between the version of an EKB that it attempts to use and the EKB version recorded in the media, and becomes able to perform EKB-used content recording only when the version of the EKB for use is not older than the version recorded in the media.“; Unterstreichungen hinzugefügt).

Da der EKB auf dem Datenträger („MEDIA“) über seine Herkunft vom KDC letztlich auch die Quellenangabe eines vertrauenswürdigen Verteilers für ein „valid user device“ beinhaltet, bestätigt er somit, dass der Datenträger unter Mitwirkung einer unmittelbar in den am Beginn stehenden Speicherprozess eingebundenen und verlässlichen Quelle mit sicherheitsrelevanten Daten beschickt wird. Damit ist auch ein „to validate the authenticity“ auf dem Datenträger vorhandener Steuerungsdaten im o.g. fachüblichen Verständnis der Begrifflichkeit verwirklicht, d.h. im Sinne einer engeren Auslegung, wie sie die Beklagte vertritt.

c) Aus der Druckschrift D1/D1a ist auch ein streitpatentgemäßer „control processing block“ bekannt. Dieser ist dort zumindest mit all den beteiligten Komponenten des „ENCRYPTION PROCESSING MEANS 810“ zu identifizieren, die unter Einbeziehung und Verarbeitung des EKB die einem Abspielvorgang

vorgeschalteten Sicherheitsroutinen ausführen (vgl. D1a, Fig. 17 („content recording“-Ablauf), Fig. 18 (für den Abspielvorgang zugrundegelegte Struktur) und Fig. 19 („content playback“-Ablauf), insb. Bezugszeichen 811, 812, 813, 814 und 815).

Er validiert damit die Echtheit der Steuerungsinformationen, die ihm über die Schnittstelle „MEDIA I/F 830“ zugeführt werden, die bei erfolgreicher Validierung u.a. am „ENCRYPTION PROCESSOR 825“ anliegen und (letztlich auch über den ICV-Wert) sowohl quellenbezogene als auch inhaltsbezogene Informationen inkorporieren und die für den Entscheid über eine Freischaltung benötigt werden (z.B. D1a, S.5, Abs. 4 und S.11, Abs. 4 (für die MAC-Umsetzung, Quelle und Integrität werden geprüft)).

Neben dem EKB-Bereich auf „MEDIA“ wird - wie die Figur 12 der Druckschrift D1/D1a weiter zeigt - im zweiten Bereich („PROTECTED AREA“) der durch die „MEDIA WRITE UNIT“ des „AUTHORING DEVICE 400“ – unter Einbeziehung u.a. des „EKB KEY“ und von „DRM DATA“ – ermittelte ICV-Wert und ein durch den „KEY GENERATOR 421“ unabhängig generierter „ICV key“ abgespeichert. Der dritte Bereich („USER AREA“) umfasst die unter „DRM DATA“ zusammengefassten Rechte und den verschlüsselten Nutzdateninhalt („ENCRYPTED MUSIC CONTENT“).

Ist der ICV-Wert laut Lehre der Druckschrift D1/D1a im Abspielgerät („DEVICE 800“) verifiziert worden, d.h. ist das Abspielen der Nutzdaten aus sicherheitstechnischer Sicht zulässig, wird analog zum streitpatentgemäßen „content processing block“ ein weiterer funktionaler Bereich des „ENCRYPTION PROCESSING MEANS 810“ tätig, der in Folge den verschlüsselten Nutzdateninhalt entschlüsselt und dem Nutzer zum Abspielen zur Verfügung stellt (vgl. D1a, S. 46, Abs. 2 i.V.m. Fig. 18 und 19, Datenwege zum und vom „ENCRYPTION PROCESSOR 824, 825“ zum Ausgang „CONTENT“; Merkmal **1.2b**).

Ergänzend sei zu den diesbezüglichen Einlassungen der Beklagten ausgeführt, dass es auch aus Sicht des Senates zutrifft, dass der EKB in Anhängigkeit von bestimmten Randbedingungen durchaus nicht nur singulär für einen einzigen Empfänger der gewünschten Daten („valid user device“) Gültigkeit entfalten kann, sondern ggf. auch für eine Gruppe mit gleichen Zugriffsrechten auf ein „MEDIA“. Dies spielt beim gegebenen Merkmalswortlaut jedoch keine Rolle, kommt es doch auch bei der beklagtenseitigen engeren Auslegung der Begrifflichkeit „to validate the authenticity“ letztlich nur darauf an, dass an einem Empfänger technische Mittel realisiert sind, um nachzuvollziehen, von welcher Quelle diese Daten stammen, was mit der Lehre der Druckschrift D1/D1a zweifelsohne realisiert ist (erneut D1/D1a, Figuren 11, 12, 14 und 18).

d) Auch nach der mit der Druckschrift D1/D1a vermittelten Lehre kommt es – ist ein Abspielen als zulässig bewertet und eingeleitet worden – zu einem „UPDATE“ sicherheitsrelevanter Information(en) - d.h. Steuerungsinformation(en) im Sinne des Streitpatents (vgl. D1a, S. 45, Abs. 3 i.V.m. Fig. 18, rechts unten: „UPDATE ORIGINAL MEDIA“ und Fig. 19, insb. Schritte „S508“ und „S509“) - um sich mit einer Nutzung verändernde Rechte auf dem genutzten Datenträger zu dokumentieren (etwa einer um eins verminderten Abspielerlaubnis etc.) und sie so für einen ggf. weiteren Aufruf auf aktuellem Stand zu halten (Merkmal **1.2c**).

Damit ist der Gegenstand des mit Hauptantrag verteidigten Patentanspruchs 1 in allen seinen Merkmalen aus der Druckschrift D1/D1a bekannt.

Soweit die Beklagte vorgetragen hat, dass die Lehre der Druckschrift D1/D1a für den Streitgegenstand generell nicht herangezogen werden könne, da dort lediglich ganz allgemein ein Aufnehmen („recording“) und Wiedergeben („playback“) von Inhalten thematisiert werde und kein „streaming“ derselben über das Internet, so ist dies nicht entscheidungsrelevant, da der Wortlaut des eben abgehandelten Patentanspruchs 1 nirgends - und im Übrigen auch keiner der von diesem abhängigen Ansprüche - explizit ein „streaming“ benennt oder ein solches gar

konkret ausgestaltet.

Der in der mündlichen Verhandlung erstmalig ausführlich diskutierte Begriff „EKB“ rechtfertigt entgegen der Ansicht der Beklagten weder eine Vertagung noch einen Schriftsatznachlass. Es handelt sich um kein neues Angriffsmittel der Beklagten, sondern um eine Ausgestaltung innerhalb der Druckschrift D1/D1a, die in der dortigen Beschreibung breiten Raum einnimmt. Dabei ist es unerheblich, ob der Begriff „EKB“ im schriftsätzlichen Vortrag der Beklagten bereits erörtert wurde oder nicht. Die Beklagte hat in ihre Vorbereitung auf die mündliche Verhandlung die gesamte Offenbarung der jeweiligen Entgegenhaltung einzubeziehen, unabhängig davon, ob die Klägerin zu einem Merkmal darin bereits vorgetragen hat.

4. Da der mit dem Hauptantrag verteidigte Gegenstand des nebengeordneten Patentanspruchs 8 letztlich nur das zum Systemanspruch 1 zugehörige Verfahren darstellt, gilt mit derselben Begründung für die entsprechenden Verfahrensmerkmale das zum Patentanspruch 1 Ausgeführte in analoger Weise. Der Gegenstand des Patentanspruchs 8 kann somit ebenfalls keinen Bestand haben.

Ausführungen zu den abhängigen Patentansprüchen erübrigen sich an dieser Stelle, da die Beklagte den Anspruchssatz als Ganzes verteidigt und im Rahmen der beantragten Reihenfolge ihrer Hilfsanträge versucht, zur Patentfähigkeit der dort beanspruchten Gegenstände zu gelangen.

5. Bei dieser Sachlage kann es dahinstehen, ob die seitens der Klägerin vorgebrachten Mängel einer unzulässigen Erweiterung bzw. mangelnden ursprünglichen Offenbarung im Rahmen des Hauptantrags tatsächlich vorliegen.

III. Zu den Hilfsanträgen 1 bis 4 vom 28. August 2020

Die nebengeordneten Patentansprüche in der Fassung der Hilfsanträge 1 bis 4 sind mangels Patentfähigkeit nicht zur Selbstbeschränkung des Streitpatents geeignet.

1. Hilfsantrag 1

Der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 1 ist dem Fachmann aus der Druckschrift **D1/D1a** nahegelegt und beruht daher nicht auf einer erfinderischen Tätigkeit.

1.1 Angelehnt an die Merkmalsgliederung des Patentanspruchs 1 gemäß Hauptantrag lässt sich der Patentanspruch 1 in der Fassung des Hilfsantrags 1 mit folgenden Ergänzungen gliedern (Änderungen gegenüber der Version gemäß Hauptantrag fett hervorgehoben):

1.1

1.2$_{H1}$ the integrated circuit is operable to receive content and associated control information **included in frames carried through the input connection from a central content provider,**

1.2a – 1.2c

1.3$_{H1}$ **an input interface coupled to the integrated circuit and adapted to be coupled to an input connection**

Diesen Ergänzungen legt der Senat folgendes Verständnis zugrunde:

Das Merkmal **1.2$_{H1}$**, stellt darauf ab, dass die schon mit dem Hauptantrag beanspruchte Steuerungsinformation nun in „frames“ durch eine Eingabeverbindung von einem zentralen Inhalteanbieter („central content provider“) empfangen werden können soll.

Im Gegensatz zu den Ausführungen der Beklagten, die dieses Merkmal so verstanden wissen will, dass seitens des beanspruchten Systems eine direkte internetbasierte Verbindung zu einem Medienserver hergestellt wird, konkretisiert das Streitpatent nichts, auf das sich explizit diese Auslegung stützen ließe. Es wird dort in Absatz [0045] lediglich ganz allgemein offenbart, dass so genannte „frames“ über das „input interface 50“ empfangen werden können, und ein so genannter „central content provider“ Daten zu einem nicht weiter bestimmten „subscriber“ sendet. Eine weitergehende Definition dieser Begrifflichkeiten ist dem Streitpatent nicht zu entnehmen. Insbesondere ist dort kein Medien- oder anderer Server erwähnt, und auch keine spezielle Form der Datenübertragung thematisiert (z. B. paketorientiert, drahtgebunden, etc.). Daher umfasst für den Fachmann zum einen die Quelle der genannten Daten in natürlicher Weise z.B. auch eine CD oder DVD, in der Dateninhalte abgespeichert sind, die als „frames“ im Sinne des Streitpatents gelesen werden können, und zum anderen ist ohne weitere Erläuterung unter einem „subscriber“ nur ein nicht weiter bestimmtes Ziel für einen nicht näher spezifizierten Datentransfer zu verstehen.

Mit dem am Ende des Anspruchs ergänzten Merkmal **1.3$_{H1}$** wird für das System ganz allgemein eine Eingangsschnittstelle für einen IC und ein Anschluss an bzw. für einzulesende Daten beansprucht.

Aus der Druckschrift D1/D1a, Figur 1 (rechts unten) ist bekannt, dass ein Datenträger („MEDIA“) von einem Anbieter / Distributor existiert, und mittels eines „recording / playback device 100“ eine digitale Verbindung zu diesem hergestellt werden kann; damit ist das Merkmal **1.2$_{H1}$** gemäß obiger Auslegung bereits aus dieser Druckschrift bekannt (vgl. auch D1/D1a, Fig. 18 i.V.m S. 43, Abs. 4).

Es wird dort zusätzlich gelehrt, dass die Begrifflichkeit „MEDIA“ sich u.a. auch auf eine „structure capable of being built into the recording/playback device“ bezieht (D1a, S. 20, Abs. 4), was i.V.m. der dortigen Abhandlung des Standes der Technik

(D1a, S. 2, Abs. 3, insb.: „… there is a system configuration in which various types of content, such as music data, picture data, and game programs which are encrypted, are distributed to users by using the Internet“; Unterstreichung hinzugefügt) als Anregung dient, zur Kommunikation mit dem Datenträger bei Bedarf auch die Realisierung einer framebasierten Kommunikation vorzusehen. Damit sind sowohl die Begrifflichkeit „frames“ als auch ihre technischen Zusammenhänge, wie sie die Beklagte verstanden wissen will (s.o.), durch diese Druckschrift dem Fachmann zumindest nahegelegt (Merkmal **1.2$_{H1}$**).

Die mit dem Merkmal **1.3$_{H1}$** beanspruchte Eingangsschnittstelle für einen IC und der Anschluss an bzw. für einzulesende Daten ist ebenfalls aus der Druckschrift D1/D1a bekannt (D1a, Fig.1 i.V.m. S. 19, Abs. 4 bis S. 20, Abs. 2). Dort wird mit dem „MEDIA I/F 190“ im Rahmen des „recording/playback device 100“ eine Eingangsschnittstelle gezeigt, über die das „MEDIA“ als Dateneingabemittel in das „recording/playback device 100“ – und dort insbesondere mit dem als IC zu wertenden „ENCRYPTION PROCESSING MEANS (e.g. ENCRYPTION LSI) 150“ (vgl. Ausführungen zu Merkmal 1.2 in Abschnitt II.3 a) über den „bus 110“ in Verbindung tritt (Merkmal **1.3$_{H1}$**).

Somit beruht der Gegenstand des mit dem Hilfsantrag 1 verteidigten Patentanspruchs 1 nicht auf erfinderischer Tätigkeit ausgehend von der Lehre der Druckschrift D1/D1a.

1.2 Ausführungen zu den abhängigen Patentansprüchen und zum nebengeordneten Patentanspruch 8 erübrigen sich an dieser Stelle, da die Beklagte den Anspruchssatz als Ganzes verteidigt und im Rahmen der beantragten Reihenfolge ihrer Hilfsanträge versucht, zur Patentfähigkeit der dort beanspruchten Gegenstände zu gelangen.

1.3 Bei dieser Sachlage kann es auch dahinstehen, ob die seitens der Klägerin vorgebrachten Mängel einer unzulässigen Erweiterung bzw. mangelnden ursprünglichen Offenbarung im Rahmen des Hilfsantrags 1 tatsächlich vorliegen.

2. Hilfsantrag 2

Der Gegenstand des Patentanspruchs 1 wird durch die Druckschrift D1/D1a zusammen mit dem Fachwissen nahegelegt.

2.1 Angelehnt an die Merkmalsgliederung des Patentanspruchs 1 gemäß Hilfsantrag 1 lässt sich der Patentanspruch 1 in der Fassung des Hilfsantrags 2 mit folgenden Ergänzungen gliedern (Änderungen gegenüber der Version gemäß Hilfsantrag 1 fett hervorgehoben):

1.1. 1.2_{H1}, 1.2a – 1.2c

$1.2d_{H2}$ the integrated circuit further comprises an authentication application block adapted to authenticate the modified control information.

1.3_{H1}

Das hinzugefügte Merkmal **$1.2d_{H2}$** entspricht dem kennzeichnenden Merkmal des erteilten Unteranspruchs 2.

Der mit dem neuen Merkmal $1.2d_{H2}$ verbundene technische Sachverhalt, besagt, dass im IC ein Authentisierungsblock („authentication application block“) vorgesehen sein soll, um aktualisierte Steuerungsinformation („control information“ gemäß Merkmal 1.2c) zu authentisieren.

Dieser Sachverhalt ist insbesondere aus der Figur 18 der Druckschrift D1/D1a bekannt. Dort wird im Rahmen des „ENCRYPTION PROCESSING MEANS 810“ ein „UPDATE ORIGINAL MEDIA“ durchgeführt, in denen Aktualisierungen in Form

der dort genannten Parameter „ICV key“, „ICV“ und „DRM DATA“ vorgenommen werden, bevor diese in/auf den/einen Datenträger („MEDIA“) übertragen und dort gespeichert werden. Dabei geht der oben bereits als Authentisierungsnachweis beschriebene „EKB“ an unterschiedlichen Stellen der Datenverarbeitung des Systems mit in die Aktualisierung ein (vgl. Ausführungen zum Merkmal 1.2a des Hauptantrages und D1a, Fig. 18, dort die Datenwege, die in „UPDATE ORIGINAL MEDIA“ münden, insbesondere über die Bezugszeichen 821 - 825). Somit ist durch „EKB“ auch eine streitpatentgemäße Authentisierung aktualisierter bzw. modifizierter Steuerungsinformation(en) realisiert.

Somit beruht der Gegenstand des mit Hilfsantrag 2 verteidigten Patentanspruchs 1 nicht auf erfinderischer Tätigkeit gegenüber der Lehre der Druckschrift D1/D1a.

2.2 Ausführungen zu den abhängigen Patentansprüchen und zum nebengeordneten Patentanspruch 7 erübrigen sich an dieser Stelle, da die Beklagte den Anspruchssatz als Ganzes verteidigt und im Rahmen der beantragten Reihenfolge ihrer Hilfsanträge versucht, zur Patentfähigkeit der dort beanspruchten Gegenstände zu gelangen.

2.3 Bei dieser Sachlage kann es dahinstehen, ob die seitens der Klägerin vorgebrachten Mängel einer unzulässigen Erweiterung im Rahmen des Hilfsantrags 2 tatsächlich vorliegen.

3. Hilfsantrag 3

Der Gegenstand des Patentanspruchs 1 ist gegenüber der Druckschrift D1/D1a nicht neu.

3.1 Angelehnt an die Merkmalsgliederung des Patentanspruchs 1 gemäß Hauptantrag lässt sich der Patentanspruch 1 in der Fassung des Hilfsantrags 3 mit folgenden Ergänzungen gliedern (Änderungen gegenüber der Version gemäß Hauptantrag fett hervorgehoben):

1.1, 1.2, 1.2a

1.2a$_{H3}$ wherein the control information includes a key that links the control information to source and destination points,

1.2b, 1.2c

Das zum Patentanspruch 1 gemäß Hilfsantrag 3 gegenüber der Fassung nach Hauptantrag neu hinzugetretene Merkmal **1.2a$_{H3}$** beansprucht zusätzlich, dass ein Schlüssel die Steuerungsdaten („control information“) mit Quell- und Zielpunkten („source and destination points“) verknüpft.

Da weder im Streitpatent noch im beanspruchten Merkmalswortlaut ausgeführt ist, welchen konkreten Aufbau, welche expliziten Eigenschaften oder Funktionen ein dort ganz allgemein als „key“ bezeichneter Schlüssel beinhalten soll, und was in diesem Wirkzusammenhang explizit unter dem Verb „links“ zu subsummieren ist (vgl. Streitpatent, Abs. [0049]), ist im gegebenen Merkmalskontext beides allgemein, jedenfalls nicht unter Wortlaut, auszulegen. Zur Überzeugung des Senates wird mit der Begrifflichkeit „key“ daher lediglich beansprucht, dass ein nicht näher spezifizierter Schlüssel geeignet ist, Daten ausgehend von einer Quelle mit einem Ziel zu verknüpfen („links“). In der praktischen Umsetzung bedeutet dies, dass er im Rahmen von Steuerungsdaten als ein Sicherungsmittel dafür eingesetzt wird, ob Daten an einem Ziel entschlüsselt werden dürfen und können oder nicht.

Dieses Vorgehen ist in der Lehre der Druckschrift D1/D1a im Rahmen der Figur 18 durch die Arbeitsweise des so genannten „ENCRYPTION PROCESSING MEANS 810“ im Abspielgerät („DEVICE 800“) für das „RECORDING MEDIA 900“ verwirklicht, und zwar u.a. unter Einsatz von „ICV“ und „EKB“ sowie damit

verknüpften Parametern, wie dokumentiert durch die Figur 14 - für eine Quelle im Sinne des Streitpatents - mit dem dortigen „AUTHORING DEVICE 400“ beim Beschreiben und Verschlüsseln der Daten für „MEDIA 500“ (entspricht „RECORDING MEDIA 900“ der Figur 18) und „DEVICE NODE KEY“ (auf Seiten des Abspielgeräts), wie auch in den Ausführungen zu den vorangegangenen Anträgen bereits detailliert aufgeführt (vgl. u.a. die Funktionsaussagen der Merkmale 1.2a bis 1.2c und $1.2d_{H2}$ im Lichte der Figuren 11, 12, 14 und 18; Merkmal **$1.2a_{H3}$**).

Folglich ist der Gegenstand des mit Hilfsantrag 3 verteidigten Patentanspruchs 1 nicht neu gegenüber der Lehre der Druckschrift D1/D1a.

3.2 Ausführungen zu den abhängigen Patentansprüchen und zum nebengeordneten Patentanspruch 8 erübrigen sich an dieser Stelle, da die Beklagte den Anspruchssatz als Ganzes verteidigt und im Rahmen der beantragten Reihenfolge ihrer Hilfsanträge versucht, zur Patentfähigkeit der dort beanspruchten Gegenstände zu gelangen.

3.3 Bei dieser Sachlage kann es dahinstehen, ob die seitens der Klägerin vorgebrachten Mängel einer unzulässigen Erweiterung im Rahmen des Hilfsantrags 3 tatsächlich vorliegen.

4. Hilfsantrag 4

Der Gegenstand des Patentanspruchs 1 wird durch die Druckschrift D1/D1a neuheitsschädlich vorweggenommen.

4.1 Angelehnt an die Merkmalsgliederung des Patentanspruchs 1 gemäß Hauptantrag lässt sich der Patentanspruch 1 in der Fassung des Hilfsantrags 4 mit folgenden Ergänzungen gliedern (Änderungen gegenüber der Version gemäß Hauptantrag fett hervorgehoben):

1.1, 1.2, 1.2a

1.2a$_{H4_1}$ wherein validating the authenticity includes authenticating a link between the control information and the associated content to verify that the control information has not been modified

1.2a$_{H4_2}$ and a key that links the control information to the authentication of the source and destination points

1.2a$_{H4_3}$ as well as the means to unlock access to the corresponding content,

1.2b, 1.2c

Die zum Patentanspruch 1 neu hinzugetretenen Merkmale beanspruchen aus Sicht des Fachmanns im Einzelnen Folgendes:

- Merkmal **1.2a$_{H4_1}$**:
  Die Authentisierung eines „links“ zwischen Steuerungsinformation („control information“) und „associated content“, um sicherzustellen, dass die Steuerungsinformation unverändert ist. Dies bedeutet letztlich eine Integritätsprüfung der Steuerungsinformation, die nach obiger Auslegung von „to validate the authenticity“ nicht zwingend Quell(en)information enthält, also deren inhaltliche Unversehrtheit seit der Erstellung des Mediums / der Datei, die die Nutzdaten (wie etwa Video-/ Audiodaten) für den Nutzer enthält.

- Merkmal **1.2a$_{H4_2}$**:
  Den Einsatz eines Schlüssels, der die Steuerungsinformation zur Authentisierung von Quell- und Zielpunkt(en) verknüpft („link“). Zur Auslegung der Begrifflichkeit des Schlüssels („key“) sei auf die entsprechenden Ausführungen zum Hilfsantrag 3 verwiesen, denn diese sind mit derselben Begründung auch für das vorliegende Merkmal gültig, da die Begrifflichkeit „authenticating a link between the control information and the associated content …“ letztlich nicht über das, was datenverarbeitungstechnisch mit dem Merkmal 1.2a$_{H3}$ gemäß Hilfsantrag 3 verbunden ist, hinausgeht.

- Merkmal **1.2a$_{H4_3}$**:
  Dass der Einsatz des eben genannten Schlüssels zur Authentisierung der Mittel dient, die den Zugriff auf den sog. „corresponding content“ freigeben.

Aus der Druckschrift D1/D1a, Figuren 11, 12, 14 und 18 ist die Authentisierung eines „links“ zwischen Steuerungsinformation und „associated content“ bereits bekannt, insbesondere was die mit dem „EKB“ und dem letztlich daraus resultierenden „ICV“-Wert verbundenen Abfragen, Vergleiche und Aktualisierungsprozeduren anbelangt (und das selbst in Form der engen Auslegung wie sie die Beklagte zugrunde legt). In der Druckschrift D1/D1a wäre im Ergebnis kein erfolgreiches Abspielen von „CONTENT“ auf Seiten des Nutzers möglich, würden die Steuerungsdaten nicht zunächst auf ihre Unversehrtheit hin überprüft und nach erfolgter Bestätigung eine davon abhängige Entschlüsselung der Nutzdaten stattfinden, wie in den oben genannten Figuren gezeigt (Merkmal **1.2a$_{H4_1}$**).

Da von der Sachaussage her mit dem Merkmal **1.2a$_{H4_2}$** im Vergleich zum Merkmal 1.2a$_{H3}$ gemäß Hilfsantrag 3 letztlich nichts Anderes verbunden bzw. beansprucht ist als dort, wird zum Nachweis desselben in der Druckschrift D1/D1a auf die dortigen Ausführungen verwiesen (Merkmal **1.2a$_{H4_2}$**).

Über die von der Herstellerseite auf dem „MEDIA 900“ eingebrachten Schlüssel („EKB“ und damit verknüpfte Parameter), wird durch eine von „EKB“ angeleitete und auf Seiten des Abspielgeräts durch den „DEVICE NODE KEY“ veranlasste Prozedur, ein Entsperren der Nutzdaten verantwortet, sofern ein positiver Abgleich des ICV zwischen einzulesendem „MEDIA 900“ und im „DEVICE 800“ abgelegter ICV-Information erfolgt. Dies ist folglich auch als Authentisierung der Entschlüsselungsmittel i.e.S. anzusehen (vgl. insb. D1/D1a, Fig. 18, Datenwege zwischen den Bezugszeichen 811 – 815 und den „ENCRYPTION PROCESSOR(S) 824, 825“, die letztlich den „CONTENT“ (rechts unten) freigeben; Merkmal **1.2a$_{H4_3}$**).

Somit sind auch alle im Rahmen des Hilfsantrags 4 neu hinzugekommenen Merkmale bereits aus der Druckschrift D1/D1a bekannt.

Folglich führt auch eine Verteidigung des Streitpatents mit Hilfsantrag 4 nicht zum Erfolg, da der Gegenstand des antragsgemäßen Patentanspruchs 1 nicht neu gegenüber dem Stand der Technik ist, wie er durch die Druckschrift D1/D1a repräsentiert wird.

4.2 Ausführungen zu den abhängigen Patentansprüchen und zum nebengeordneten Patentanspruch 8 erübrigen sich an dieser Stelle, da die Beklagte den Anspruchssatz als Ganzes verteidigt und im Rahmen der beantragten Reihenfolge ihrer Hilfsanträge versucht, zur Patentfähigkeit der dort beanspruchten Gegenstände zu gelangen.

4.3 Bei dieser Sachlage kann es dahinstehen, ob die seitens der Klägerin vorgebrachten Mängel einer unzulässigen Erweiterung im Rahmen des Hauptantrags tatsächlich vorliegen.

IV. Zu den Hilfsanträgen 5 und 6, überreicht in der mündlichen Verhandlung

Die nebengeordneten Patentansprüche in der Fassung der für den Fachmann klaren Hilfsanträge 5 und 6 sind mangels Patentfähigkeit nicht zur Selbstbeschränkung des Streitpatents geeignet.

Der Patentanspruch 1 gemäß den Hilfsanträgen 5 und 6 soll laut Ausführungen der Beklagten in der mündlichen Verhandlung Bedenken einer möglichen unzulässigen Erweiterung desselben im Rahmen der Hilfsanträge 3 und 4 ausräumen, denn die neu formulierten Merkmale der Hilfsanträge 5 und 6 (s.u.) stimmen nun mit dem Wortlaut der Offenlegungsschrift zum Streitpatent nahezu überein (vgl. NK4, S. 11, Z. 8 – 12 i.V.m. Streitpatentschrift, Sp. 8, Z. 40 – 46).

1. Hilfsantrag 5

Der Gegenstand des Patentanspruchs 1 in der Fassung nach Hilfsantrag 5 wird durch die Druckschrift D1/D1a neuheitsschädlich vorweggenommen.

1.1 Angelehnt an die Merkmalsgliederung des Patentanspruchs 1 gemäß Hauptantrag lässt sich der Patentanspruch 1 in der Fassung des Hilfsantrags 5 mit folgenden Ergänzungen gliedern (Änderungen gegenüber der Version gemäß Hauptantrag fett hervorgehoben):

1.1, 1.2, 1.2a

1.2a$_{H5_1}$ **wherein the control data is validated according to an authentication algorithm in the control processing block**

1.2a$_{H5_2}$ **wherein the authentication also includes a key that links it to the authentication of the source and destination points**

1.2b, 1.2c

Der Fachmann versteht das Merkmal **1.2a$_{H5_1}$** dahingehend, dass die Steuerdaten („control data“), die offensichtlich als diejenigen die Steuerinformation tragenden Daten zu verstehen sind, durch einen Authentifizierungsalgortihmus („authentication algorithm“) im „control processing block“ validiert werden. Unter dem hier erstmals im Merkmalskontext genannten „authentication algorithm“ ist – nachdem das Streitpatent in den Absätzen [0022], [0035], [0049] und [0050], in denen diese Begrifflichkeit offenbart ist, keine eigenständige Definition liefert – allgemein eine Rechenvorschrift zu verstehen (z. B. umgesetzt als Softwareprozedur und/oder Schaltung), die zum Zwecke einer wie auch immer gearteten Authentisierung von Steuerungsdaten eingesetzt wird; dass diese Rechenvorschrift explizit im Rahmen des „content processing blocks“ vorgesehen ist, ändert die Auslegung hierzu nicht, stellt dieser Block doch selbst nur eine

Rechenprozedur im IC dar, in dem die Datenverarbeitung stattfindet. Das dergestalt beanspruchte System wird auf die genannte Art jedenfalls nicht in räumlich-körperlicher und somit entscheidungserheblicher Weise dadurch ausgestaltet, an welcher konkreten Stelle bzw. an welchem Ort einer Rechenvorschrift eine bestimmte Prozedur abläuft.

Das Merkmal **1.2a$_{H5_2}$** ist prinzipiell analog zum Merkmal 1.2a$_{H3}$ des Hilfsantrages 3 zu verstehen, allerdings dergestalt abgewandelt, dass anstatt des dortigen allgemein als Steuerinformation („control information“) bezeichneten Inhalts nun konkret die Authentifzifierung („authentication“) – die ebenfalls als Steuerungsinformation anzusehen ist - den genannten Schlüssel enthalten soll.

Aus der Druckschrift D1/D1a, Figur 18 ist es bekannt, dass im „ENCRYPTION PROCESSING MEANS 810“ ein Authentfizierungsalgorithmus ausgeführt wird. Dort erfolgt dies, indem unter Berücksichtigung bzw. Einbezug des EKB, des Device Node Key und des ICV in den Bausteinen mit den Bezugszeichen 811 – 814 und 824 entsprechend gerechnet wird, um im Ergebnis die Freigabe zum Entschlüsseln der gewünschten Inhaltsdaten zu erhalten oder diese zu negieren (Merkmal **1.2a$_{H5-1}$**).

Da das Merkmal 1.2a$_{H5_2}$ von seiner Sachaussage her betrachtet vom Merkmal 1.2a$_{H3}$ mit umfasst wird, gilt hier das zum Hilfsantrag 3 Ausgeführte in entsprechender Konsequenz. Folglich ist auch dieses Merkmals aus der Druckschrift D1/D1a bekannt (Merkmal **1.2a$_{H5-2}$**).

Auch eine Verteidigung des Streitpatents mit Hilfsantrag 5 führt somit nicht zum Erfolg, da der Gegenstand des Patentanspruchs 1 nicht neu gegenüber der Druckschrift D1/D1a ist.

1.2 Ausführungen zu den abhängigen Patentansprüchen und zum nebengeordneten Patentanspruch 8 erübrigen sich an dieser Stelle, da die Beklagte

den Anspruchssatz als Ganzes verteidigt und im Rahmen der beantragten Reihenfolge ihrer Hilfsanträge versucht, zur Patentfähigkeit der dort beanspruchten Gegenstände zu gelangen.

2. Hilfsantrag 6

Der Gegenstand des Patentanspruchs 1 in der Fassung nach Hilfsantrag 6 wird durch die Druckschrift D1/D1a neuheitsschädlich vorweggenommen.

2.1 Angelehnt an die Merkmalsgliederung des Patentanspruchs 1 gemäß Hilfsantrag 5 lässt sich der Patentanspruch 1 in der Fassung des Hilfsantrags 6 mit folgenden Ergänzungen gliedern (Änderungen gegenüber der Version gemäß Hilfsantrag 5 fett hervorgehoben):

1.1, 1.2, 1.2a, 1.2a$_{H5}$
1.2a$_{H6}$ as well as the means to unlock access to the corresponding content
1.2b, 1.2c

Da das einzig neu zum Patentanspruch 1 gemäß Hilfsantrag 6 hinzugetretene Merkmal technisch nichts Anderes aussagt, als das Merkmal **1.2a$_{H4_3}$** des Hilfsantrags 4, wird zur Auslegung und Realisierung desselben in der Lehre der Druckschrift D1/D1a auf die dortigen Ausführungen verwiesen.

Somit führt auch eine Verteidigung des Streitpatents mit Hilfsantrag 6 nicht zum Erfolg, da mit dem antragsgemäßen Patentanspruch 1 keine Neuheit gegenüber dem Stand der Technik verbunden ist, wie ihn die Druckschrift D1/D1a darstellt.

2.2 Ausführungen zu den abhängigen Patentansprüchen und zum nebengeordneten Patentanspruch 8 erübrigen sich an dieser Stelle, da die Beklagte

den Anspruchssatz als Ganzes verteidigt und im Rahmen der beantragten Reihenfolge ihrer Hilfsanträge versucht, zur Patentfähigkeit der dort beanspruchten Gegenstände zu gelangen.

2.3 Bei dieser Sachlage kann es dahinstehen, ob die seitens der Klägerin in der mündlichen Verhandlung vorgebrachten Mängel einer mangelnden Klarheit in Bezug auf die das System nun beschreibenden Merkmale tatsächlich vorliegen.

V. Zu Patentanspruch 1 nach dem Hauptantrag und den Hilfsanträgen vom 28. August 2020

Da sich die jeweiligen Patentansprüche 1 gemäß Hauptantrag und gemäß den Hilfsanträgen 1 bis 4 als nicht patentfähig erwiesen haben (vgl. hierzu die entsprechenden Ausführungen in den Abschnitten II. und III.), kann auch eine Verteidigung des Streitpatents, die jeweils nur auf den jeweiligen Patentansprüchen 1 beruht, keinen Erfolg haben.

Das Streitpatent ist somit auch im Rahmen dieser Verteidigung jeweils nicht bestandsfähig.

B.

Die Kostenentscheidung beruht auf § 84 Abs. 2 PatG i. V. m. § 91 Abs. 1 Satz 1 ZPO, die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus § 99 Abs. 1 PatG i. V. m. § 709 Satz 1 und Satz 2 ZPO.

C.

Rechtsmittelbelehrung

Gegen dieses Urteil ist das Rechtsmittel der Berufung gemäß § 110 PatG gegeben. Die Berufungsfrist beträgt einen Monat. Sie beginnt mit der Zustellung des in vollständiger Form abgefassten Urteils, spätestens aber mit dem Ablauf von fünf Monaten nach der Verkündung (§ 110 Abs. 3 PatG).

Die Berufung wird nach § 110 Abs. 2 PatG durch Einreichung der Berufungsschrift beim Bundesgerichtshof, Herrenstr. 45a, 76133 Karlsruhe eingelegt.

Voit Martens Albertshofer Dr. Wollny Bieringer

prö