BUNDESPATENTGERICHT

IM NAMEN DES VOLKES

URTEIL

Verkündet am
20. Oktober 2021
…

5 Ni 13/19 (EP)

(Aktenzeichen)

In der Patentnichtigkeitssache

…

ECLI:DE:BPatG:2021:201021U5Ni13.19EP.0

betreffend das europäische Patent EP 1 973 297
(DE 603 38 312)

hat der 5. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf Grund der mündlichen Verhandlung vom 20. Oktober 2021 durch den Vorsitzenden Richter Voit, die Richterin Martens sowie die Richter Dipl.-Ing. Univ. Albertshofer, Dipl.-Phys. Univ. Bieringer und Dr.-Ing. Ball

für Recht erkannt:

I. Das europäische Patent 1 973 297 wird mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland dadurch teilweise für nichtig erklärt, dass seine Patentansprüche 1 und 16, denen sich die erteilten Patentansprüche 2 bis 15 sowie 17 und 18 anschließen, folgende Fassung erhalten:

1. A method of determining whether protected content stored on a first communication device (201) are to be accessed by a second communication device (203),

the method comprising the step of performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval,

characterized in that the distance measurement is an authenticated distance measurement and in that the first and the second communication device share a common secret and said common secret is used for performing the distance measurement and

wherein the first device (201) authenticates the second device (203), and then the first device (201) securely shares the common secret with the second device (203) according to a key management protocol,

and wherein the first device (201) generates a secure authenticated channel using the shared secret, if the measured distance is within the predefined distance interval, and transmits the protected content to the second device (203) via the secure authenticated channel.

16. A first communication device (201) configured for determining whether protected content stored on the first communication device (201) are to be accessed by a second communication device (203),

the first device comprising means for performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval,

characterized in that the distance measurement is an authenticated distance measurement and that the first device comprises a memory storing a common secret also stored on the second communication device, which common secret is used for performing the distance measurement,

the first device being configured (411, 413, 417) for authenticating the second device 203 and then securely sharing the secret with the second device,

and the first device (201) being configured to generate a secure authenticated channel using the shared secret if the measured distance is within the predetermined distance interval and transmits the protected content to the second device (203) via the secure authenticated channel.

Im Übrigen wird die Klage abgewiesen.

II. Von den Kosten des Rechtsstreits tragen die Klägerinnen 70%, die Beklagte 30%.

III. Das Urteil ist gegen Sicherheitsleistung in Höhe von 120 % des 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 1 973 297 (Streitpatent), das am 27. Juni 2003 angemeldet wurde und die Priorität einer Europäischen Anmeldung vom 26.07.2002 (EP 02078076) in Anspruch nimmt. Das Streitpatent wird beim Deutschen Patent- und Markenamt unter dem Aktenzeichen DE 603 38 312.2 geführt und trägt die Bezeichnung „Secure authenticated distance measurement“ („Sichere authentifizierte Abstandsmessung“). Es umfasst 18 Patentansprüche, die alle mit der Nichtigkeitsklage angegriffen sind.

Die nebengeordneten Patentansprüche 1 und 16 haben nach der Streitpatentschrift (EP 1 973 297 B1) folgenden Wortlaut:

1. A method of determining whether protected content stored on a first communication device (201) are to be accessed by a second communication device (203), the method comprising the step of performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval, **characterized in that** the distance measurement is an authenticated distance measurement and **in that** the first and the second communication device share a common secret and said common secret is used for performing the distance measurement and wherein

- the first device (201) authenticates the second device (203), and
- the first device (201) securely shares the common secret with the second device (203) according to a key management protocol.

16. A first communication device (201) configured for determining whether protected content stored on the first communication device (201) are to be accessed by a second communication device (203), the first device comprising means for performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval, **characterized in that** the distance measurement is an authenticated distance measurement and that the first device comprises a memory storing a common secret also stored on the second communication device, which common secret is used for performing the distance measurement, the first device being configured (411, 413, 417) for authenticating the second device 203 and then securely sharing the secret with the second device.

In deutscher Übersetzung nach der Streitpatentschrift lauten die nebengeordneten Patentansprüche:

1. Verfahren zum Ermitteln, ob auf geschützte Inhalte, die auf einer ersten Kommunikationsvorrichtung (201) gespeichert sind, durch eine zweite Kommunikationsvorrichting (203) zuzugreifen ist, wobei das Verfahren den Schritt umfasst, eine Abstandsmessung zwischen der ersten (201) und der zweiten Kommunikationsvorrichtung (203) durchzuführen und zu prüfen, ob der genannte gemessene Abstand innerhalb eines vordefinierten Abstandintervalls liegt, **dadurch gekennzeichnet, dass** die Abstandsmessung eine authentifizierte Abstandsmessung ist und dass die erste und die zweite Kommunikationsvorrichtung ein gemeinsames Geheimnis miteinander teilen und das genannte gemeinsame Geheimnis verwendet wird, um die Abstandsmessung durchzuführen, und wobei

- die erste Vorrichtung (201) die zweite Vorrichtung (203) authentifiziert, und
- die erste Vorrichtung (201) das gemeinsame Geheimnis gemäß einem Schlüsselverwaltungsprotokoll sicher mit der zweiten Vorrichtung (203) teilt.

16. Erste Kommunikationsvorrichtung (201), konfiguriert zum Ermitteln, ob auf geschützte Inhalte, die auf der ersten Kommunikationsvorrichtung (201) gespeichert sind, durch eine zweite Kommunikationsvorrichtung (203) zuzugreifen ist, wobei die erste Vorrichtung Mittel zum Durchführen einer Abstandsmessung zwischen der ersten (201) und der zweiten Kommunikationsvorrichtung (203) und zum Prüfen, ob der genannte gemessene Abstand innerhalb eines vordefinierten Abstandsintervalls liegt, umfasst, **dadurch gekennzeichnet, dass** die Abstandsmessung eine authentifizierte Abstandsmessung ist und dass die erste Vorrichtung einen Speicher umfasst, in dem ein gemeinsames Geheimnis gespeichert ist, welches auch auf der zweiten Kommunikationsvorrichtung gespeichert ist, wobei das gemeinsame Geheimnis verwendet wird, um die Abstandsmessung durchzuführen, wobei die erste Vorrichtung konfiguriert ist (411, 413, 417), um die zweite Vorrichtung 203 zu authentifizieren und dann das Geheimnis mit der zweiten Vorrichtung sicher zu teilen.

Wegen der Unteransprüche 2 bis 15 sowie 17 und 18 wird auf die Streitpatentschrift Bezug genommen.

Die Klägerin zu 1 hat am 6. Juni 2019 Nichtigkeitsklage erhoben, der die Klägerin zu 2 einen Tag später als weitere Klägerin mit Zustimmung der Klägerin zu 1 beigetreten ist. Beide Klägerinnen machen mangelnde Patentfähigkeit des Gegenstands des Streitpatents (Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i.V.m. Art. 138 Abs. 1 lit. a EPÜ) geltend. Sie tragen zudem vor, das Streitpatent gehe in den Ansprüchen 1 und 16 über den Inhalt der europäischen Patentanmeldung (NK4) hinaus und sei auch mangels deutlicher und vollständiger Offenbarung der Lehre des Patentanspruchs 16 in vollem Umfang für nichtig zu erklären.

Zur fehlenden Patentfähigkeit stützen sich die Klägerinnen auf folgende Dokumente:

D1 High-bandwidth Digital Content Protection System, Revision 1.0, 17. Februar 2000

D2 WO 97/39553 A1

D3 WO 01/93434 A2

D4 Brands, Stefan und Chaum, David: „Distance-Bounding Protocols", Eurocrypt (1993), S. 344 – 359, 1994

D5 US 2002/0077984 A1

D6 US 5 126 746 A

D7 US 2003/065918 A1

D8 Epstein, Michael A. und Pasieka, Michael S.: „Open Copy Protection System - Philips Research Proposal to Broadcast Protection Discussion Group", Version 1.4, 7. Mai 2002 mit weiteren Unterlagen **D8a** bis **D8k**

D9 Asokan, N., Debar, H., Steiner M. und Waidner, M.: „Authenficating public terminals", Computer Networks 31 (1999), S. 861-870

D10 US 5 995 624 A

NK11 Sutikno, S. et al.: „An Implementation of ElGamal Elliptic Curves Cryptosystems“, 1998 IEEE, ohne weitere Quellenangabe

NK12 Auszug aus Jung, V., Warnecke H. (Hrsg.): „Handbuch für die Telekommunikation“, ISBN 978-3-642-97703-9, Springer, 1998, Inhaltsverzeichnis und Seite 3-126 (eine Seite)

NK13 Auszug aus Kaufman, Perlman, Speciner: „Network Security, Private Communication in a Public World” ISBN 0-13-046019-2, Second Edition, 2002 by Prentice Hall PTR, Inhaltsverzeichnis und Seiten 48, 49, 268.

NK14 Auszug aus Krüger, Reschke (Hrsg) “Lehr- und Übungsbuch Telematik“, Fachverlag Leipzig, 2000, Vorwort, Inhaltsverzeichnis und Seiten 316 bis 321.

Die Klägerinnen beantragen,

das europäische Patent 1 973 297 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland in vollem Umfang für nichtig zu erklären.

Die Beklagte beantragt,

die Klage abzuweisen,
hilfsweise nach Maßgabe der Hilfsanträge I, II, VI bis VIII, vorgelegt als Anlagen zum Schriftsatz vom 12. August 2021, bzw. der Hilfsanträge III, IV, V und IX, überreicht mit Schriftsatz vom 18. Oktober 2021, in der Reihenfolge ihrer Nummerierung.

Die Klägerinnen treten auch den Fassungen nach den Hilfsanträgen entgegen.

Patentanspruch 1 nach Hilfsantrag I lautet:

1. A method of determining whether protected content stored on a first communication device (201) are to be accessed by a second communication device (203),

the method comprising the step of performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval,

characterized in that the distance measurement is an authenticated distance measurement and in that the first and the second communication device share a common secret and said common secret is used for performing the distance measurement and

wherein the first device (201) authenticates the second device (203), and then the first device (201) securely shares the common secret with the second device (203) according to a key management protocol,

and wherein the common secret is shared before performing the distance measurement.

Patentanspruch 16 nach Hilfsantrag I lautet:

16. A first communication device (201) configured for determining whether protected content stored on the first communication device (201) are to be accessed by a second communication device (203),

the first device comprising means for performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval,

characterized in that the distance measurement is an authenticated distance measurement and that the first device comprises a memory storing a common secret also stored on the second communication device, which common secret is used for performing the distance measurement,

the first device being configured (411, 413, 417) for authenticating the second device 203 and then securely sharing the secret with the second device before performing the distance measurement.

Patentanspruch 1 nach Hilfsantrag II lautet:

1. A method of determining whether protected content stored on a first communication device (201) are to be accessed by a second communication device (203),

the method comprising the step of performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval,

characterized in that the distance measurement is an authenticated distance measurement and in that the first and the second communication device share a common secret and said common secret is used for performing the distance measurement and

wherein the first device (201) authenticates the second device (203), and then the first device (201) securely shares the common secret with the second device (203) according to a key management protocol,

wherein the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of

- performing the authentication of the second device (203) by the first device (201), by checking whether the second device (203) is compliant with a set of predefined compliance rules, and
- if the second device (203) is compliant, sharing the common secret by transmitting said secret to the second device (203).

Der nebengeordnete Patentanspruch 15 nach Hilfsantrag II lautet:

15. A first communication device (201) configured for determining whether protected content stored on the first communication device (201) are to be accessed by a second communication device (203),

the first device comprising means for performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval,

characterized in that the distance measurement is an authenticated distance measurement and that the first device comprises a memory storing a common secret also stored on the second communication device, which common secret is used for performing the distance measurement,

the first device being configured (411, 413, 417) for authenticating the second device (203) and then securely sharing the secret with the second device,

wherein the first device (201) is configured to share the common secret before performing the distance measurement, the sharing being performed by the steps of

- performing the authentication of the second device (203) by the first device (201), by checking whether the second device (203) is compliant with a set of predefined compliance rules, and
- if the second device (203) is compliant, sharing the common secret by transmitting said secret to the second device (203).

Hilfsantrag III in der Fassung der Anlage zum Schriftsatz vom 18. Oktober 2021 ist im Tenor hinsichtlich seiner tragenden Ansprüche 1 und 16 wiedergegeben.

Wegen des Wortlauts der weiteren Hilfsanträge IV bis IX wird auf die Anlagen zu den Schriftsätzen vom 12. August 2021 bzw. vom 18. Oktober 2021 Bezug genommen.

Die Beklagte, die sich zum Beitritt der Klägerin zu 2 nicht geäußert hat, tritt im Übrigen dem Vorbringen der Klägerinnen in allen Punkten entgegen. Sie führt weiter aus, die von den Klägerinnen vorgebrachten Druckschriften nähmen die im Streitpatent offenbarte Erfindung weder neuheitsschädlich vorweg noch legten sie

diese nahe. Jedenfalls in einer der hilfsweise verteidigten Fassungen habe das Streitpatent daher Bestand.

Mit einem Hinweis nach § 83 Abs. 1 PatG vom 28. Juni 2021 hat der Senat den Parteien die Gesichtspunkte mitgeteilt, die für die Entscheidung voraussichtlich von besonderer Bedeutung sind.
Wegen des Vorbringens der Parteien im Übrigen wird auf deren Schriftsätze mit sämtlichen Anlagen sowie auf das Protokoll der mündlichen Verhandlung Bezug genommen.

E n t s c h e i d u n g s g r ü n d e

A.

Die Klage ist zulässig, der Beitritt der Klägerin zu 2 jedenfalls sachdienlich. In der Sache hat die Klage nur teilweise Erfolg. Hinsichtlich der erteilten Fassung wie auch der Fassungen nach den Hilfsanträgen I und II fehlt es an der Patentfähigkeit der unabhängigen Patentansprüche 1 und 16 - bzw. 15 in der Fassung des Hilfsantrags II. In der Fassung nach Hilfsantrag III vom 18. Oktober 2021 hat das Streitpatent jedoch Bestand, so dass die darüber hinaus gehende Klage abzuweisen war.

I. Zum Gegenstand des Streitpatents

1. Das Streitpatent betrifft ein Verfahren zur Durchführung einer authentifizierten Abstandsmessung zwischen zwei Kommunikationsvorrichtungen, sowie ein Verfahren zur Bestimmung, ob geschützter Inhalt auf einer ersten Kommunikationsvorrichtung gespeichert ist und einem zweiten Kommunikationsgerät Zugriff auf diesen Inhalt gewährt wird. Darüber hinaus betrifft das Streitpatent ein Kommunikationsgerät, das eine authentifizierte Abstandsmessung zu einem zweiten Kommunikationsgerät ausführen kann (Streitpatentschrift, [0001]).

Die Streitpatentschrift geht davon aus, dass digitale Medien als Träger digitaler Informationen beliebt sind und mit Datenträgern wie beschreibbaren Platten („recordable discs“) und Festkörperspeichern („solid state memory“) ein beachtliches Wachstum für den Markt der Software- und Datenverteilung entstehe (Streitpatentschrift, [0002]). Die substanziell bessere Qualität digitaler Formate mache sie gegenüber analogen Formen anfälliger für unerlaubte Vervielfältigung, da die Daten leichter und schneller zu kopieren sind, was grundsätzlich ohne Qualitätsverlust beliebig oft geschehen kann („multi-generation copying“) (Streitpatentschrift, [0003]). Dies führte zu zahlreichen Verfahren zum Kopierschutz und zum digitalen Rechtemanagement („DRM systems“), die Technologien wie Verschlüsselung, Wasserzeichen und Rechteverwaltung nutzen (Streitpatentschrift, [0004]). Ein Weg zum Schutz digitaler Inhalte sei es auch, sicherzustellen, dass eine Übertragung nur stattfinde, wenn das empfangende Gerät als konformes Gerät identifiziert werde und der Nutzer auch die Berechtigung zur Übertragung habe (Streitpatentschrift, [0005]). Falls die Übertragung zulässig sei, erfolge diese typischerweise in verschlüsselter Form, um sicherzustellen, dass der Inhalt nicht unerlaubterweise abgefangen werde (Streitpatentschrift, [0006]). Über einen gesicherten, authentifizierten Kanal (SAC, „secure authenticated channel“) sei eine Technologie verfügbar, die eine Geräteauthentifizierung und eine verschlüsselte Übertragung erlaube, jedoch sei die Content-Branche („content industry“) uneinig in Bezug auf die Verbreitung von Inhalten über passende Schnittstellen, wie z.B. Ethernet (Streitpatentschrift, [0007]). Zudem sollte es einem berechtigten Nutzer möglich sein, einen Nachbarn zu besuchen und etwa einen Film auf dessen Gerät

anzusehen. Typischerweise würde der „content owner“ dies nicht erlauben, aber es könnte erlaubt werden, wenn gewährleistet wäre, dass sich der Berechtigte oder eines seiner Geräte in der Nähe des benutzten Geräts befinde (Streitpatentschrift, [0008]). Bei der Frage, ob Inhalte für ein weiteres Gerät zugänglich gemacht oder kopiert werden dürfen, gebe es daher ein Interesse an einer authentifizierten Abstandsmessung (Streitpatentschrift, [0009]). Im Aufsatz „Distance bounding protocols“ (vorgelegt von der Klägerin als Anlage D4) beschrieben Brands und Chaum auf Laufzeitmessungen basierende Abstandsmessungen, wobei ein Anforderungsbit („challenge“) und ein Antwortbit („response“) nach einem verbindlichen Protokoll verwendet würden. Dies würde jedoch keine Kompatibilitätsprüfung für ein authentifiziertes Gerät erlauben und es sei auch nicht effizient, wenn beide Geräte sich gegenseitig authentifizieren müssten (Streitpatentschrift, [0010]).

2. Es sei daher Aufgabe der Erfindung, eine Lösung für das Problem der Durchführung einer sicheren Übertragung von Inhalten innerhalb einer begrenzten Entfernung zu erhalten (Streitpatentschrift, [0011]).

3. Bei dem einschlägigen **Fachmann** handelt es sich um einen Ingenieur der Nachrichtentechnik (Universitätsdiplom bzw. Master) mit Erfahrung auf dem Gebiet der sicheren Übertragung von Daten und Kenntnissen zur Abstandsmessung zwischen Kommunikationsgeräten.

II. Zur erteilten Fassung

1. Zur Lösung der oben genannten Aufgabe wird mit dem erteilten Patentanspruch 1 ein Verfahren für eine sichere authentifizierte Abstandsmessung beansprucht, dessen Merkmale sich folgendermaßen gliedern lassen:

M1.1 A method of determining whether protected content stored on a first communication device are to be accessed by a second communication device, the method comprising

M1.2 the step of performing a distance measurement between the first and the second communication device and checking whether said measured distance is within a predefined distance interval, characterized in that

M1.3 the distance measurement is an authenticated distance measurement and in that

M1.4 the first and the second communication device share a common secret and said common secret is used for performing the distance measurement and wherein

M1.5.1 - the first device authenticates the second device, and

M1.5.2 - the first device securely shares the common secret with the second device according to a key management protocol.

Der nebengeordnete Patentanspruch 16 betrifft ein Kommunikationsgerät, dessen Merkmale sich folgendermaßen gliedern lassen:

M16.1 A first communication device configured for determining whether protected content stored on the first communication device are to be accessed by a second communication device,

M16.2 the first device comprising means for performing a distance measurement between the first and the second communication device and checking whether said measured distance is within a predefined distance interval,
characterized in that

M16.3 the distance measurement is an authenticated distance measurement and that

M16.4 the first device comprises a memory storing a common secret also stored on the second communication device, which common secret is used for performing the distance measurement,

M16.5.1 the first device being configured for authenticating the second device and

M16.5.2 then securely sharing the secret with the second device.

2. Der Senat legt den nebengeordneten Patentansprüchen 1 und 16 folgendes Verständnis zugrunde:

Mit Patentanspruch 16 wird ein Kommunikationsgerät beansprucht (Merkmal M16.1). Gemäß Merkmal M16.1 ist das Kommunikationsgerät („first communication device“) geeignet, per Konfiguration zu bestimmen, ob einem anderen (zweitem – „second“) Kommunikationsgerät geschützter Inhalt („protected content“), der auf dem ersten Gerät gespeichert ist, zugänglich gemacht wird.

Das Streitpatent beschreibt in einem Ausführungsbeispiel (vgl. Fig. 1 i.V.m. Abs. [0034]), wonach ein Nutzer auf die gespeicherten Inhalte des ersten Geräts zugreift und diese an andere Geräte (i.e. das zweite Kommunikationsgerät) versendet, welche die Inhalte empfangen dürfen. In einem weiteren Ausführungsbeispiel (vgl. Fig. 2 i.V.m. Abs. [0037] bis [0044]) fordert das zweite Kommunikationsgerät die auf dem ersten Gerät gespeicherten Inhalte hingegen explizit an (vgl. Streitpatentschrift, [0037], Sp. 6, Z. 32 ff.: „In the example the first device 201 comprises content which the second device 203 has requested.“). In der Ausführungsform betreffend das Verfahren gemäß dem rückbezogenen Patentanspruch 10 wird beansprucht, dass ein Versenden der Daten durch das erste Gerät in Abhängigkeit von einem detektierten „Access“ durch das zweite Gerät erfolgen soll. Insofern versteht der Fachmann die Begrifflichkeit „to be accessed“ des Merkmals M16.1 dahingehend, dass bestimmt wird, ob dem zweiten Gerät ein „Zugang(srecht) auf die gespeicherten Inhalte“ eingeräumt wird, wobei das zweite

Gerät die Inhalte direkt vom ersten Gerät anfordern oder vom ersten Gerät auch ohne Anforderung gesendete Inhalte zumindest empfangen kann. Ein direkter Zugriff des zweiten Geräts auf den Speicher des ersten Geräts ist damit nicht notwendigerweise verbunden.

Gemäß Merkmal M16.2 verfügt das erste Gerät (dazu) über Mittel (Singular oder Plural), das/die geeignet sein muss/müssen,

a) eine Abstandsmessung zwischen diesem und dem zweiten Gerät auszuführen („performing a distance measurement“) und

b) zu prüfen („checking“), ob der gemessene Abstand („said measured distance“) innerhalb eines vordefinierten Intervalls liegt.

Der Fachmann entnimmt dem Merkmal M16.2, dass das Ergebnis der Abstandmessung („said measured distance“) die Grundlage für einen Vergleich mit dem vordefinierten Intervall bildet.

Das Bestimmen des Abstands auf eine andere Art und Weise als durch Messung fällt somit nicht unter den Wortlaut des Patentanspruchs. Das Bestimmen des Abstands resultiert bzw. basiert also auf einem Messergebnis. Das Kommunikationsgerät muss daher ein Mittel aufweisen, das ein Messergebnis erzeugen kann und dieses mit dem vordefinierten Intervall vergleichen kann. Der Wortlaut des Patentanspruchs 16 ist jedoch nicht explizit auf ein bestimmtes Messverfahren beschränkt und umfasst daher auch eine (Um-) Laufzeitmessung („round trip time“) von gesendeten/empfangenen Signalen, um damit den Abstand zwischen zwei Geräten zu bestimmen. Insofern stellt eine (gemessene) Signallaufzeit auch eine den Abstand repräsentierende Messgröße dar, wenn die Laufzeitparameter bekannt sind. Der Wortlaut des Patentanspruchs 16 lässt insofern auch einen Vergleich von zwei Zeiten zu, nämlich der gemessenen Signallaufzeit mit einer maximalen Laufzeit, die die obere Intervallgrenze für den Abstand repräsentiert. Eine Umrechnung der Zeiten in die Dimension einer Länge verlangt der Anspruchswortlaut somit nicht.

Unter den Parteien wurde strittig diskutiert, ob ein Timeout unter den Wortlaut der Abstandsbestimmung i. S. des Patentanspruchs 16 fällt. Der Senat ist überzeugt, dass sich ein Mittel, das einen Timeout ausführt, unter das Merkmal 16.2 nicht subsumieren lässt. Denn mit einem Timeout wird keine Abstandsmessung i.S. des Streitpatents durchgeführt, da erstens kein Messergebnis vorliegt, das den gemessenen Abstand repräsentieren könnte, und zweitens kein Vergleich des Messergebnisses mit einem vorbestimmten Intervall vorliegt, das einen (maximal zulässigen) Abstand repräsentieren könnte. Dem Fachmann ist bekannt, dass ein Timeout in der Kommunikationstechnik die Zeitspanne betrifft, die ein Vorgang in Anspruch nehmen darf, bevor er (ggf. mit einem Fehler) abgebrochen wird. Selbst in der Ausführungsform gemäß Unteranspruch 18, wonach der Abstand mittels Signallaufzeiten gemessen wird, erfordert die den Abstand repräsentierende Zeitdifferenz der Zeiten t1 und t2, dass das zur Zeit t1 gesendete Signal (nach Modifikation am zweiten Gerät) zur Zeit t2 am ersten Gerät wieder erfasst wird. Im Gegensatz dazu würde das Eintreten eines Timeouts nur einen Abbruch des Vorgangs ohne Durchführung einer (authentifizierten) Messung bedeuten und somit folglich auch nicht die zweite Zeit t2 liefern.

Gemäß Merkmal M16.3 ist die Abstandsmessung eine authentifizierte Abstandsmessung. Eine allgemeingültige Definition, was unter einer authentifizierten Abstandsmessung („authenticated distance measurement“) zu verstehen ist, findet sich in der Streitpatentschrift nicht. Aufgrund des schriftsätzlichen Vorbringens der Parteien auf den gerichtlichen Hinweis des Senats vom 28. Juni 2021, präzisiert der Senat die Auslegung des Merkmals M16.3 dahingehend, dass als Voraussetzung für eine authentifizierte Abstandsmessung zunächst die Authentifizierung des zweiten Geräts erfolgen muss und dann das geteilte gemeinsame Geheimnis für die Abstandsmessung verwendet wird (vgl. auch Merkmal M16.4). Insofern ist die authentifizierte Abstandsmessung dahingehend zu verstehen, dass die Abstandmessung das geteilte Geheimnis nach

einer Authentifizierung des zweiten Geräts verwendet. Der Senat teilt die Auffassung der Beklagten, dass es sich bei der Authentifizierung und der Abstandsmessung um zwei unterschiedliche Schritte handele (vgl. Schriftsatz der Beklagten vom 20. September 2021, S. 2, vorletzter Absatz), teilt der Senat diese Auffassung. Soweit die Beklagte dem Anspruchswortlaut gemäß Vortrag in der mündlichen Verhandlung nun ein dreischrittiges Verfahren dahingehend entnehmen will, dass erst die Authentifizierung, danach das Teilen des Geheimnisses erfolgen soll und erst als drittes mit der Abstandsmessung begonnen werden soll, greift diese Trennung nicht durch. Denn der Wortlaut des erteilten Patentanspruchs 16 fordert lediglich, dass das geteilte Geheimnis für die Abstandsmessung verwendet wird, nicht dass diese erst nach dem Teilen des Geheimnisses begonnen wird.

Gemäß Merkmal M16.4 weist das Kommunikationsgerät einen Speicher auf, in dem das bereits o.g. gemeinsame Geheimnis („common secret“) gespeichert ist. Das gemeinsame Geheimnis als solches ist nicht spezifiziert, es muss lediglich auf beiden Geräten gespeichert sein („also stored on the second communication device“). Insofern sind weitere Spezifika betreffend das gemeinsame Geheimnis nicht beansprucht. Es kommt lediglich darauf an, dass nur die beiden Geräte das gemeinsame Geheimnis kennen bzw. zusammensetzen können (z.B. private/public-Paar) und dass es sicher geteilt wird (Zusammenschau mit Merkmal M16.5.2). Dem Streitpatent entnimmt der Fachmann, (vgl. Figur 2 Bezugszeichen 207 i.V.m. Absatz [0037]), dass es sich bei dem sicher geteilten Geheimnis um eine Zufallszahl handeln könne (dort: „transmitting a random generated bit word“).

Gemäß Merkmal M16.5.1 ist das erste Gerät lediglich konfiguriert, um das zweite Gerät zunächst zu authentifizieren und dann gemäß Merkmal M16.5.2 das Geheimnis mit dem zweiten Gerät zu teilen. Somit ist das erste Kommunikationsgerät geeignet, erst zu authentifizieren, bevor das Geheimnis geteilt wird. Im Ausführungsbeispiel zu Fig. 2 i.V.m. Abs. [0034] bis [0041] ist dieser Ablauf beschrieben.

Das Authentifizieren gemäß Merkmal M16.5.1 ist gemäß Anspruchswortlaut nicht näher bestimmt, insofern auch nicht beschränkt und umfasst jede dem Fachmann bekannte Ausführungsform der Authentifizierung.

Für den Patentanspruch 1 gilt das zum korrespondierenden Vorrichtungsanspruch 16 Ausgeführte entsprechend, wobei gemäß den Verfahrensschritten M1.5.1 und M1.5.2 die Reihenfolge hinsichtlich der Authentifizierung und des Austauschs des Geheimnisses offenbleibt und der Austausch des Geheimnisses mittels eines Schlüsselmanagementprotokolls („key management protocol“) erfolgt. Dem Fachmann bleibt überlassen, welche Protokolle für Authentifizierung und Teilen verwendet werden sollen. Gemäß Beschreibung kann er bspw. bekannte Protokolle gemäß ISO 9798 und ISO 11770 verwenden (vgl. Streitpatentschrift, Abs. [0041]).

3. Zum Nichtigkeitsgrund der unzulässigen Erweiterung

Der Nichtigkeitsgrund der unzulässigen Erweiterung gemäß Art. 138 Abs. 1 Buchst. c EPÜ liegt nicht vor.

Soweit die Klägerin zu 1 schriftsätzlich vorgetragen hat, ursprünglich sei lediglich „data“, jedoch nicht der „protected content“ gemäß den Merkmalen M1.1 bzw. M16.1 beansprucht worden und der Begriff „protected content“ tauche nur am Ende der ursprünglichen Beschreibung in Absatz [0043] der NK4 auf (vgl. Nichtigkeitsklage, S. 14), widerspricht die Beklagte (vgl. Widerspruchsbegründung, S. 13) und benennt weitere Fundstellen in der ursprünglichen Offenbarung NK4, die Kopierschutz und geschützte Inhalte betreffen. Insbesondere nennt sie in der NK4 die Absätze [0004] bis [0006] der Beschreibungseinleitung, die Aufgabenstellung (NK4, Abs. [0011]) und die Beschreibung zu Figur 1 (Abs. [0031]).

In den ursprünglichen Anmeldeunterlagen ist nach Auffassung des Senats ausgeführt, dass die vom ersten zum zweiten Kommunikationsgerät übertragenen

Daten einen geschützten Inhalt betreffen. Darüber hinaus ist der streitpatentgemäße geschützte Inhalt („protected content“) dahingehend spezifiziert, dass er auf dem ersten Gerät gespeichert sein muss und dass dem authentifizierten zweiten Gerät, welches sich innerhalb eines vordefinierten räumlichen Abstands befindet, ein Zugangsrecht auf den Inhalt eingeräumt wird (siehe die Ausführungen zur Auslegung der Merkmale M1.1 bzw. M16.1 oben). Diese technische Lehre entnimmt der Fachmann ebenfalls unmittelbar und eindeutig der ursprünglichen Anmeldung (vgl.NK4, Abs. [0004]: „… copy protection and DRM systems…“, [0011]: „It is an object of the invention to obtain a solution to the problem of performing a secure transfer of content within a limited distance.“ und [0031]: „…authenticated distance measurement is being used for content protection.“).

b. Die Klägerin zu 1 hat auch schriftsätzlich vorgetragen, dass ursprünglich eine strikte Reihenfolge offenbart sei, wonach zunächst die Authentifizierung durchgeführt und gegebenenfalls im Anschluss daran das Geheimnis geteilt werde (vgl. Nichtigkeitsklage, S. 15), worauf der Wortlaut gemäß Merkmal M1.5 des Patentanspruchs 1 nicht beschränkt sei. Die Beklagte vertritt die Auffassung, dass es auf die Reihenfolge nicht ankäme (vgl. Widerspruchsbegründung, S. 14). Der Senat teilt diese Auffassung. Gemäß den Verfahrensschritten M1.5.1 und M1.5.2 bleibt die Reihenfolge hinsichtlich der Authentifizierung und des Austauschs des Geheimnisses offen. Gemäß obiger Auslegung zur authentifizierten Abstandsmessung (siehe Auslegung der Merkmale M1.3 bzw. M16.3 oben) kommt es lediglich insoweit auf die Reihenfolge an, dass die Authentifizierung vor der Abstandsmessung erfolgt und das geteilte Geheimnis für die Abstandsmessung verwendet wird. Darüber geht der Gegenstand des erteilten Patentanspruchs 1 nicht hinaus.

4. Zum Nichtigkeitsgrund der mangelnden Ausführbarkeit

Soweit mit der Klageschrift auch der Nichtigkeitsgrund der mangelnden Ausführbarkeit gemäß Art. 138 Abs. 1 Buchst. b EPÜ geltend gemacht wurde und die Klägerin zu 1 dazu ausgeführt hat, dass der in der Beschreibung, Abs. [0038] und [0039] angegebene Algorithmus lückenhaft sei, da einzelne Variablen nicht definiert seien (vgl. Replik, S. 11 ff.), greift dies nicht durch. Denn auf den konkreten Algorithmus kommt es nicht an, da der Fachmann einen geeigneten Algorithmus mit den offenbarten Informationen implementieren kann. Die Streitpatentschrift verweist auf ISO 9798 und ISO 11770 (vgl. Streitpatentschrift, Abs. [0041]). Im Übrigen wurde die Auffassung des Senats mit dem gerichtlichen Hinweis vom 28. Juni 2021 mitgeteilt und von den Klägerinnen weder schriftsätzlich noch in der mündlichen Verhandlung kommentiert.

5. Zum Nichtigkeitsgrund der mangelnden Patentfähigkeit

Der Gegenstand des Patentanspruchs 16 ist in sämtlichen Merkmalen aus der D8 bekannt und mithin gegenüber der Druckschrift D8 nicht neu (Art. 54 EPÜ). Gleiches gilt für den Gegenstand des Patentanspruchs 1.

Die Druckschrift D8 ist eine Vorlage (Proposal) der Fa. Philips Research an die Broadcast Protection Discussion Group (BPDG) für eine Technologie, um digitale Ausgänge bzw. Ausgangsdaten zu schützen („digital output protection technology“).

Die Druckschrift D8 ist Stand der Technik. Die Klägerin hat darlegen können, dass die D8 vor dem Prioritätstag des Streitpatents öffentlich zugänglich war (vgl. Anlagen D8a bis D8g der Replik vom 13. November 2020).

Das gemäß Druckschrift D8 vorgestellte Open Copy Protection System (OCPS) soll digitalen Inhalt u.a. vor dem Angriffsszenario eines geklonten Geräts schützen (vgl. D8, S. 5, vorletzter Abs.). Die Lehre der D8 sieht vor, das OCPS (octopus)-Protokoll vor dem Übertragen geschützter Daten von einem Gerät (Quelle – „source“) zu

einem zweiten Gerät (Senke – „sink“) auszuführen. Das Octopus-Protokoll sieht fünf Phasen vor, wobei vor allem die erste und teilweise die zweite Phase den streitpatentgemäß beanspruchten Gegenstand betreffen. In der ersten Phase des Octopus-Protokolls authentifizieren sich die beiden Geräte (Quelle und Senke) gegenseitig, wobei Zufallszahlen und Schlüssel ausgetauscht werden (vgl. D8, S. 6 - 9 mit Fig. 1 auf S. 8). Mittels Laufzeitmessung des kryptographisch verarbeiteten Parameters R_{source} von der Quelle zur Senke und nach kryptographischer Verarbeitung zurück zur Quelle sowie anschließendem Abgleich gegen einen maximalen Schwellwert von 1 ms wird bestimmt, ob die Übertragung im zulässigen Nahbereich stattfindet (D8, S. 9, 5. Abs.: „forbids non-local transmission“). Erst nach erfolgter Messung und Überprüfung, ob sich die Senke innerhalb eines Nahbereichs (und weiterer Schritte) befindet, wird ihr Zugriff auf die Daten der Quelle gewährt (vgl. D8, S. 6 - 9 mit Fig. 1 auf S. 8).

Im Einzelnen entnimmt der Fachmann aus der Druckschrift D8 folgende Merkmale:

M16.1 *A first communication device configured for determining whether protected content stored on the first communication device are to be accessed by a second communication device,*

Gemäß D8 gibt es ein Quellgerät („source device“), das Inhalt sendet und dem ersten Kommunikationsgerät i. S. des Streitpatents entspricht. Das Senke-Gerät („sink device“) empfängt Inhalt über die OPCS-Verbindung und entspricht dem zweiten Kommunikationsgerät i. S. des Streitpatents (vgl. D8, S. 6, Abschnitt 1.3).

M16.2 *the first device comprising means for performing a distance measurement between the first and the second communication device and checking whether said measured distance is within a predefined distance interval,*

D8, Seite 9, 5. Absatz offenbart, dass die (Um-)Laufzeit („round trip time“) der Zufallszahl **R_{source}** von der Quelle zur Senke und zurück gemessen sowie mit einem Schwellwert von 1 ms verglichen wird („At this point the

time needed for **R_{source}** to make the round trip is measured against an accepted maximum threshold of 1 milliseconds.“, Unterstreichung hinzugefügt). Es handelt sich um eine Abstandsmessung i.S. des Streitpatents, denn erstens wird gemessen und zweites wird, falls die Umlaufzeit zu groß ist, die Übertragung als nicht lokal („OCCI forbids non-local transmission“) betrachtet. Insofern repräsentiert die Signallaufzeit einen gemessenen Abstand, und der Schwellwert ein vordefiniertes Intervall. Es wird also gemessen und geprüft, ob die Senke innerhalb eines vorbestimmten Abstands zur Quelle positioniert ist.

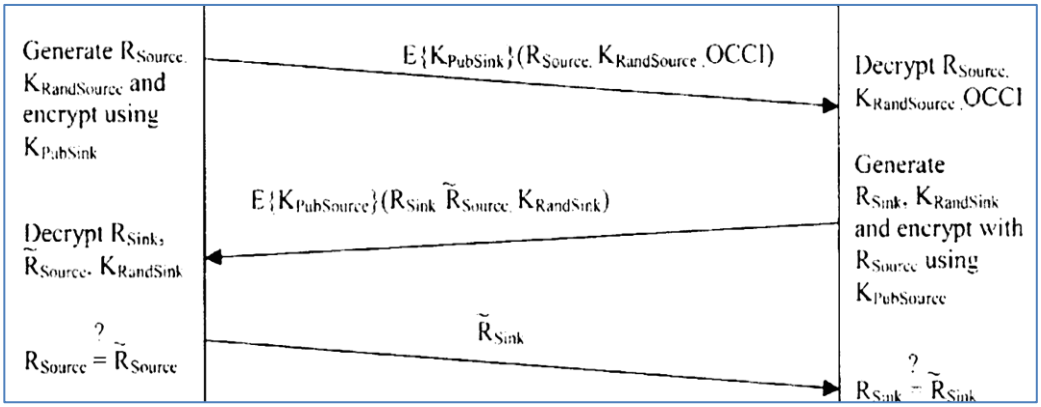
M16.3 *the distance measurement is an authenticated distance measurement and that*

Gemäß D8 wird die Senke authentifiziert (siehe Ausführungen zu Merkmal M16.5.1; vgl. D8, S. 7, Abschnitt 1.4.4 i.V.m. Fig. 1 auf S. 9; dort: „authentication phase“). Darüber hinaus wird das gemeinsame Geheimnis, d.h. die Zufallszahl **R_{source},** für die Abstandsmessung verwendet (siehe Ausführungen zu Merkmal M16.2 und M16.4; vgl. D8, S. 9, 4. Abs.). Aus beiden Gründen ist die Abstandsmessung gemäß D8 eine authentifizierte Abstandsmessung i.S. des Streitpatents (siehe auch obige Ausführungen zur Auslegung).

M16.4 *the first device comprises a memory storing a common secret also stored on the second communication device, which common secret is used for performing the distance measurement,*

Gemäß der Lehre der D8 werden Zufallszahlen und Schlüsselmaterial („random numbers and key material“) zwischen Quelle und Senke ausgetauscht (vgl. D8, S. 7, Abschnitt 1.4.4). Somit ist für den Fachmann klar, dass das Schlüsselmaterial der D8 auch auf beiden Geräten gespeichert ist und insbesondere die Quelle (entsprechend dem ersten Kommunikationsgerät i.S. des Streitpatents) einen Speicher aufweisen muss. Gemäß D8 wird **R_{source}** von der Quelle mit dem Schlüssel **$K_{PubSink}$**

der Senke verschlüsselt und nachdem es als $\widetilde{\mathbf{R}}_{\mathbf{Source}}$ von der Senke verschlüsselt mit dem Schlüssel $\mathbf{K_{PubSource}}$ zurückgesendet wurde von der Quelle wieder entschlüsselt (vgl. D8, S. 8 Fig. 1, Ausschnitt):



Darüber hinaus wird geprüft, ob $\mathbf{R_{source}}$ und $\widetilde{\mathbf{R}}_{\mathbf{Source}}$ identisch sind, was dem unter den Wortlaut des Anspruchs fallenden Ausführungsbeispiel gemäß Streitpatentschrift, Absatz [0045], entspricht. $\mathbf{R_{source}}$ entspricht i.V.m den Ver- und Entschlüsselungsvorgängen einem gemeinsamen Geheimnis i.S. des Streitpatents. Es wird auch zur Abstandsmessung verwendet (vgl. D8, S. 9, 5. Absatz; siehe Ausführungen zu Merkmal M16.2)

M16.5.1 *the first device being configured for authenticating the second device and*

Gemäß D8 authentifizieren sich beide Geräte gegenseitig (vgl. D8, S. 7, Abschnitt 1.4.4: „The first phase is the authentication phase where the source and sink devices authenticate each other.“). Somit wird insbesondere auch die Senke durch die Quelle authentifiziert, was i.S. des Streitpatents dem Authentifizieren des zweiten Geräts durch das erste Gerät entspricht.

M16.5.2 *then securely sharing the secret with the second device.*

Gemäß der Lehre der D8 werden in einem zweiten Schritt des OCPS-Protokolls nach der Authentifizierungsphase Zufallszahlen und Schlüssel

erzeugt, verschlüsselt und ausgetauscht (vgl. D8, S. 7, Abschnitt 1.4.4: „The second phase is the key exchange phase where random numbers and key material are created, encrypted and exchanged.“). Der verschlüsselte Austausch von Zufallszahlen und Schlüsseln gemäß D8 entspricht dem sicheren Teilen des Geheimnisses i.S. des Streitpatents. Detailliert wird in D8, S. 9, 3. Abs., 2. und 3. Satz beschrieben, dass das Schlüsselmaterial verschlüsselt zur Senke gesendet wird (dort: „The source device generates a 64 bit random number, $\mathbf{R_{source}}$, 128 bits of true random key material, $\mathbf{K_{RandSource}}$, and the OCCI bits encrypts all values using the public key of the sink device creating $\mathbf{E\{K_{PubSink}\}(R_{source},K_{RandSource},}$OCCI). This encrypted value is sent to the sink device, … “.).

Soweit die Beklagte vorgetragen hat, dass gemäß D8 das Teilen des Geheimnisses nicht vor der Abstandsmessung erfolgen würde, sondern ein Teil der Abstandsmessung sei, ändert das nichts an der Beurteilung des Senats. Denn der Anspruchswortlaut verlangt lediglich, dass das Geheimnis bei der Abstandsmessung verwendet wird, und eben nicht, dass die Abstandsmessung erst nach dem Teilen des Geheimnisses begonnen wird (siehe auch Ziff. I. 2 zur Auslegung).

Auch dem Vortrag der Beklagten, wonach jedes Gerät das Geheimnis bekommen könnte, wenn das Teilen des Geheimnisses während der Abstandsmessung erfolge, und damit die Wirkung der Erfindung verfehlt würde, folgt der Senat nicht. Denn, wie die Klägerin zu 1 vorgetragen hat, kennt nur das zuvor authentifizierte Senke-Gerät („sink device“) der D8 den privaten Teil des Schlüsselpaars, mit dem das Geheimnis R_{Source} entschlüsselt werden kann. Im Übrigen stellt damit auch die Abstandsmessung gemäß D8 sicher, dass nur das „richtige Gerät“ die Zufallszahl $\mathbf{R_{source}}$ als $\mathbf{\widetilde{R}_{Source}}$ zurücksenden kann und insofern auch die Wirkung der beanspruchten Erfindung eintritt.

III. Zur Fassung nach dem Hilfsantrag I

Die Patentansprüche 1 und 16 in der Fassung nach Hilfsantrag I eignen sich nicht zur Selbstbeschränkung des Patents, da der Gegenstand des Patentanspruchs 16 nicht neu ist. Gleiches gilt für den Gegenstand des Patentanspruchs 1.

In der Fassung des Patentanspruchs 1 gemäß Hilfsantrag I wurde das Merkmal M1.5.2 der erteilten Fassung durch das Merkmal M1.5.2^{H1} ersetzt, wobei dem Merkmalswortlaut ein „then“ vorangestellt wurde. Darüber hinaus wurde nach dem Merkmal M1.5.2^{H1} das Merkmal M1.5.3^{H1} hinzugefügt (Merkmalsgliederung und Unterstreichung diesseits hinzugefügt):

M1.5.2^{H1} then the first device securely shares the common secret with the second device according to a key management protocol,

M1.5.3^{H1} and wherein the common secret is shared before performing the distance measurement.

In der Fassung des Vorrichtungsanspruchs 16 gemäß Hilfsantrag I wurde gegenüber der erteilten Fassung das Merkmal M16.5.3^{H1} hinzugefügt (Merkmalsgliederung und Unterstreichung diesseits hinzugefügt):

M16.5.3^{H1} before performing the distance measurement.

Gemäß Merkmal M1.5.2^{H1} wird das Verfahren des Patentanspruchs 1 in der Fassung gemäß Hilfsantrag I dahingehend konkretisiert, dass das Teilen des gemeinsamen Geheimnisses zeitlich nach dem Authentifizieren des zweiten Geräts erfolgt, also erst das zweite Gerät authentifiziert wird und dann das Geheimnis geteilt wird. In der erteilten Fassung war diese Reihenfolge zwar im Vorrichtungsanspruch, jedoch nicht im Verfahrensanspruch festgelegt.

Hinsichtlich der Patentfähigkeit gelten die Ausführungen zur erteilten Fassung entsprechend für die Fassung gemäß Hilfsantrag I. Denn hinsichtlich der Reihenfolge (Merkmale M1.5.2^{H1} und M1.5.3^{H1} bzw. M16.5.3^{H1}) lehrt die Druckschrift D8, dass das Geheimnis R_{source} geteilt wird, bevor die Umlaufzeit gemessen wird. Denn für die Laufzeitmessung muss R_{Source} nach dem Teilen noch vom Sink-Gerät als Wert $\widetilde{R}_{Source}$ verschlüsselt an das Source-Gerät zurückgesendet werden, wobei die eigentliche Round-Trip-Zeitmessung sowie die Validierung/der Check des gewünschten Sink-Geräts bei der Abstandsmessung im Source-Gerät nach Empfang der Antwort vom Sink-Gerät durchgeführt wird. Das Messergebnis liegt daher erst nach Empfang und Entschlüsselung des Werts $\widetilde{R}_{Source}$ am Source-Gerät der D8 vor (vgl. D8, S.9, 4. und 5. Abs.; dort: „This encrypted value is sent to the source device, which decrypts the value using $K_{PrvSource}$ and retrieving R_{Sink}, R_{Source} and $K_{RandSink}$. At this point the time needed for R_{Source} to make the round trip is measured“; Unterstreichung diesseits hinzugefügt). Der Wert $\widetilde{R}_{Source}$ wird sodann dort mit dem ursprünglichen Wert R_{Source} zwecks Validierung/Check des korrekten Sink-Geräts verglichen (vgl. D8, S. 9, 6. Abs.; dort: „The source then compares the received R_{Source} with the random number just sent.“). Somit sind auch die gemäß Hilfsantrag I hinzugefügten Merkmale aus der D8 bekannt.

IV. Zur Fassung nach dem Hilfsantrag II

Die Patentansprüche 1 und 15 in der Fassung nach Hilfsantrag II eignen sich nicht zur Selbstbeschränkung des Patents, da der Gegenstand des Patentanspruchs 15 nicht auf einer erfinderischen Tätigkeit beruht. Gleiches gilt für den Gegenstand des Patentanspruchs 1.

In der Fassung des Patentanspruchs 1 gemäß Hilfsantrag II wurde das Merkmal M1.5.3^{H1} der Fassung gemäß Hilfsantrag I durch das Merkmal M1.5.3^{H2} ersetzt und

daran anschließend das Merkmal M1.6^{H2} hinzugefügt (Merkmalsgliederung und Unterstreichung diesseits hinzugefügt):

M1.5.2^{H1} then the first device securely shares the common secret with the second device according to a key management protocol,

M1.5.3^{H2} wherein the common secret has been shared before performing the distance measurement,

M1.6^{H2} the sharing being performed by the steps of
- performing the authentication of the second device by the first device, by checking whether the second device is compliant with a set of predefined compliance rules, and
- if the second device is compliant, sharing the common secret by transmitting said secret to the second device.

In der Fassung des Vorrichtungsanspruchs 15 gemäß Hilfsantrag II wurde das Merkmal M16.5.3^{H2} gegenüber dem Merkmal M16.5.3^{H1} der Fassung des Patentanspruchs 16 gemäß Hilfsantrag I geändert und daran anschließend das Merkmal M16.5.3^{H2} hinzugefügt (Merkmalsgliederung und Unterstreichung diesseits hinzugefügt):

M16.5.3^{H2} wherein the first device is configured to share the common secret before performing the distance measurement,

M16.6^{H2} the sharing being performed by the steps of
- performing the authentication of the second device by the first device, by checking whether the second device is compliant with a set of predefined compliance rules, and
- if the second device is compliant, sharing the common secret by transmitting said secret to the second device.

Mit dem geänderten Merkmal M1.5.3^{H2} bzw. M16.5.3^{H2} wird beansprucht, dass das Teilen des Geheimnisses vor dem Durchführen der Abstandsmessung erfolgen soll bzw. das Kommunikationsgerät geeignet sein soll, jenes vor der Durchführung der Messung zu teilen. Dies ist auch Gegenstand der Patentansprüche in der Fassung nach Hilfsantrag I. Insofern gelten die Ausführungen zur mangenden Neuheit entsprechend.

Mit dem hinzugefügten Merkmal M1.6^{H2} bzw. M16.6^{H2} wird der Anspruchswortlaut in zwei Teilmerkmalen dahingehend konkretisiert, dass erstens die Authentifizierung des zweiten Geräts eine Konformitätsprüfung („checking … compliance rules“) beinhaltet bzw. das erste Gerät geeignet ist, eine Konformitätsprüfung des zweiten Geräts vorzunehmen, und zweitens das Geheimnis an das zweite Gerät übertragen wird bzw. das erste Gerät zur Übertragung des Geheimnisses an das zweite Gerät geeignet ist. Zur Konformitätsprüfung („compliant with a set of predefined compliance rules“) wird in der Streitpatentschrift, Absatz [0023] ausgeführt, dass geprüft wird, ob das zweite Gerät eine erwartete Identität hat, um sicherzustellen, dass das zweite Gerät das Gerät ist, welches es sein sollte. Dies erfolgt durch Überprüfen eines Zertifikats, das im zweiten Kommunikationsgerät gespeichert ist. Insofern versteht der Fachmann, dass das Zertifikat für die Identitätsprüfung zu den „compliance rules“ gehört.

Das zweite Teilmerkmal entnimmt der Fachmann explizit der Druckschrift D8. Denn gemäß D8 wird das Geheimnis R_{Source} vom ersten Gerät („source device“) an das zweite Gerät („sink device“) in verschlüsselter Form übertragen (vgl. D8, S. 8, Fig. 1, dritter Pfeil von oben i.V.m. D8, S. 9, 3. Abs.: „This encryptcd value is sent to the sink device, which decrypts the value using $K_{PrvSink}$ thus receiving R_{Source}, …“).

Somit unterscheidet sich der Gegenstand des Patentanspruchs 15 von der Lehre der D8 lediglich durch das erste Teilmerkmal des Merkmals M16.6^{H2}. Jedoch werden gemäß D8 mit der Authentifizierung auch Zertifikate ausgetauscht (vgl. D8, Fig. 1, „Authentication Phase“), die zur Bestätigung der Identität der Geräte geeignet

sind. Gemäß der Schlüsselverwaltung („key management“) der D8 wird zumindest während der Authentifizierungsphase geprüft, ob bspw. geklonte Geräte kompromittierte Schlüssel verwenden, wobei ein Medienzugriff dieser Geräte mittels kompromittierter Schlüssel durch das Versenden von Widerrufs-Mitteilungen („revocation notice“) durch eine Vertrauensbehörde (TA, „trust authority“) unterbunden werden kann (vgl. D8, Fig. 3 und Kapitel 2, 8, 13).
Auch wenn die Prüfung der Identität eines Geräts nicht explizit in D8 genannt ist, liegt es für den Fachmann nahe, diese Zertifikate für die Prüfung der Identität zu nutzen. Eine erfinderische Tätigkeit kann der Senat darin nicht erkennen.

Gleiches gilt für den Gegenstand des Patentanspruchs 1.

V. Zur Fassung nach dem Hilfsantrag III

Der Senat konnte nicht feststellen, dass dem Gegenstand des Patentanspruchs 16 in der Fassung gemäß Hilfsantrag III vor dem Hintergrund des geltend gemachten Standes der Technik die Neuheit fehlt. Der Gegenstand des Patentanspruchs 16 erweist sich entgegen dem Vortrag der Klägerinnen auch als auf einer erfinderischen Tätigkeit beruhend. Gleiches gilt für den Patentanspruch 1 in der Fassung nach Hilfsantrag III. Die ebenfalls angegriffenen Unteransprüche 2 bis 15 und 17 bis 18 werden von der Patentfähigkeit des Anspruchs 1 bzw. 16 getragen. Der Nichtigkeitsgrund der fehlenden Patentfähigkeit (Art. II, § 6 (1) Nr. 1 IntPatÜG i.V.m. Art. 138 Abs. 1 Buchst. a) liegt daher nicht vor.

In der Fassung des Patentanspruchs 1 gemäß Hilfsantrag III wurde das Merkmal M1.5.2 der erteilten Fassung durch das Merkmal M1.5.2^{H1} ersetzt und daran anschließend das Merkmal M1.7^{H3} hinzugefügt:

M1.5.2^{H1} then the first device securely shares the common secret with the second device according to a key management protocol,

M1.7^{H3} and wherein the first device generates a secure authenticated channel using the shared secret, if the measured distance is within the predefined distance interval, and transmits the protected content to the second device via the secure authenticated channel.

In der Fassung des Patentanspruchs 16 gemäß Hilfsantrag III wurde am Ende des Patentanspruchs in der erteilten Fassung das Merkmal M16.7^{H3} hinzugefügt:

M16.7^{H3} and the first device being configured to generate a secure authenticated channel using the shared secret if the measured distance is within the predetermined distance interval and transmits the protected content to the second device via the secure authenticated channel.

Merkmal **M16.7^{H3}** versteht der Fachmann dahingehend, dass ein sicherer authentifizierter Kanal („secure authenticated channel“) aufgebaut wird, um die geschützten Daten vom ersten Gerät zum zweiten Gerät zu übertragen, wenn (nachdem) der gemessene Abstand zum zweiten Gerät innerhalb des vorbestimmten Bereichs liegt, und dass dafür dasselbe geteilte Geheimnis verwendet wird, das auch für die Abstandsmessung verwendet wurde. Analoges gilt für das Merkmal **M1.7^{H3}**.

1. Der Patentanspruch 16 ist zulässig. Gleiches gilt für den Patentanspruch 1. Aus den ursprünglich eingereichten Anmeldeunterlagen (Offenlegungsschrift, NK4, Abs. [0041]) geht hervor, dass nach der Abstandsmessung Daten gesendet werden können. Der Fachmann liest dabei mit, dass die Abstandsmessung zunächst erfolgreich gewesen sein muss, d.h. der gemessene Abstand innerhalb des vordefinierten Intervalls liegt. Dass das geteilte Geheimnis verwendet werden kann,

um einen SAC aufzubauen, wird ursprünglich offenbart in NK4, Absatz [0022] (dort: „Further, the shared secret can afterwards be used for generating a SAC channel between the two devices.“).

Soweit die Klägerin zu 1 die Auffassung vertritt, ursprünglich sei nicht offenbart, dass das gemeinsame Geheimnis für den Aufbau des SAC benutzt werde (vgl. Schriftsatz der Klägerin v. 20.09.2021, S. 19 ff.), folgt der Senat dieser Auffassung nicht. Denn aus dem Kontext der NK4, Absätze [0021] und [0022] geht hervor, dass das gemeinsame Geheimnis vor der Abstandsmessung geteilt wird und auch für die Abstandsmessung verwendet wird (dort: „the common secret has been shared before performing the distance measurement,“). Dem Fachmann ist klar, dass es sich hierbei um dasselbe Geheimnis wie für den Aufbau des sicheren authentifizierten Kanals (SAC) handelt (dort: „the shared secret can afterwards be used for generating a SAC channel between the two devices“).

2. Der Gegenstand des jeweiligen Patentanspruchs 16 bzw. 1 gilt als neu gegenüber dem Stand der Technik.

a. Der Gegenstand des Patentanspruchs 16 unterscheidet sich von der Lehre gemäß Druckschrift **D8** dadurch, dass das Proposal D8 nicht offenbart, das für die Abstandsmessung verwendete gemeinsame Geheimnis R_{Source} ebenfalls für den Aufbau eines sicheren authentifizierten Kanals zu verwenden. Zwar kennt auch die Lehre gemäß D8 einen solchen sicheren Kanal („secure authenticated channel“, SAC), jedoch wird für diesen der Hashwert H der Parameterkombination **H**($K_{RandSource}$, $K_{RandSink}$, C, $K_{PubSource}$ und $K_{PubSink}$) verwendet, um einen Sitzungsschlüssel („session key“; $K_{Session}$) zu erzeugen, mit dem der Inhalt dann verschlüsselt übertragen wird (vgl. D8, Fig. 1 auf S. 8 und S. 9 vorletzter und letzter Absatz). Die zur Abstandsmessung gemäß D8 geheim übertragene Zufallszahl R_{Source} wird in der D8 somit für den Aufbau des sicheren Übertragungskanals nicht verwendet.

Somit gilt der Gegenstand des Patentanspruchs 16 als neu gegenüber der D8.

Soweit die Klägerinnen vorgetragen haben, dass auch die Zufallszahl $K_{RandSource}$ ein geteiltes Geheimnis sei, da beim Schritt des Schlüsselaustauschs („key exchange phase“) gemäß D8, Fig. 1 auch $K_{RandSource}$ zusammen mit dem Schlüssel $K_{PubSource}$ geheim übertragen werde, führt das nach Überzeugung des Senats nicht zum Gegenstand des Patentanspruchs 16 in der Fassung nach Hilfsantrag III, da die Zufallszahl $K_{RandSource}$ in der D8 nicht für die Abstandsmessung verwendet wird. Denn $K_{RandSource}$ wird vom Quellen-Gerät nur zum Senke-Gerät hinwärts übertragen, aber nicht mehr zurück, wobei die Abstandsmessung erst nach Empfang der Rücknachricht im Quellen-Gerät durchgeführt wird.
Soweit die Klägerinnen weiterhin vorgetragen haben, dass der Fachmann die Zufallszahlen und Schlüssel, die am Quellen-Gerät („source device“) erzeugt wurden, zusammengenommen als gemeinsames, geteiltes Geheimnis betrachten würde, und es gemäß Anspruchswortlaut lediglich erforderlich sei, einen ersten Teil eines Geheimnisses für die Abstandsmessung und einen anderen, zweiten Teil für den Aufbau des sicheren authentifizierten Kanals SAC zu verwenden, greift diese Betrachtungsweise ebenfalls nicht durch. Denn selbst bei dieser Betrachtungsweise, die der Fachmann allenfalls rückschauend in Kenntnis des Anspruchswortlauts angestellt hätte, handelt es sich bei der zur Abstandsmessung verwendeten Zufallszahl R_{Source} um ein anderes Geheimnis als den Schlüssel $K_{RandSource}$, der zur Generierung des Sitzungsschlüssels bzw. letztendlich zum Aufbau des Übertagungskanals SAC verwendet wird.

b. Der Gegenstand des Patentanspruchs 16 in der Fassung nach Hilfsantrag III ist auch neu gegenüber den übrigen Druckschriften D1 bis D7 und D9 bis D10.

Soweit die Klägerinnen bereits schriftsätzlich ihrer Argumentation hinsichtlich mangender Neuheit der Gegenstände der Patentansprüche 1 und 16 in der erteilten Fassung gegenüber jeder der Druckschriften **D1**, **D2** und **D10** die Auslegung

zugrunde legen, dass ein Timeout eine Abstandsmessung sei, was der Senat verneint (siehe oben, Ziff. II.2), vermag der Fachmann diesen Druckschriften jeweils nicht die Merkmale M16.2 und M16.3 in Gänze und das Merkmal M16.4 allenfalls teilweise entnehmen. Entsprechendes gilt für die Merkmale M1.2, M1.3 und M1.4. Dies gilt ebenso für die entsprechenden Merkmale der nebengeordneten Patentansprüche 1 und 16 in der Fassung gemäß Hilfsantrag III.

Darüber hinaus offenbart die Lehre der D1 nicht das Merkmal M16.5.2 (bzw. $M1.5.2^{H1}$), wonach das Teilen des Geheimnisses nach der Authentifizierung des zweiten Geräts erfolgt. Denn das Teilen des Geheimnisses *Km*/*Km'* erfolgt gemäß D1 während der Authentifizierung (vgl. D1, Fig. 2-1 bis 2-3; dort: „First/Second/Third Part of Authentication Protocol").

Die Neuheit des Gegenstandes des Patentanspruchs 16 in der Fassung nach Hilfsantrag III gegenüber den weiteren Druckschriften D2 bis D7 und D9 wurde seitens der Klägerinnen nicht infrage gestellt. Gleiches gilt für den Gegenstand des Patentanspruchs 1 in der Fassung nach Hilfsantrag III.

c. Soweit die Klägerinnen die Beweismittel NK11 bis NK14 vorgelegt haben, ändert sich dadurch an dem Verständnis des Fachmanns hinsichtlich der druckschriftlich genannten Entgegenhaltungen D1 bis D10 nichts.

3. Der Gegenstand des jeweiligen Patentanspruchs 16 bzw. 1 in der Fassung nach Hilfsantrag III beruht auch auf einer erfinderischen Tätigkeit, da er dem Fachmann ausgehend von jeweils einer der Druckschriften D1 bis D10 nicht nahegelegen hatte.

a. Soweit sich der schriftsätzliche Vortrag der Klägerinnen zum Hilfsantrag III hinsichtlich der D1 und D8 in einer Neuheitsbetrachtung erschöpfte (vgl. Schriftsatz der Klägerin zu 1 vom 20. September 2021, S. 20 - 26), stellt der Senat in der Einführung der mündlichen Verhandlung eine ggf. mögliche Kombination der beiden o.g. Druckschriften hinsichtlich der erfinderischen Tätigkeit zur Diskussion. Eine durchgreifende Argumentation, welche Veranlassung der Fachmann gehabt haben könnte, die beiden o.g. Druckschriften in der Weise zu kombinieren, dass ihm der hier in Rede stehende beanspruchte Gegenstand nahegelegen haben könnte, konnte der Vortrag der Klägerinnen nicht überzeugend darlegen. Selbst die mosaikartige Zusammenschau der Druckschriften D1 und D8 führt nicht zum Gegenstand des Patentanspruchs 16, da weder D1 noch D8 lehren, das für die Abstandsmessung verwendete geteilte Geheimnis auch noch für den Aufbau des SAC-Kanals zu verwenden. Denn die Lehre der D8 verwendet für die Abstandsmessung die Zufallszahl R_{Source} und für den Aufbau des SAC-Kanals den SessionKey $K_{session}$ basierend auf $K_{RandSource}$. Die D1 hingegen offenbart überhaupt keine Abstandsmessung, die ein geteiltes Geheimnis verwenden könnte.

Selbst wenn der Fachmann die Lehre des HDCP-Standards zum Anmeldetag gemäß der D1 um eine Abstandsmessung hätte ergänzen wollen, wäre er mit der Anwendung der Abstandsmessung aus D8 noch nicht zum Gegenstand des Patentanspruchs 16 gelangt. Der Fachmann hätte dann noch zusätzlich die Lehre der D8 dahingehend verändern müssen, dass er das in der D8 für die Abstandsmessung verwendete Geheimnis R_{Source} durch das gemeinsame Geheimnis *Km*/*Km‘* der D1 ersetzt hätte, das dann für den Aufbau des SAC-Kanals verwendet werden könnte. Die Schlüssel *Km*/*Km‘* sind für eine Abstandsmessung jedoch nicht geeignet, da sie gemäß D1 überhaupt nicht übertragen werden. Alternativ hätte der Fachmann, um zum Gegenstand des Patentanspruchs 16 zu gelangen, statt R_{Source} den Schlüssel $K_{RandSource}$ gemäß der D8 für die Abstandsmessung verwenden müssen. Dies hätte der Fachmann jedoch nicht vorgesehen. Denn wie die Beklagte zu Recht vorgetragen hat, würde der Fachmann den Schlüssel $K_{RandSource}$ schon deshalb nicht für die Abstandsmessung verwenden,

weil der Schlüssel zur Laufzeitmessung dann von der Quelle zur Senke und zurück hätte übertragen werden müssen, so wie es die D8 für die Abstandsmessung mittels R_{Source} lehrt. Denn wie die Beklagte ebenfalls zu Recht vorträgt, sei jedes unnötige Hin- und Hersenden eines Schlüssels bei einem kryptographischen Verfahren gefährlich, da dies Einfallstore für potenzielle Angreifer bieten würde. Auch aus diesem Grunde hätte der Fachmann diesen Weg sicherlich nicht beschritten. Darüber hinaus hätte der Fachmann auch das asymmetrische Schlüsselprotokoll der D8 durch ein symmetrisches Verfahren – wie in der D1 gelehrt - ersetzen müssen. Entgegen der Auffassung der Klägerin zu 1, wonach der Fachmann sich in der Kryptografie gleich einem Baukasten bedienen würde und im Bewusstsein der Vor - und Nachteile, eine Modifikation der D8 falls nötig vornehmen würde, hatte er nach Überzeugung des Senats keinerlei Veranlassung das asymmetrische Verfahren der D8 zu verlassen und stattdessen ein symmetrisches Schlüsselprotokoll gemäß der D1 anzuwenden.

Auch andersherum hatte der Fachmann keine Veranlassung, ausgehend von der D8 die Lehre der D1 heranzuziehen, denn auch die D1 lehrt nicht das der D8 fehlende Merkmal M16.7 (bzw. M1.7). Vielmehr fehlt der D1 sogar das weitere Merkmal M16.5.2 (bzw. $M1.5.2^{H1}$), wonach das Teilen des Geheimnisses nach der Authentifizierung des zweiten Geräts erfolgt. Denn anders als beim streitpatentgemäßen Gegenstand erfolgt das Teilen des Geheimnisses *Km*/*Km'* gemäß D1 bereits während der Authentifizierung (vgl. D1, Fig. 2-1 bis 2-3, die nur den Authentifizierungsvorgang beschreiben).

Soweit die Klägerinnen vorgetragen haben, dass die Druckschriften D1 und D8 denselben HDCP-Standard beträfen und der Fachmann daher bei der Weiterentwicklung alles in Betracht ziehen würde und grundsätzlich nach der besten Lösung für den Markt suchen würde, wobei er auch die in der D8 als Schwellwert genannte Zeit von 1 ms als zu kurz für eine Abstandsmessung mittels eines rechenintensiven asymmetrischen Verfahrens erkennen und daher weiterhin das symmetrische Protokoll der D1 verwenden würde, teilt der Senat diese Auffassung

nicht. Denn gemäß D8 wird der Abstand mittels des geteilten Geheimnisses R_{Source} gemessen (vgl. D8, S. 9, 5. Abs.) und der Fachmann hatte keine Veranlassung davon abzuweichen. Wenn sich der Vergleichswert von 1 ms für die Laufzeitmessung bei einer Implementierung als zu klein herausstellen sollte, würde der Fachmann als naheliegendste und einfachste Lösung zuerst einmal den Vergleichswert erhöhen, jedoch sicherlich nicht das asymmetrische Verfahren der D8 durch das symmetrische Verfahren der D1 ersetzen.

b. Soweit die Klägerin zu 1 in der mündlichen Verhandlung vorgetragen hat, die Druckschrift D8 allein würde dem Fachmann den Gegenstand des Patentanspruchs 16 nahelegen, da die Druckschrift D8 die Parameter R_{Source} und $K_{RandSource}$ lehre, die der Fachmann ohne weiteres als einen einzigen Parameter zusammenfassen würde, da er durch diese Maßnahme den Parameter R_{Source} einsparen könne, kann der Senat dieser Auffassung nicht beitreten. Denn R_{Source} ist eine 64-bit Zufallszahl (vgl. D8, S. 9, 3. Abs.: „64 bit random number“) und $K_{RandSource}$ ist ein durch spezielle Hardware erzeugter 128-bit Schlüssel (vgl. D8, S. 9, 3. Abs.: „128 bits true random key material“; Unterstreichung hinzugefügt). Sie haben somit unterschiedliche Qualitäten und sind daher weder austauschbar noch zuammenfassbar. Darüber hinaus würde der Fachmann einen kryptographischen Schlüssel auch nicht unnötigerweise hin- und wieder zurückübertragen, wenn er auch eine einfachere Zufallszahl – wie bspw. R_{Source} – für diesen Zweck zur Verfügung hat.

Gleiches gilt für den Gegenstand des Patentanspruchs 1 in der Fassung gemäß Hilfsantrag III.

c. Soweit die Klägerin zu 1 schriftsätzlich (vgl. Schriftsatz von 20. September 2021, S. 27 bis S. 31 oben; dazu nahezu wortgleich in der Nichtigkeitsklage vom 6. Juni 2019, S. 38, Ziff. IV. 1. bis S. 42, 2. Abs) vorgetragen hat, dass die Zusammenschau der Druckschriften D4 und D5 dem Fachmann den Gegenstand

des Patentanspruchs 16 in der Fassung nach Hilfsantrag III nahelegen würde, teilt der Senat diese Auffassung nicht.

Die Druckschrift „Distance-Bounding Protocols“ von S. Brands und D. Chaum (D4) wurde in der Streitpatentschrift zutreffend gewürdigt (vgl. dort, Abs. [0010]). Die D4 offenbart ein Protokoll, das bspw. bei der Zutrittskontrolle zu einem Gebäude genutzt werden kann, um zu bestimmen, ob sich eine zu authentifizierende Partei/Person in räumlicher Nähe zum Eingang befindet. Dazu wird die Signallaufzeit zwischen dem Zugangskontrollrechner des Gebäudes und (dem Gerät) der Person, die Zugang wünscht, verwendet, um den Abstand zu messen, den die Person höchstens vom Eingang des Gebäudes entfernt sein darf. Dieser wird dann mit einer zulässigen Abstandsobergrenze verglichen. Die Laufzeitmessung erfolgt, indem auf ein (einziges) gesendetes Bit unmittelbar mit einem (einzigen) Bit geantwortet wird. Dies wird sequenziell für die Bits jeweils eines Bitmusters α und β (Zufallszahlen) auf beiden Seiten wiederholt. Die für die Abstandmessung verwendeten Signale basieren auf geheimen Schlüsseln (vgl. D4, Abstract i. V. m. D4, Abschnitt 2.3 und 2.4). Ein Zugriff auf geschützte Inhalte, die auf einem der beteiligten Geräte gespeichert sein könnten, wird in der D4 hingegen nicht angesprochen. Der Fachmann entnimmt der D4 also das Merkmal M16.1 nur teilweise sowie die Merkmale M16.5.1, M16.5.2 und $M16.7^{H3}$ gar nicht.

Die Lehre der US 2002/0077984 A1 (D5) betrifft das Teilen von digitalen Medieninhalten („protected digital media“) zwischen Wiedergabegeräten (vgl. D5, Abs. [0001]). Das System gemäß D5 erlaubt Verbrauchern („consumer“), Zugriff auf Kopien digitaler Medien an verschiedenen Orten zu erhalten, ohne die Nutzungsbedingungen zu verletzen (vgl. D5, Abs. [0019]). Das System gemäß Druckschrift D5 verfügt über Mittel, die Nutzungsrechte für die Wiedergabe an unterschiedliche Geräte zu übertragen (vgl. D5, Abs. [0019], letzter Satz). Gemäß der Lehre der D5 wird ein sicherer und authentifizierter Kanal über die Kommunikationsinfrastruktur bereitgestellt (vgl. D5, Abs. [0022]: „A secure and authenticated channel over such communication infrastructures can be used to

transfer digital media and or its associated rights.“). Insbesondere sieht eine Ausführungsform vor, einen SAC („secure authenticated channel“) zu etablieren (vgl. D5, Abs. [0033]: „In one embodiment, each connection to other system components (whether a permanent or temporary connection) is established with a secure authenticated channel (SAC). Generally, a SAC is a mechanism for communicating digital data between two system components over a connection ("channel") that is secure by virtue of the encrypted or otherwise encoded digital data. In addition, each component can verify or authenticate the identity of other components included in the system. “).
Eine Abstandsmessung, insbesondere eine authentifizierte Abstandsmessung, gemäß den Merkmalen M16.2, M16.3 und M16.4 entnimmt der Fachmann der D5 allerdings überhaupt nicht.

Soweit die Klägerin zu 1 schriftsätzlich vorgetragen hat, die D4 liefere dem Fachmann bereits den Anlass, die Lehre der D4 um eine Geräte-Authentifizierung zu erweitern (vgl. Schriftsatz vom 20. Sept. 2021, S. 27, 2. Abs.) und dazu Kapitel 5 der D4 zitiert, teilt der Senat diese Auffassung nicht. Denn die D4 adressiert das Problem, dass ein weit entfernter Teilnehmer mit einem nahen Teilnehmer kooperiere („The techniques presented do not prevent frauds in which a distant party with access to the secret keys is cooperating with a party close by (without conveying the secret keys).“, vgl. D4, S. 358, 2. Abs.). Einen Hinweis bzw. eine Notwendigkeit, eine Authentifizierung vorzusehen, entnimmt der Fachmann daraus nicht. Vielmehr erkennt er, dass an Lösungsansätzen zu o.g. Problem noch gearbeitet werde (ebenda: „We are currently working on some ideas preventing such frauds using distance bounding.“).

Insbesondere erlaubt die D5 keine Kombination mit einer Abstandsmessung, da gemäß D5 ein sicherer authentifizierter Kanal über beliebige Entfernungen (z.B. innerhalb eines Büros, über das Internet, Telefonnetze) aufgebaut wird und keine geographische Beschränkung vorgesehen ist (vgl. D5, Abs. [0022]: „The system can be deployed in a home, office, or any location where a consumer might be

interested in using digital media. Alternatively, the system can span across several different locations such as both the home and office, or multiple homes.“ … ebenda: „Generally stated, the system is not constrained by geographic limitations given access to conventional communication infrastructures such as the Internet, telephone lines and cable systems. A secure and authenticated channel over such communication infra structures can be used to transfer digital media and or its associated rights.“).

Somit stehen beide Druckschriften mit ihren jeweiligen Lehren offensichtlich nebeneinander und ausgehend von der einen gibt es keinen Anlass für den Fachmann dies mit der Lehre der jeweils anderen zu kombinieren.

d. Zu den übrigen Druckschriften D2, D3, D6, D7 und D9 haben die Klägerinnen hinsichtlich des Hilfsantrags III nicht vorgetragen. Auch der Senat kann nicht erkennen, wie diese im Einzelnen oder in Kombination zum Gegenstand des Patentanspruchs 16 in der Fassung nach Hilfsantrag III hätten führen können. Denn diese Druckschriften weisen nicht einmal sämtliche Merkmale des erteilten Patentanspruchs 16 auf. Im Übrigen gehört die am 3. April 2003 und damit nach dem Zeitrang bzw. Prioritätsdatum des Streitpatents veröffentlichte, auch nicht neuheitsschädliche D7 nicht einmal zum Stand der Technik.

4. Mit den Patentansprüchen 1 und 16 haben auch die auf diese rückbezogenen Unteransprüche 2 bis 15 und 17 bis 18 Bestand, da sie jeweils vorteilhafte Weiterbildungen des sie tragenden nebengeordneten Anspruchs beschreiben.

B.

Die Kostenentscheidung beruht auf § 84 Abs. 2 PatG i. V. m. §§ 92 Abs. 1, 100 Abs. 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.

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

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