BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

X ZR 6/22

Verkündet am:
23. Januar 2024
Anderer
Justizangestellte
als Urkundsbeamtin
der Geschäftsstelle

in der Patentnichtigkeitssache

Nachschlagewerk: ja
BGHZ: nein
BGHR: ja

Authentifizierte Abstandsmessung

EPÜ Art. 56; PatG § 4

Eine erfinderische Tätigkeit kann nicht auf ein Merkmal gestützt werden, das eine beliebige, von einem bestimmten technischen Zweck losgelöste Auswahl aus mehreren Möglichkeiten darstellt (Bestätigung von BGH, Urteil vom 13. Juni 2023 - X ZR 51/21, GRUR 2023, 1259 Rn. 72 - Schlossgehäuse).

BGH, Urteil vom 23. Januar 2024 - X ZR 6/22 - Bundespatentgericht

ECLI:DE:BGH:2024:230124UXZR6.22.0

Der X. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 23. Januar 2024 durch den Vorsitzenden Richter Dr. Bacher, die Richter Hoffmann und Dr. Deichfuß, die Richterin Dr. Kober-Dehm und den Richter Dr. Crummenerl

für Recht erkannt:

Auf die Anschlussberufung der Beklagten und unter Zurückweisung der Berufung der Klägerinnen wird das Urteil des 5. Senats (Nichtigkeitssenats) des Bundespatentgerichts vom 20. Oktober 2021 abgeändert.

Das europäische Patent 1 973 297 wird mit Wirkung für die Bundesrepublik Deutschland dadurch teilweise für nichtig erklärt, dass die Patentansprüche 1 und 16 die nachfolgende Fassung erhalten und sich die übrigen Ansprüche auf diese Fassung beziehen.

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.

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.

Im Übrigen wird die Klage abgewiesen.

Von den Kosten des Rechtsstreits erster Instanz tragen die Beklagte 15 % und die Klägerinnen jeweils 42,5 %. Die Kosten des Berufungsverfahrens tragen die Klägerinnen je zur Hälfte.

Von Rechts wegen

Tatbestand:

1 Die Beklagte ist Inhaberin des mit Wirkung für die Bundesrepublik Deutschland erteilten europäischen Patents 1 973 297 (Streitpatents), das am 27. Juni 2003 unter Inanspruchnahme einer europäischen Priorität vom 26. Juli 2002 angemeldet worden ist und eine sichere authentifizierte Abstandsmessung betrifft.

2 Patentanspruch 1, auf den weitere vierzehn Patentansprüche zurückbezogen sind, lautet in der Verfahrenssprache:

> 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 pre-defined 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.

3 Patentanspruch 16, auf den zwei weitere Ansprüche zurückbezogen sind, hat ein Kommunikationsmittel zur Durchführung eines entsprechenden Verfahrens zum Gegenstand.

4 Die Klägerin zu 2, die wegen Verletzung des Streitpatents gerichtlich in Anspruch genommen wird, und die Klägerin zu 1, die diesem Rechtsstreit auf Seiten der Verletzungsbeklagten beigetreten ist, haben geltend gemacht, der Gegenstand des Streitpatents gehe über den Inhalt der ursprünglichen Anmeldeunterlagen hinaus und sei nicht patentfähig. Zudem sei die Erfindung nicht so offenbart, dass ein Fachmann sie ausführen könne. Die Beklagte hat das Streitpatent wie erteilt und hilfsweise in neun geänderten Fassungen verteidigt.

5 Das Patentgericht hat das Streitpatent für nichtig erklärt, soweit es über die mit dem erstinstanzlichen Hilfsantrag III verteidigte Fassung hinausgeht, und die Klage im Übrigen abgewiesen.

6 Mit ihrer dagegen gerichteten Berufung streben die Klägerinnen weiterhin die vollständige Nichtigerklärung des Streitpatents an. Die Beklagte tritt dem Rechtsmittel entgegen. Mit ihrer Anschlussberufung verteidigt sie das Streitpatent vorrangig in den Fassungen der erstinstanzlichen Hifsanträge I und II. Hilfsweise verfolgt sie ihre erstinstanzlichen Hilfsanträge IV bis IX weiter.

Entscheidungsgründe:

7 Die Berufung und die Anschlussberufung sind zulässig. Nur die Anschlussberufung hat Erfolg.

8 I. Das Streitpatent befasst sich mit dem Zugriff auf geschützte digitale Inhalte.

9 1. Nach der Beschreibung des Streitpatents gewinnt die digitale Speicherung von Informationen wie Musik, Video oder Software (im Folgenden: Inhalte) auf Speichermedien wie CD, DVD oder Festplatten zunehmend an Bedeutung. Da das Kopieren digitaler Inhalte anders als beim analogen Format keinen Qualitätsverlust verursache, bestehe die Gefahr unberechtigter Vervielfältigung in besonderem Maße. Dies habe zu einer Vielzahl von Verfahren zum Schutz gegen unerlaubte Kopien geführt (Abs. 1-4).

10 Eine Möglichkeit des Schutzes bestehe darin sicherzustellen, dass Inhalte nur zwischen Vorrichtungen übertragen würden, bei denen die empfangende Vorrichtung als konform (compliant) authentifiziert worden und der Nutzer befugt sei, den Inhalt auf eine solche Vorrichtung zu übertragen. Sei eine Übertragung danach zulässig, erfolge sie typischerweise in verschlüsselter Form (Abs. 5 f.).

11 Die Technologie des sicheren authentifizierten Kanals (secure authenticated channel, SAC) ermögliche die Authentifizierung von Vorrichtungen und die verschlüsselte Übertragung von Inhalten. Dennoch stünden die Rechteinhaber einer Übertragung über das Internet ablehnend gegenüber. Es sei jedoch wünschenswert, dass etwa eine berechtigte Person, die ihren Nachbarn besuche, um mit diesem einen Film anzuschauen, dessen großformatiges Fernsehgerät nutzen könne. Für den Rechteinhaber könne das akzeptabel sein, wenn sichergestellt werde, dass sich der Nutzungsberechtigte in räumlicher Nähe des Fernsehgeräts befinde. Deshalb sei es von Interesse, für die Entscheidung darüber, ob der Zugriff oder die Kopie von Inhalten durch andere Geräte gestattet wird, eine authentifizierte Abstandsmessung zu nutzen (Abs. 7-9).

12 2. Vor diesem Hintergrund betrifft das Streitpatent das technische Problem, eine Möglichkeit zur sicheren Übertragung von Inhalten im Nahbereich bereitzustellen.

13 3. Zur Lösung dieses Problems schlägt Patentanspruch 1 in der in erster Linie verteidigten Fassung ein Verfahren vor, dessen Merkmale sich wie folgt gliedern lassen (Abweichungen von der erteilten Fassung sind hervorgehoben):

14

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),	Verfahren, um zu bestimmen, ob auf geschützten Inhalt, der auf einer ersten Kommunikationsvorrichtung (201) gespeichert ist, von einer zweiten Kommunikationsvorrichtung (203) zugegriffen werden darf,
2	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;	umfassend die Durchführung einer Abstandsmessung zwischen der ersten (201) und der zweiten (203) Kommunikationsvorrichtung und die Prüfung, ob der gemessene Abstand innerhalb eines vorbestimmten Intervalls liegt;
3	the distance measurement is an authenticated distance measurement,	die Abstandsmessung ist eine authentifizierte Abstandsmessung,
4	the first and the second communication device share a common secret,	die erste und die zweite Kommunikationsvorrichtung teilen ein gemeinsames Geheimnis,
4.1	said common secret is used for performing the distance measurement;	das gemeinsame Geheimnis wird für die Durchführung der Abstandsmessung genutzt;

5	the first device (201)	die erste Vorrichtung (201)
5.1	authenticates the second device (203), and	authentifiziert die zweite Vorrichtung (203) und
5.2	then securely shares the common secret with the second device (203) according to a key management protocol;	teilt danach auf sichere Weise das gemeinsame Geheimnis mit der zweiten Vorrichtung (203) entsprechend einem Key-Management-Protokoll;
5.3	the common secret is shared before performing the distance measurement.	das gemeinsame Geheimnis wird geteilt, bevor die Abstandsmessung durchgeführt wird.

15 4. Einige Merkmale bedürfen der Erläuterung:

16 a) Die in Merkmal 5.1 vorgesehene Authentifizierung der zweiten Vorrichtung durch die erste Vorrichtung ist in Patentanspruch 1 nicht näher spezifiziert.

17 Aus dem Zweck der Authentifizierung ergibt sich, dass sie brauchbare Anhaltspunkte dafür ergeben muss, ob das zweite Gerät zur Wiedergabe des Inhalts berechtigt ist. Nach den allgemeinen Erläuterungen in der Beschreibung kann hierzu geprüft werden, ob das zweite Gerät einem Satz vorbestimmter Regeln entspricht (Abs. 22: is compliant with a set of predefined compliance rules). Der Inhalt dieser Regeln und die Kriterien für die Beurteilung, ob das zweite Gerät ihnen entspricht, sind nicht näher festgelegt.

18 Als Möglichkeiten zur technischen Umsetzung der Authentifizierung und des Teilens eines gemeinsamen Geheimnisses führt die Beschreibung beispielhaft die in den ISO-Standards 9798 und 11770 beschriebenen Protokolle an (Abs. 41). Patentanspruch 1 schreibt diese Protokolle nicht zwingend vor.

19 b) Das in Merkmal 4 vorgesehene Teilen eines gemeinsamen Geheimnisses stellt eine weitere Maßnahme zur Berechtigungsprüfung dar.

20 aa) Merkmal 4.1 gibt seinem Wortlaut nach zwar nur vor, dass das gemeinsame Geheimnis zur Durchführung der Abstandsmessung genutzt wird. Aus dem Zusammenhang mit Merkmal 3, wonach es sich um eine authentifizierte Abstandsmessung handeln muss, ergibt sich aber, dass das Teilen des Geheimnisses zugleich der Berechtigungsprüfung dient.

21 Nach den hierauf bezogenen Ausführungen in der Beschreibung gewährleistet die Nutzung des gemeinsamen Geheimnisses bei der Abstandsmessung, dass die Messung nicht mit einer dritten Vorrichtung erfolgt, die das Geheimnis nicht kennt (Abs. 17). Dies stellt sicher, dass die Abstandsmessung in Bezug auf diejenige Vorrichtung erfolgt, die gemäß Merkmal 5.1 authentifiziert worden ist.

22 bb) Nach dem ergänzten Merkmal 5.2 darf das gemeinsame Geheimnis erst nach der Authentifizierung im Sinne von Merkmal 5.1 geteilt werden. Ferner ist ein Key-Management-Protokoll einzusetzen.

23 Als Beispiel für ein hierbei einzusetzendes Key-Management-Protokoll führt die Beschreibung die in ISO 11770-3 beschriebenen Methoden zum Transport oder zum Aushandeln von Schlüsseln an (Abs. 23). Patentanspruch 1 enthält keine Festlegung auf diesen Standard.

24 Die Funktion eines solchen Protokolls besteht darin, das gemeinsame Geheimnis auf sicherem Weg zu teilen, so dass nur berechtigte Vorrichtungen (devices being compliant with compliance rules) das Geheimnis empfangen können (Abs. 23). Auf welche Weise und mit welchem Grad an Sicherheit dies geschieht, gibt Patentanspruch 1 nicht vor.

25 Vor diesem Hintergrund ist nicht zwingend erforderlich, dass das gemeinsame Geheimnis dadurch geteilt wird, dass es von der ersten Vorrichtung an die zweite übermittelt wird. Vielmehr ist auch ein Aushandeln möglich, wie es in der

Beschreibung beispielhaft angeführt wird, also ein Vorgang, bei dem sich die beteiligten Vorrichtungen auf die Verwendung eines bestimmten, ihnen schon zuvor bekannten Geheimnisses verständigen.

26 cc) Der Inhalt des gemeinsamen Geheimnisses ist in Patentanspruch 1 ebenfalls nicht näher festgelegt.

27 Aus dem bereits aufgezeigten Zweck von Merkmal 4 ergibt sich, dass es sich um eine Information handeln muss, auf die nur berechtigte Vorrichtungen Zugriff haben. Bestimmte Mindestanforderungen an die Sicherheit und an die Maßnahmen, um einen unbefugten Zugriff zu verhindern, ergeben sich daraus nicht.

28 c) Die Merkmale 5.1, 4 und 4.1 schließen nicht aus, dass zusätzliche Prüfungen erfolgen, um die Authentizität oder Berechtigung der an dem Verfahren beteiligten Vorrichtungen zu überprüfen.

29 aa) Dem Zusammenspiel der genannten Merkmale ist lediglich zu entnehmen, dass die Prüfung von Authentizität und Berechtigung mindestens mit den beiden darin definierten Verfahrensschritten zu erfolgen hat. Zusätzliche Prüfungen sind weder durch den Zweck dieser Merkmale noch durch sonstige Umstände ausgeschlossen.

30 bb) Für solche zusätzlichen Prüfungen gilt die in den Merkmalen 5.1 und 5.2 definierte Vorgabe für die Reihenfolge nicht.

31 Wie bereits dargelegt wurde, dient auch das Teilen eines gemeinsamen Geheimnisses im Sinne von Merkmal 4 einer zusätzlichen Berechtigungsprüfung. Für diesen Schritt kann die Vorgabe, dass das Geheimnis erst nach Authentifizierung geteilt werden darf, schon deshalb nicht gelten, weil das Teilen des Geheimnisses die zusätzliche Überprüfung erst ermöglichen soll.

32 Vor diesem Hintergrund kann den Merkmalen 5.1 und 5.2 nicht entnommen werden, dass optionale weitere Überprüfungsschritte zwingend vor dem Teilen des Geheimnisses erfolgen müssen. Die Vorgabe zur Reihenfolge gilt vielmehr nur für einen ersten Schritt der Authentifizierung, mit dem sichergestellt wird, dass die zweite Vorrichtung zum Teilen eines gemeinsamen Geheimnisses berechtigt ist.

33 d) Die in den Merkmalen 2 und 3 vorgesehene Abstandsmessung dient dazu, eine Wiedergabe nur auf solchen Vorrichtungen zu ermöglichen, die sich in räumlicher Nähe zur ersten Vorrichtung befinden.

34 aa) Als Mittel zur Durchführung der Messung führt die Beschreibung beispielhaft eine Messung der Umlaufzeit eines Signals (round trip time) an, also der Zeitspanne zwischen dem Aussenden eines bestimmten Signals durch die erste Vorrichtung und dem Eintreffen eines daraufhin von der zweiten Vorrichtung versandten zweiten Signals. Anhand dieser Zeitspanne kann die Entfernung errechnet werden (Abs. 16, 38, 45).

35 Um eine authentifizierte Messung im Sinne von Merkmal 3 zu gewährleisten, kann die zweite Vorrichtung das von ihr empfangene Signal mit Hilfe des gemeinsamen Geheimnisses modifizieren und die modifizierte Fassung an die erste Vorrichtung zurücksenden. Diese kann überprüfen, ob die Modifikation unter Einsatz des gemeinsamen Geheimnisses erfolgt ist (Abs. 16-19, 38, 45).

36 bb) Patentanspruch 1 schreibt diese Vorgehensweise nicht zwingend vor. Er definiert auch keine Anforderungen in Bezug auf die höchstens zulässige Entfernung, die Zeitspanne, aus der die Entfernung gegebenenfalls berechnet wird, und die Genauigkeit der Messmethode.

37 Wie die Parteien im Ansatz übereinstimmend vortragen, hängt die Umlaufzeit eines Signals, also die Zeitspanne zwischen dem Aussenden eines Signals und dem Empfang einer Antwort, nicht nur vom Abstand zwischen den beteiligten Vorrichtungen ab, sondern auch von dem Zeitraum, der für die Verarbeitung des

Signals in der zweiten Vorrichtung benötigt wird. Sofern das Signal über Zwischenstationen geleitet wird, etwa über Router, ist auch deren Verarbeitungsdauer von Bedeutung. Insbesondere die Verarbeitungsdauer in der zweiten Vorrichtung ist nicht ohne weiteres vorhersehbar. Sie hängt von der Rechenleistung des Geräts und dessen aktueller Auslastung ab. Eine auf der Umlaufzeit basierende Abstandsmessung ist deshalb mit Ungenauigkeiten verbunden.

38 Mangels diesbezüglicher Festlegungen in Patentanspruch 1 genügt zur Verwirklichung der Merkmale 2 und 3 jedes Messverfahren, bei der die gemessene Umlaufzeit oder sonstige Messwerte eine Abstandsbestimmung mit einer für praktische Zwecke brauchbaren Genauigkeit ermöglichen.

39 cc) Ob aus dem Fehlen näherer Festlegungen des weiteren folgt, dass es genügt zu prüfen, ob das zweite Signal innerhalb einer bestimmten Zeitspanne eintrifft, ist für die Entscheidung über den Rechtsbestand nicht erheblich und kann daher offen bleiben.

40 e) Die in Merkmal 5.3 definierte Vorgabe für die zeitliche Reihenfolge zwischen dem Teilen des gemeinsamen Geheimnisses und der Durchführung der Abstandsmessung bezieht sich entgegen der Auffassung des Patentgerichts nicht nur auf die Berechnung des Messergebnisses, sondern bereits auf die Ermittlung der Messwerte, die für die Berechnung der Entfernung herangezogen werden.

41 aa) Wie das Patentgericht im Ausgangspunkt zutreffend angenommen hat, ergibt sich eine Festlegung auf diese Reihenfolge nicht schon aus der Vorgabe aus Merkmal 4.1, wonach das gemeinsame Geheimnis für die Durchführung der Abstandsmessung genutzt wird.

42 Dieser Vorgabe mag zu entnehmen sein, dass das gemeinsame Geheimnis für die Erzeugung des Signals genutzt werden muss, das die zweite Vorrichtung zur Durchführung der Messung an die erste Vorrichtung übersendet. Sie schließt aber nicht aus, dass das gemeinsame Geheimnis erst während der

Durchführung der Messung geteilt wird, etwa dergestalt, dass die Zeitmessung in dem Augenblick beginnt, in dem die erste Vorrichtung einen geheimen Wert zum Zwecke des Teilens an die zweite Vorrichtung versendet, und in dem Augenblick endet, in dem das von der zweiten Vorrichtung unter Einsatz des Geheimnisses erzeugte Signal bei der ersten Vorrichtung eintrifft.

43 bb) Entgegen der Auffassung des Patentgerichts ergibt sich aus Merkmal 5.3 jedoch eine weitergehende Anforderung.

44 (1) Merkmal 5.3 ist dahin auszulegen, dass sich die Durchführung der authentifizierten Abstandsmessung nicht in der Berechnung eines Abstands anhand einer ermittelten Laufzeit oder eines sonstigen Messwerts erschöpft.

45 Dieses Merkmal normiert die Anforderung, dass das Geheimnis bereits zuvor geteilt wurde, nicht nur für einzelne Schritte, die zur Durchführung der Abstandsmessung gehören, sondern für diesen Vorgang insgesamt. Es gibt mithin vor, dass die Teilung des gemeinsamen Geheimnisses erfolgen muss, bevor die zur Durchführung der Messung erforderlichen Schritte begonnen haben.

46 (2) Der Vorgabe in Merkmal 4.1 ist zu entnehmen, dass sich die Durchführung der Abstandsmessung nicht in der Berechnung eines Abstands anhand einer ermittelten Laufzeit oder eines sonstigen Messwerts erschöpft.

47 Das gemeinsame Geheimnis findet keinen Eingang in diese Berechnung. Wie bereits oben dargelegt wurde, dient es der Überprüfung, ob das zweite Signal von einer nach Merkmal 5.1 authentifizierten Vorrichtung stammt. Zumindest diese Überprüfung gehört zur Durchführung der (authentifizierten) Abstandsmessung im Sinne der Merkmale 2, 3 und 4.1.

48 (3) Dieses Verständnis von Merkmal 5.3 wird durch die Beschreibung gestützt.

49 Für den Fall der Ermittlung des Abstands anhand der Laufzeit eines Umlaufsignals beginnt die Abstandsmessung danach bereits mit der Übermittlung

des erstens Signals von der ersten Vorrichtung an die zweite Vorrichtung (Abs. 16, ebenso Anspruch 4). Die Verwendung des bereits zuvor geteilten Geheimnisses soll gewährleisten, dass der Abstand nur zu einer authentifizierten Vorrichtung gemessen wird (Abs. 17). Im Einklang damit führt die Beschreibung aus, dass das Geheimnis bereits geteilt worden ist, bevor die Abstandsmessung durchgeführt wird (Abs. 22, ebenso Abs. 45, Sp. 7 Z. 48-51).

50 Die von den Klägerinnen herangezogene Stelle der Beschreibung (Abs. 45, Sp. 8 Z. 8 ff.) rechtfertigt keine abweichende Beurteilung. Sie bestätigt lediglich, dass durch Nutzung des geteilten Geheimnisses für die Durchführung der Abstandsmessung zur Authentifizierung des rücklaufenden Signals sichergestellt wird, dass die Messung nur im Verhältnis zu berechtigten Vorrichtungen erfolgt, nötigt aber nicht zu einem Verständnis des Anspruchs dahin, dass mit der Durchführung der Abstandsmessung nur die Berechnung des Abstands gemeint ist.

51 5. Die in Patentanspruch 16 geschützte Vorrichtung wird durch ihre Eignung für ein Verfahren mit den Merkmalen von Patentanspruch 1 geprägt und unterliegt deshalb derselben Beurteilung.

52 Der Umstand, dass in der erteilten Fassung nur Patentanspruch 16 eine Reihenfolge zwischen der Authentifizierung der zweiten Vorrichtung und dem Teilen des gemeinsamen Geheimnisses vorsieht, ist für die Beurteilung der in der Berufungsinstanz verteidigten Fassungen unerheblich, weil danach auch Patentanspruch 1 in Merkmal 5.2 den Ausdruck "then" enthält.

53 II. Das Patentgericht hat seine Entscheidung im Wesentlichen wie folgt begründet:

54 Die Nichtigkeitsgründe der unzulässigen Erweiterung und der mangelnden Ausführbarkeit lägen nicht vor.

55 Der Gegenstand der erteilten Fassung der Patentansprüche 16 und 1 sei gegenüber dem aus dem Hause der Beklagten stammenden Vorschlag für ein

Open Copy Protection System (OCPS; Epstein/Pasieka, Philips Research Proposal to Broadcast Protection Discussion Group, Version 1.4 vom 7. Mai 2002, D8) nicht neu. Für die Fassung nach dem erstinstanzlichen Hilfsantrag I (jetzt: Hauptantrag) gelte nichts anderes. Der mit dem erstinstanzlichen Hilfsantrag I (jetzt: Hilfsantrag II) verteidigte Gegenstand sei durch D8 nahegelegt.

56 Der mit dem erstinstanzlichen Hilfsantrag III verteidigte Gegenstand sei ursprünglich offenbart und patentfähig. D8 offenbare nicht, dass das gleiche gemeinsame Geheimnis sowohl für die Abstandsmessung als auch für den Aufbau eines sicheren authentifizierten Kanals verwendet werde. Der von I. stammende Vorschlag für ein High-bandwith Digital Content Protection System (HDCP; Revision 1.0 vom 17. Februar 2000, D1) zeige keine Abstandsmessung und offenbare nicht, dass das Geheimnis erst geteilt werde, nachdem das zweite Gerät authentifiziert worden sei. Der verteidigte Gegenstand beruhe auch auf erfinderischer Tätigkeit. Selbst wenn die Lehre der D1 um eine Abstandsmessung nach D8 ergänzt werde, fehle es an einer Anregung, das für die Abstandsmessung genutzte Geheimnis auch für den Aufbau des sicheren authentifizierten Kanals zu verwenden. Ausgehend von D8 sei der verteidigte Gegenstand durch keine Entgegenhaltung nahegelegt.

57 III. Diese Beurteilung hält den Angriffen der Anschlussberufung nicht stand.

58 1. Der mit dem Hauptantrag (erstinstanzlich: Hilfsantrag I) verteidigte Gegenstand geht entgegen der Auffassung der Klägerinnen nicht über den Inhalt der ursprünglich eingereichten Unterlagen hinaus.

59 a) Nach der Rechtsprechung des Senats ist ein beanspruchter Gegenstand ursprünglich offenbart, wenn die im Anspruch bezeichnete technische Lehre den Ursprungsunterlagen in ihrer Gesamtheit unmittelbar und eindeutig als eine mögliche Ausführungsform der Erfindung zu entnehmen ist.

60 Danach ist ein "breit" formulierter Anspruch unter dem Gesichtspunkt der unzulässigen Erweiterung jedenfalls dann unbedenklich, wenn sich ein in der Anmeldung beschriebenes Ausführungsbeispiel der Erfindung aus fachlicher Sicht als Ausgestaltung der im Anspruch beschriebenen allgemeineren technischen Lehre darstellt und diese Lehre in der beanspruchten Allgemeinheit bereits der Anmeldung als zu der angemeldeten Erfindung gehörend entnehmbar ist. Dies gilt insbesondere dann, wenn von mehreren Merkmalen eines Ausführungsbeispiels, die zusammengenommen, aber auch für sich betrachtet, dem erfindungsgemäßen Erfolg förderlich sind, nur eines oder nur einzelne in den Anspruch aufgenommen worden sind (vgl. nur BGH, Urteil vom 13. Juni 2023 - X ZR 47/21, GRUR 2023, 1274 Rn. 161 f. - Anschlussklemme).

61 b) Diesen Anforderungen wird die mit dem Hauptantrag verteidigte Fassung von Patentanspruch 1 gerecht.

62 aa) Wie die Beklagte zutreffend dargelegt hat, findet diese Fassung ihre Grundlage in den Absätzen 34 und 35 mit der nachstehend wiedergegebenen Figur 2 der ursprünglichen Anmeldung (NK4).

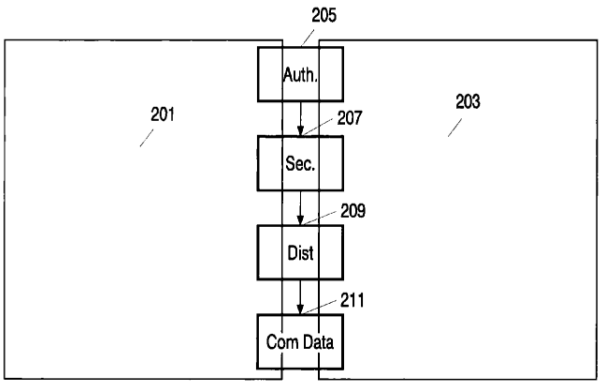

FIG. 2

63 In den genannten Absätzen wird die Abfolge der Ereignisse dahin beschrieben, dass die erste Vorrichtung (201) zunächst die zweite Vorrichtung (203) authentifiziert (Schritt 205), sodann ein Geheimnis mit ihr teilt (Schritt 207) und

nachfolgend eine Abstandsmessung durchgeführt wird (Schritt 209), bevor schließlich Daten übertragen werden (Schritt 211).

64 bb) Entgegen der Auffassung der Klägerinnen führt der Umstand, dass diese Reihenfolge in der Anmeldung sowohl an den oben wiedergegebenen Stellen (Abs. 35 f.) als auch an anderer Stelle (Abs. 42) nur in Zusammenhang mit einer Messung der Umlaufzeit eines Signals beschrieben wird, nicht zu einer abweichenden Beurteilung.

65 Schon der Bezug auf Figur 2, in der die aufeinanderfolgenden Schritte ohne Konkretisierung der Messmethode aufgeführt werden, spricht dafür, dass zwischen der dargestellten Reihenfolge und der Art und Weise, in der die Abstandsmessung erfolgt, kein zwingender Zusammenhang besteht. Dies wird bestätigt durch den Umstand, dass eine Abstandsmessung, wie sie in Figur 2 und den darauf bezogenen Ausführungen dargestellt ist, an anderer Stelle der Anmeldung (Abs. 15) unabhängig von der in Figur 2 dargestellten Reihenfolge als Beispiel für eine authentifizierte Abstandsmessung beschrieben wird.

66 Vor diesem Hintergrund ergibt sich aus den ebenfalls in der Anmeldung enthaltenen Ausführungen, wonach zunächst eine Authentifizierung erfolgt und danach ein gemeinsames Geheimnis geteilt wird (Abs. 21), ebenfalls keine abweichende Beurteilung. Auch diese Passage deutet vielmehr darauf hin, dass die im Anschluss beschriebene Abstandsmessung erst nach dem Teilen des gemeinsamen Geheimnisses beginnt und nicht zwingend nach dem Vorbild der in der Anmeldung geschilderten Ausführungsbeispiele erfolgen muss.

67 2. Der mit dem Hauptantrag (erstinstanzlich: Hilfsantrag I) verteidigte Gegenstand von Patentanspruch 1 ist neu.

68 a) D8 nimmt diesen Gegenstand nicht vollständig vorweg.

69 aa) D8 unterbreitet einen Vorschlag für einen verbesserten Schutz gegen unberechtigten Zugriff bei der Übertragung geschützten Inhalts von einer als

Quelle (source) bezeichneten ersten Vorrichtung an eine als Senke (sink) bezeichnete zweite Vorrichtung.

70 Die Entgegenhaltung schlägt eine Vorgehensweise vor, die fünf Phasen umfasst und in der nachfolgend wiedergegebenen Figur 1 schematisch dargestellt ist.

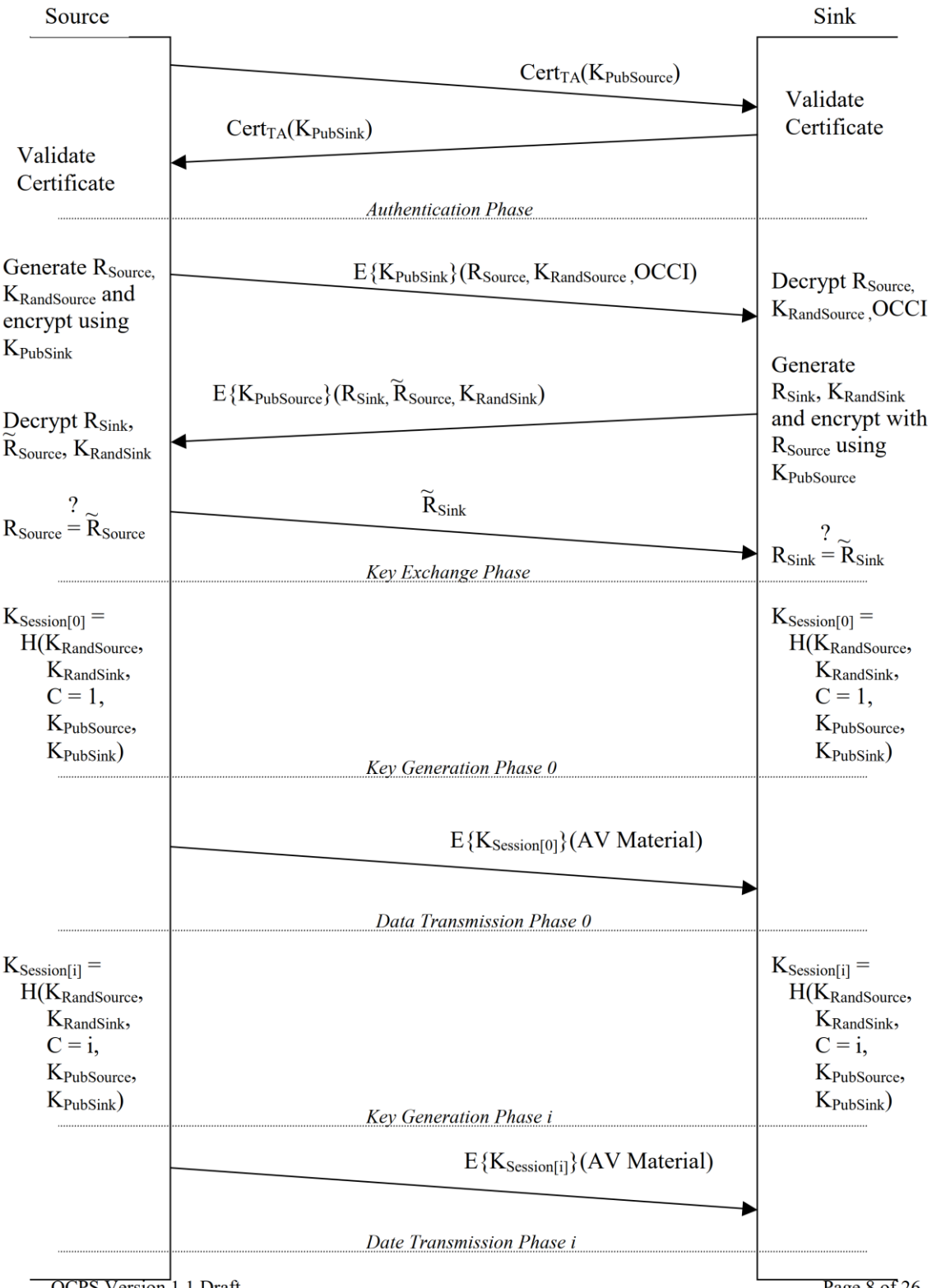

Figure 1 OCPS Key Agreement Protocol

71 In der ersten Phase (authentication phase) authentifizieren die Quelle und die Senke sich wechselseitig. Dazu übermittelt die Quelle der Senke einen öffentlichen Schlüssel und ein Zertifikat einer vertrauenswürdigen Stelle (Trust Authority). Stellt die Senke fest, dass diese in Ordnung sind, übermittelt sie ihrerseits der Quelle einen öffentlichen Schlüssel und ein Zertifikat einer vertrauenswürdigen Stelle. Sind Zertifikat und öffentlicher Schlüssel der Senke nicht zu beanstanden, wird der Schlüssel akzeptiert (S. 7 letzter Absatz und S. 9 Abs. 1 f.).

72 In der zweiten Phase (key exchange phase) erzeugt die Quelle zwei Zufallszahlen (R_{Source}, $K_{RandSource}$). Diese werden zusammen mit weiteren Daten mit dem öffentlichen Schlüssel der Senke verschlüsselt und an die Senke übertragen. Die Senke entschlüsselt die Zufallszahl (R_{Source}) mit Hilfe ihres privaten Schlüssels und erzeugt zwei weitere Zufallszahlen (R_{Sink}, $K_{RandSink}$). Sie verschlüsselt alle drei Zahlen (R_{Sink}, R_{Source}, $K_{RandSink}$) sodann mit dem öffentlichen Schlüssel der Quelle und übermittelt sie an diese. Die Quelle entschlüsselt die Zahlen mit Hilfe ihres privaten Schlüssels (S. 9 Abs. 3 f.).

73 Die Quelle misst die Zeit, die benötigt wurde, um die Zufallszahl (R_{Source}) von der Quelle zur Senke und wieder zurück zu übertragen und vergleicht diese mit einem Grenzwert von einer Millisekunde. Wenn die gemessene Zeit den Grenzwert überschreitet und die einschlägigen Regelungen eine nicht-lokale Übertragung verbieten, wird der Vorgang abgebrochen (S. 9 Abs. 5).

74 Anderenfalls vergleicht die Quelle, ob der empfangene Wert (R_{Source}) mit dem von ihr übermittelten übereinstimmt. Wenn dies der Fall ist, übermittelt sie die von der Senke erzeugte Zufallszahl (R_{Sink}) verschlüsselt an die Senke. Diese überprüft ebenfalls, ob der empfangene Wert mit dem übermittelten übereinstimmt und ob die gemessene Zeit unterhalb des Grenzwerts von einer Millisekunde liegt (S. 9 Abs. 6 f.).

75 In der dritten Phase (key generation phase) erzeugen die Quelle und die Senke jeweils einen Sitzungsschlüssel. Diesen errechnen sie mit Hilfe ihrer beiden öffentlichen Schlüssel ($K_{PubSource}$, $K_{PubSink}$) und der in der zweiten Phase übermittelten Zufallswerte ($K_{RandSource}$, $K_{RandSink}$).

76 Dieser Schlüssel wird in der vierten Phase (information transmisson stage) zur Verschlüsselung der übermittelten Inhalte eingesetzt (S. 9 Abs. 8 f.).

77 bb) Damit sind die Merkmale 1 bis 5.2 offenbart.

78 (1) Zu Recht ist das Patentgericht zu dem Ergebnis gelangt, dass die Abstandsmessung anhand der Umlaufzeit der Zufallszahl (R_{Source}) den Anforderungen von Merkmal 2 entspricht.

79 Der Umstand, dass ein sich mit Lichtgeschwindigkeit ausbreitendes Signal innerhalb der in D8 offenbarten Obergrenze von einer Millisekunde eine Entfernung von 300 Kilometern zurücklegen kann (also je 150 Kilometer Hin- und Rückweg), deutet allerdings darauf hin, dass die in D1 offenbarte Methode nur dann einen Rückschluss auf eine lokale Gegenstelle ermöglicht, wenn die Zeitspanne bis zum Eintreffen der Antwort nicht nur durch die Laufzeit des Signals bestimmt wird, sondern auch durch die für dessen Verarbeitung benötigten Zeiträume.

80 Wie bereits oben dargelegt wurde, schließt Merkmal 2 den Einsatz von Methoden, die mit derartigen Unsicherheiten verbunden sind, indes nicht aus.

81 (2) Ebenfalls zu Recht hat das Patentgericht entschieden, dass die Zufallszahl (R_{Source}) ein gemeinsames Geheimnis von Quelle und Senke im Sinne von Merkmal 4.1 darstellt. Aufgrund der für die Übertragung eingesetzten Verschlüsselung ist dieser Wert nur für die beiden an dem Vorgang beteiligten Vorrichtungen zugänglich.

82 cc) Entgegen der Auffassung des Patentgerichts ist Merkmal 5.3 hingegen nicht offenbart.

83 Das Teilen des gemeinsamen Geheimnisses und die Durchführung der Abstandsmessung erfolgen bei dem in D8 offenbarten Verfahren nicht zeitlich nacheinander. Die Übermittlung des gemeinsamen Geheimnisses (R_{Source}) von der Quelle an die Senke stellt zugleich den ersten Schritt der Abstandsmessung dar.

84 Die abweichende Auffassung der Klägerinnen beruht auf einer abweichenden Auslegung von Merkmal 5.3. Diese Auslegung trifft aus den oben aufgezeigten Gründen nicht zu.

85 b) Der mit dem Hauptantrag verteidigte Gegenstand ist auch durch D1 nicht vorweggenommen.

86 aa) D1 befasst sich mit dem Schutz der Übertragung von Videodaten von einem Sender (Digital Visual Interface Video Transmitter, DVI-Transmitter, Host) zu einem Empfänger (Digital Visual Interface Video Receiver).

87 Der erste Schritt der Authentifizierung ist in der nachfolgend wiedergegebenen Figur 2-1 schematisch dargestellt.

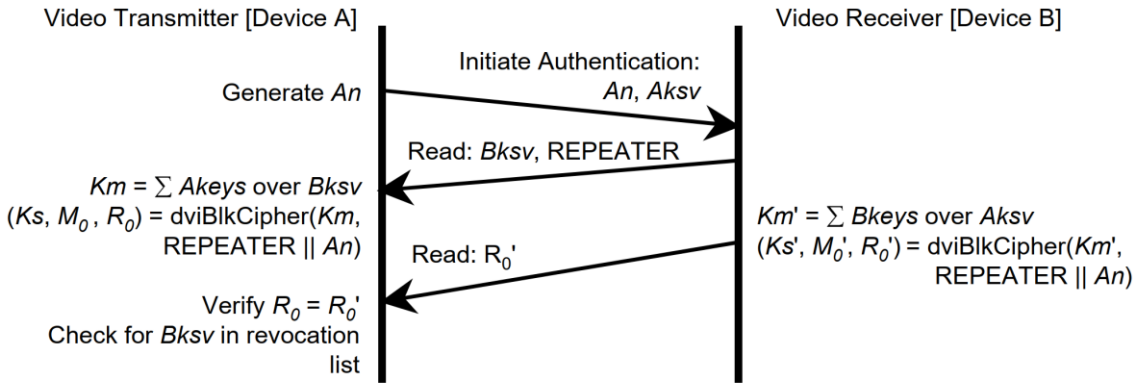

Figure 2–1. First Part of Authentication Protocol

88 Autorisierte Teilnehmer erhalten von einem mit dieser Aufgabe befassten Unternehmen (Digital Content Protection LLC) für ihre Anzeigegeräte einen Key Selection Vector (KSV) und einen Satz von geheimen Geräteschlüsseln (S. 6 Abschnitt 2.1).

89 Der Sender übermittelt dem Empfänger eine Zufallszahl (An) und den Key Selection Vector des Senders (Aksv). Der Empfänger antwortet mit der Übermittlung des ihm zugewiesenen Key Selection Vectors (Bksv). Dieser wird darauf geprüft, ob er nicht widerrufen ist und je zwanzigmal die Werte 1 und 0 enthält (S. 6 Abschnitt 2.2).

90 Auf der Grundlage des Key Selection Vectors der jeweiligen Gegenstelle berechnen Sender und Empfänger einen geheimen Wert (Km bzw. Km'). Diese Werte stimmen überein, wenn alle geheimen Geräteschlüssel und der verwendete Key Selection Vector valide sind (S. 7 Abs. 1-3).

91 Auf der Grundlage des geheimen Werts (Km bzw. Km') und der Zufallszahl (An) berechnen Sender und Empfänger je drei Werte (Ks, M_0, R_0). Der Empfänger übermittelt den von ihm errechneten Wert (R_0') an den Sender. Dieser Wert muss für den Sender innerhalb von 100 Millisekunden nach Beendigung des Schreibens von Aksv an den Empfänger zum Lesen verfügbar sein. Die in Sender und Empfänger berechneten Werte (R_0 bzw. R_0') stimmen überein, wenn die Authentifikation erfolgreich war (S. 7 Abs. 4 f.).

92 Die Prüfung, ob der Key Selection Vector (Bksv) widerrufen wurde, ist in Figur 2-1 - abweichend von der oben wiedergegeben textlichen Beschreibung (S. 6 Abschnitt 2.2) - erst als letzter Schritt dargestellt. Bei der Beschreibung des Betriebszustandes, in dem der Sender die Werte (R_0, R_0') vergleicht (State A3), wird darauf hingewiesen, die Überprüfung der Widerrufsliste für Bksv könne asynchron zu den übrigen Teilen des Protokolls ausgeführt werden und unmittelbar nach der Übermittlung dieses Vektors beginnen; sie müsse aber spätestens vor dem Übergang in den authentifizierten Status (A4) beendet sein (S. 12 zu Status A3).

93 Im zweiten Teil des in D1 beschriebenen Authentifizierungsprotokolls überprüft der Sender, ob der Empfänger Bereitschaft meldet und ob eine Weitergabe von Inhalten an Geräte dieser Ebene zulässig ist (S. 8 f.).

94 Ein dritter Teil des Authentifizierungsprotokolls wird vor der Übermittlung einzelner Videoframes ausgeführt. Hierbei erzeugen Sender und Empfänger zusätzliche Schlüssel (K_i, M_i, R_i) und der Sender überprüft, ob der vom Empfänger erzeugte und übermittelte Parameter (R_i') mit dem von ihm erzeugten Parameter (R_i) übereinstimmt. Wenn der Lesevorgang für den Parameter (R_i') nicht innerhalb von 250 Millisekunden nach dessen Einleitung abgeschlossen ist, wird die DVI-Verbindung als nicht authentifiziert betrachtet (S. 10).

95 Die Inhalte werden vor der Übermittlung an den Empfänger verschlüsselt (S. 24 Abschnitt 3). Hierzu werden die bereits erwähnten Schlüssel (K_s, K_i) eingesetzt. Diese werden wie bereits erwähnt aus dem geheimen Wert (Km) und dem Zufallswert (An) abgeleitet.

96 bb) Damit sind die Merkmale 1, 4 und 5.1 offenbart.

97 cc) Zu Recht ist das Patentgericht zu dem Ergebnis gelangt, dass die in den Merkmalen 5.1 und 5.2 vorgegebene Reihenfolge, wonach das gemeinsame Geheimnis erst nach der Authentifizierung der zweiten Vorrichtung geteilt wird, in D1 nicht offenbart ist.

98 (1) Zutreffend hat das Patentgericht angenommen, dass das Berechnen der Werte (Km, Km') nicht nur der Festlegung eines gemeinsamen Geheimnisses dient, sondern zugleich der Authentifikation.

99 (2) Entgegen der Auffassung des Patentgerichts steht dies einer Offenbarung der in Patentanspruch 1 definierten Reihenfolge allerdings nicht schon deshalb entgegen, weil die Überprüfung der mit Hilfe des gemeinsamen Geheimnisses (Km, Km') errechneten Werte (R_0, R_0') in D1 ebenfalls als Teil des Authentifizierungsvorgangs bezeichnet wird.

100 Wie oben dargelegt wurde, gilt die Vorgabe zur Reihenfolge aus den Merkmalen 5.1 und 5.2 nur für einen ersten Schritt der Authentifizierung, mit dem sichergestellt wird, dass die zweite Vorrichtung zum Teilen eines gemeinsamen Geheimnisses berechtigt ist. Ein erster Authentifizierungsschritt in diesem Sinne

liegt bei dem in D1 offenbarten Verfahren schon im Austausch der Key Selection Vectors und der Überprüfung des vom Empfänger übermittelten Vectors durch den Sender. Folglich würde es ausreichen, wenn das Teilen eines gemeinsamen Geheimnisses diesem Schritt nachfolgt.

101 (3) Wie die Beklagte zu Recht geltend macht, dient der Austausch der Key Selection Vectors bei dem in D1 offenbarten Verfahren indes auch dem Teilen eines gemeinsamen Geheimnisses.

102 Das gemeinsame Geheimnis steht den beiden Vorrichtungen zwar erst nach dem Berechnen der Werte (Km, Km') zur Verfügung. Dieser Prozess wird aber bereits durch den Austausch der Key Selection Vectors eingeleitet, weil diese die Auswahl der Schlüssel ermöglichen, mit deren Hilfe die Werte (Km, Km') ermittelt werden. Der Austausch der Vektoren entspricht mithin einem Key-Management-Protokoll im Sinne von Merkmal 5.2. Damit überschneiden sich die Authentifizierung im Sinne von Merkmal 5.1 und das Teilen des Geheimnisses im Sinne von Merkmal 5.2 bei D1 jedenfalls teilweise. Dies entspricht nicht der in diesen Merkmalen vorgegebenen Reihenfolge.

103 dd) Ebenfalls nicht offenbart ist eine Abstandsmessung im Sinne der Merkmale 2, 3, 4.1 und 5.3.

104 (1) In diesem Zusammenhang kann dahingestellt bleiben, ob die in D1 beschriebene Timeout-Regel, nach der der Vorgang abgebrochen wird, wenn der Sender den vom Empfänger zu übermittelnden Wert R_0' nicht innerhalb von 100 Millisekunden lesen kann, eine Messung im Sinne der genannten Merkmale darstellt.

105 Diese Messung wird bei dem in D1 offenbarten Verfahren jedenfalls nicht zur Ermittlung des Abstands eingesetzt.

106 (2) Ebenfalls offen bleiben kann die Frage, ob es zur Offenbarung der Merkmale 2, 3 und 4.1 ausreichen würde, wenn eine Überschreitung des Zeitlimits bei dem in D1 beschriebenen Verfahren objektiv die Möglichkeit eröffnete,

Rückschlüsse auf den räumlichen Abstand zwischen den beteiligten Vorrichtungen zu ziehen.

107 Den Ausführungen aus D1 lässt sich nicht entnehmen, welche Faktoren für die Definition des Zeitlimits von 100 Millisekunden ausschlaggebend sind. Angesichts dessen lässt sich der Entgegenhaltung nicht eindeutig entnehmen, ob eine Überschreitung dieses Limits Rückschlüsse auf die Entfernung zwischen den beiden Vorrichtungen zulässt.

108 (3) Bezüglich des in D1 offenbarten Zeitlimits von 250 Millisekunden für die nachfolgenden Werte (R_i') gilt Entsprechendes.

109 3. Der mit dem Hauptantrag verteidigte Gegenstand beruht auch auf erfinderischer Tätigkeit.

110 a) Auf der Suche nach Lösungen für das dem Streitpatent zugrunde liegende technische Problem bestand ausgehend von D1 allerdings Anlass, ähnliche Verfahren darauf zu untersuchen, ob sie eine Möglichkeit der Entfernungsmessung bieten.

111 Hierzu bot sich eine ergänzende Heranziehung von D8 an, weil dort eine einfache Möglichkeit zur Unterscheidung von lokalen und nicht lokalen Zugriffen aufgezeigt wird und das dafür eingesetzte Mittel - eine Zeitmessung - in D1 ohnehin bereits vorgesehen ist.

112 b) Auch eine Kombination von D1 und D8 führt jedoch nicht zu einer Verwirklichung aller Merkmale von Patentanspruch 1.

113 aa) Wenn die in D1 vorgesehene Messung der Umlaufzeit für den Wert (R_0/R_0') so ausgestaltet wird, dass sie zugleich zur Abstandsmessung eingesetzt werden kann, sind zwar die Merkmale 2, 3, 4.1 und 5.3 verwirklicht, nicht aber die in den Merkmalen 5.1 und 5.2 vorgegebene Reihenfolge.

114 Auch bei einer solchen Modifikation finden die Authentifizierung und das Teilen des gemeinsamen Geheimnisses teilweise nebeneinander statt.

115 bb) Wenn die Abstandsmessung, wie von den Klägerinnen postuliert, mit Hilfe des im ersten Schritt übermittelten Wertes (An) durchgeführt wird, fehlt es zusätzlich an der Verwirklichung von Merkmal 5.3.

116 Bei dieser Ausgestaltung beginnt die Durchführung der Abstandsmessung vor dem Teilen des gemeinsamen Geheimnisses und zudem gleichzeitig mit der Authentifizierung.

117 Die Klägerinnen zeigen nicht auf, dass sich aus dem Stand der Technik eine Anregung ergab, das in D8 beschriebene Verfahren bei einem Einsatz im Umfeld von D1 dahin abzuwandeln, dass die Abstandsmessung erst erfolgt, nachdem die erste Vorrichtung ein gemeinsames Geheimnis mit der zweiten Vorrichtung geteilt hat.

118 cc) Aus dem in D8 enthaltenen Hinweis, dass der Zeitpunkt der Überprüfung des Vektors (Bksv) in unterschiedlicher Weise festgelegt werden kann, ergeben sich keine weitergehenden Anregungen in Richtung auf das Streitpatent.

119 (1) Eine nähere Analyse der in D1 und D8 offenbarten Verfahren könnte allerdings die Erkenntnis vermitteln, dass die Schritte der Authentifizierung, des Teilens eines gemeinsamen Geheimnisses und der Abstandsmessung mit Hilfe einer Umlaufzeit zumindest teilweise auch zeitgleich ausgeführt werden können.

120 Wie bereits oben dargelegt wurde, finden bei dem in D1 offenbarten Verfahren die Authentifizierung und das Teilen des gemeinsamen Geheimnisses teilweise gleichzeitig statt, während die Messung der Umlaufzeit in einem nachfolgenden Schritt erfolgt. Bei dem in D8 offenbarten Verfahren folgen demgegenüber die Authentifizierung und das Teilen eines gemeinsamen Geheimnisses aufeinander, während die Messung der Umlaufzeit sich mit dem Teilen des Geheimnisses überschneidet.

121 Technische Unterschiede, die diese Einteilung im jeweiligen Kontext als zwingend erscheinen lassen, sind in den Entgegenhaltungen nicht offenbart und

auch sonst nicht ersichtlich. Daraus könnte die Schlussfolgerung gezogen werden, dass die zeitliche Abfolge im Wesentlichen eine Frage der Zweckmäßigkeit ist und dass je nach Ausgestaltung auch alle drei Verfahrensschritte getrennt aufeinander folgen können.

122 (2) Anhaltspunkte, die eine solche analytische Betrachtung nahelegen könnten, ergeben sich jedoch weder aus D1 oder D8 noch aus sonstigen Umständen.

123 dd) Aus den in D1 enthaltenen Ausführungen zum dritten Teil des Authentifikationsprotokolls ergaben sich keine weitergehenden Anregungen.

124 Wenn bei dem in D1 offenbarten Verfahren eine Abstandsmessung erst in Zusammenhang mit dem Versand der Parameter (R_i') erfolgt, ist zwar Merkmal 5.3 verwirklicht, weil das Teilen eines gemeinsamen Geheimnisses in diesem Zeitpunkt bereits abgeschlossen ist. Auch diese Ausgestaltung verwirklicht aber nicht die zeitliche Reihenfolge nach den Merkmalen 5.1 und 5.2.

125 c) Entgegen der Auffassung der Klägerinnen ist es technisch nicht völlig belanglos und damit beliebig, ob die im Hauptantrag aufgeführten Verfahrensschritte sich überschneiden oder aufeinander folgen.

126 aa) Nach der Rechtsprechung des Senats kann eine erfinderische Tätigkeit nicht auf ein Merkmal gestützt werden, das eine beliebige, von einem bestimmten technischen Zweck losgelöste Auswahl aus mehreren Möglichkeiten darstellt (BGH, Urteil vom 13. Juni 2023 - X ZR 51/21, GRUR 2023, 1259 Rn. 72 - Schlossgehäuse).

127 bb) Die in dem Merkmal 5.3 vorgesehene zeitliche Abfolge kann nicht als technisch beliebig angesehen werden.

128 Wie bereits oben dargelegt wurde, wird die Laufzeit eines Signals unter anderem dadurch beeinflusst, in welchem Umfang das Signal Gegenstand von

Rechenoperationen ist. Je umfangreicher solche Berechnungen sind, umso eher kann sich dies nachteilig auf die Genauigkeit der Abstandsmessung auswirken.

129 Vor diesem Hintergrund eröffnet die in Merkmal 5.3 vorgegebene Reihenfolge die Möglichkeit zu einer erhöhten Genauigkeit, weil die zum Teilen des Geheimnisses erforderlichen Rechenoperationen vor Beginn der Messung ausgeführt werden, auf deren Ergebnis also keinen Einfluss haben. Die Reihenfolge dieser Schritte ist mithin aus technischer Sicht nicht beliebig.

130 d) Ausgehend von D8 ergaben sich ebenfalls keine weitergehenden Anregungen.

131 Dabei kann dahingestellt bleiben, ob ausgehend von D8 Anlass bestand, einzelne Verfahrensschritte durch vergleichbare Schritte aus D1 zu ersetzen. Selbst wenn dies der Fall gewesen wäre, hätte eine solche Kombination aus den oben dargelegten Gründen die Merkmale von Patentanspruch 1 in ihrer Gesamtheit weder verwirklicht noch nahegelegt.

132 IV. Die Kostenentscheidung beruht auf § 121 Abs. 2 PatG sowie § 91 Abs. 1 und § 97 Abs. 1 ZPO.

Bacher Hoffmann Deichfuß

Richterin am Bundesgerichtshof
Dr. Kober-Dehm kann nicht
unterschreiben, weil ihr keine
Signaturkarte zur Verfügung steht.
Bacher

Crummenerl

Vorinstanz:
Bundespatentgericht, Entscheidung vom 20.10.2021 - 5 Ni 13/19 (EP) -