# BUNDESGERICHTSHOF

## IM NAMEN DES VOLKES

## URTEIL

X ZR 29/21

Verkündet am:
4. April 2023
Schönthal
Justizangestellte
als Urkundsbeamtin
der Geschäftsstelle

in der Patentnichtigkeitssache

ECLI:DE:BGH:2023:040423UXZR29.21.0

Der X. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 4. April 2023 durch den Vorsitzenden Richter Dr. Bacher, den Richter Hoffmann, die Richterinnen Dr. Marx und Dr. Rombach und den Richter Dr. Crummenerl

für Recht erkannt:

Die Berufung gegen das Urteil des 5. Senats (Nichtigkeitssenats) des Bundespatentgerichts vom 10. März 2021 wird auf Kosten der Beklagten zurückgewiesen.

Von Rechts wegen

Tatbestand:

1 Die Beklagte ist Inhaberin des mit Wirkung für die Bundesrepublik Deutschland erteilten europäischen Patents 1 404 085 (Streitpatents), welches am 29. September 2003 unter Inanspruchnahme der Priorität US-amerikanischer Patentanmeldungen vom 27. September 2002, 18. Oktober 2002 und 4. Dezember 2002 angemeldet wurde und den sicheren Umgang mit Steuerungsinformationen betrifft.

2 Patentanspruch 1, auf den sechs weitere Ansprüche zurückbezogen sind, lautet in der Verfahrenssprache:

> A system for securely handling control information, comprising:
> An integrated circuit (30) comprising a content processing block (170) and a control processing block (130), the content processing block (170) being coupled to the control processing block (130),
> wherein the integrated circuit (30) is operable to receive content and associated control information,
> wherein the control processing block (130) is adapted to validate the authenticity of the control information received by the integrated circuit (30), and
> wherein the content processing block (170) is adapted to process the content received by the integrated circuit (30) to content output sent from the integrated circuit (30) in accordance with the validated control information;
> characterized in that the integrated circuit (30) further comprises a control modifying block (150) adapted to modify the control information received by the integrated circuit (30).

3 Patentanspruch 8, auf den vier weitere Ansprüche zurückbezogen sind, schützt ein Verfahren mit entsprechenden Merkmalen.

4 Die Klägerin hat geltend gemacht, der Gegenstand des Streitpatents gehe über den Inhalt der ursprünglich eingereichten Unterlagen hinaus und sei nicht patentfähig. Die Beklagte hat das Streitpatent mit einem Hauptantrag und sieben Hilfsanträgen in geänderten Fassungen verteidigt.

5 Das Patentgericht hat das Streitpatent für nichtig erklärt. Dagegen wendet sich die Beklagte mit ihrer Berufung. Sie verteidigt das Streitpatent mit ihrem erstinstanzlichen Hauptantrag und den erstinstanzlichen Hilfsanträgen 1 bis 6. Die Klägerin tritt dem Rechtsmittel entgegen.

Entscheidungsgründe:

6 Die zulässige Berufung hat in der Sache keinen Erfolg.

7 I. Das Streitpatent betrifft den sicheren Umgang mit Steuerungsinformationen.

8 1. Nach den Ausführungen in der Streitpatentschrift dienten im Stand der Technik bekannte Steuerungsinformationen dazu, den Zugriff auf analoge oder digitale Inhalte (z.B. Videoinhalte) zu steuern und zu beschränken. Als Beispiele hierfür werden die digitale Rechteverwaltung (Digital Rights Management, DRM) und die Kopierkontrollinformation (Copy Control Information, CCI) genannt (Abs. 2).

9 Um sicherzustellen, dass diese Steuerungsinformationen nicht manipuliert werden, könne ein Verfahren zur Authentifizierung der Verbindung zwischen den Steuerungsinformationen und den Inhalten angewandt werden. Die Verarbeitung der Steuerungsinformationen in der konventionellen reinen Softwareumgebung mache diese jedoch anfälliger für unbefugte Manipulation (Hacken). Bei anderen Systemen sei die gegen unbefugte Eingriffe immune Hardware getrennt von der anwendungsspezifischen integrierten Schaltung (ASIC), welche die Inhaltsinformationen verarbeite. Damit bleibe diese anfällig für unbefugte Manipulation. Zudem ermöglichten die bekannten Systeme keine sichere Modifizierung der Steuerungsinformationen durch eine vertrauenswürdige Partei (Abs. 3 Z. 28-45).

10 2. Vor diesem Hintergrund liegt dem Streitpatent die Aufgabe zugrunde, ein System zur Verfügung zu stellen, das eine Änderung von Steuerungsinformationen entsprechend der tatsächlichen Verwendung der ihnen zugeordneten Inhalte ermöglicht und dennoch vor Manipulationen durch unbefugte Dritte geschützt ist.

11 3. Zur Lösung schlägt das Streitpatent in der mit dem Hauptantrag verteidigten (mit der erteilten Fassung übereinstimmenden) Fassung von Patentanspruch 1 ein System vor, dessen Merkmale sich wie folgt gliedern lassen:

12

| | | |
|---|---|---|
| 1.1 | A system for securely handling control information, comprising: | System zur sicheren Verarbeitung von Steuerungsinformationen, welches aufweist: |
| 1.2 | an integrated circuit (30) operable to receive content and associated control information, and comprising: | eine integrierte Schaltung (30), die betreibbar ist, um Inhalte und zugeordnete Steuerungsinformation zu empfangen und enthält: |
| 1.2a | a control processing block (130), adapted to validate the authenticity of the control information received by the integrated circuit (30), | einen Steuerungsverarbeitungsblock (130), der dazu ausgelegt ist, die Authentizität der von der integrierten Schaltung (30) empfangenen Steuerungsinformationen zu validieren, |
| 1.2b | a content processing block (170) being coupled to the control processing block (130), adapted to process the content received by the integrated circuit (30) to content output sent from the integrated circuit (30) in accordance with the validated control information, | einen Inhaltverarbeitungsblock (170), der mit dem Steuerungsverarbeitungsblock (130) gekoppelt und dazu ausgelegt ist, den von der integrierten Schaltung (30) empfangenen Inhalt gemäß der validierten Steuerungsinformationen zu verarbeiten und auszugeben, |
| 1.2c | a control modifying block (150) adapted to modify the control information received by the integrated circuit (30). | einen Steuerungsmodifizierungsblock (150), der dazu ausgelegt ist, die von der integrierten Schaltung (30) empfangenen Steuerungsinformationen zu modifizieren. |

13 4. Einige Merkmale bedürfen der näheren Erläuterung.

14 a) Steuerungsinformationen (control information) im Sinne des Merkmals 1.1 sind Informationen, die dazu dienen, den Zugriff auf analoge oder digitale Inhalte (z.B. Videoinhalte) zu steuern (Abs. 2 Z. 16-17). Aus ihnen ergeben sich zum Beispiel Nutzungsbeschränkungen für die ihnen zugeordneten Inhalte, etwa die Angabe, wie oft die Inhalte (noch) kopiert werden dürfen.

15 b) Für Empfang, Überprüfung und Verarbeitung der Inhalte und Steuerungsinformationen ist in Merkmal 1.2 eine integrierte Schaltung vorgesehen, die (mindestens) drei Blöcke aufweisen muss.

16 aa) Der in Merkmal 1.2b vorgesehene Block dient der Verarbeitung der Inhalte, also beispielsweise der digitalen Video- oder Audiodateien, nach Maßgabe der Steuerungsinformationen.

17 Integrierte Schaltungen mit dieser Funktion waren nach der Beschreibung des Streitpatents (Abs. 3) im Stand der Technik bekannt. Um die Manipulationssicherheit zu erhöhen, sehen die Merkmale 1.2a und 1.2c vor, dass die Verarbeitung und gegebenenfalls auch die Modifizierung der Steuerdaten ebenfalls durch die integrierte Schaltung erfolgt. Dies führt zu einem verbesserten Schutz, weil alle Aktionen innerhalb einer gesicherten Hardware-Umgebung ausgeführt werden (Abs. 46 Z. 25-33).

18 bb) Der Block für die Verarbeitung der Steuerungsinformationen ist nach Merkmal 1.2a dazu ausgebildet, die Authentizität der von der integrierten Schaltung empfangenen Steuerungsinformationen zu validieren.

19 (1) Zu Recht hat das Patentgericht entschieden, dass es für eine Validierung der Authentizität genügt, wenn die Integrität der Informationen validiert, also überprüft wird, ob die Steuerungsinformationen verändert worden sind. Nicht

zwingend erforderlich ist hingegen eine Prüfung darauf, ob die Informationen von einer bestimmten Quelle stammen.

20 Dass der Begriff der Authentizität nach dem allgemeinen fachlichen Sprachgebrauch im zuletzt genannten Sinne verstanden wird, hat das Patentgericht zu Recht als im Ergebnis nicht ausschlaggebend angesehen. Aus der Beschreibung des Streitpatents ergibt sich, dass dieses den Begriff in anderem Sinne verwendet.

21 Bei der Darstellung des Standes der Technik wird als Authentifizierung die Prüfung der Verbindung zwischen den Steuerungsinformationen und den zugeordneten Inhalten bezeichnet. Diese Prüfung soll sicherstellen, dass die Steuerungsinformationen nicht verändert worden sind (Abs. 3 Z. 28-32). Darin liegt lediglich eine Prüfung auf Integrität, nicht aber auf Authentizität im engeren Sinne.

22 Das Streitpatent kritisiert die im Stand der Technik bekannten Vorgehensweisen allerdings gerade deshalb, weil sie keinen Schutz gegen unbefugte Manipulation oder Hacker-Eingriffe gewährleisten und selbst bei Einsatz von anwendungsspezifischen integrierten Schaltkreisen anfällig gegen Manipulationen durch einen nicht vertrauenswürdigen Beteiligten seien (Abs. 3 Z. 33-43).

23 Bei der Beschreibung eines erfindungsgemäßen Ausführungsbeispiels wird der Einsatz eines Schlüssels zur Verknüpfung mit Quell- und Zielpunkten, der eine solche Überprüfung ermöglichen würde, dennoch nur als Option angeführt, nicht aber als zwingendes Element der Authentifizierung (Abs. 49 Z. 43-46). Dem ist zu entnehmen, dass eine Integritätsprüfung ausreicht.

24 Entgegen der Auffassung der Beklagten führt die Beschreibung nicht nur die Verknüpfung mit Zielpunkten als optional an, so dass eine Verknüpfung mit Quellpunkten zwingend erforderlich wäre. Die Verknüpfung mit Quell- und Zielpunkten wird in diesem Zusammenhang vielmehr als zusammengehöriges Merkmal behandelt, das insgesamt optional ist.

25 (2) Selbst wenn Merkmal 1.2a zusätzlich eine Überprüfung darauf verlangte, ob die Steuerungsinformationen aus einer vertrauenswürdigen Quelle stammen, ergäbe sich daraus nicht, dass die überprüften Informationen zwingend einem bestimmten Individuum zuzuordnen sein müssen, etwa einer bestimmten Person oder einem bestimmten Gerät.

26 Das Streitpatent enthält keine näheren Angaben dazu, unter welchen Voraussetzungen eine Quelle oder ein Ziel als vertrauenswürdig angesehen werden kann.

27 Im Zusammenhang mit der Modifizierung der Steuerungsinformationen werden als Beispiele für Authentifizierungsmittel ein Steuerwort (control word), ein Nachrichten-Authentifizierungscode (message authentication code, MAC), ein Wasserzeichen oder andere mit den Steuerungsinformationen zu verbindende Daten (authentication output) benannt (Abs. 50 Z. 42-47).

28 Steuerworte oder Wasserzeichen sind nicht notwendig einer einzelnen Person zugeordnet. Der Zweck von message authentication codes wurde im Stand der Technik dahin beschrieben, dass sie sowohl die Quelle als auch die Integrität der Nachricht gewährleisten. Parameter dieser MACs sind der Dateninput und ein geheimer Schlüssel (vgl. A. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography, 1997, S. 323). Auch damit ist nicht festgelegt, dass die Quelle zwingend eine individuelle Person oder ein individuelles Gerät sein muss.

29 5. Die mit dem Hauptantrag verteidigte Fassung von Patentanspruch 8 unterscheidet sich von der erteilten Fassung dadurch, dass nunmehr ausdrücklich vorgesehen ist, dass die Validierung die Authentizität der Steuerungsinformationen betrifft.

30 Damit entsprechen alle Merkmale von Patentanspruch 8 denjenigen von Patentanspruch 1. Beide Ansprüche unterliegen deshalb derselben Beurteilung.

31 II. Das Patentgericht hat seine Entscheidung, soweit für das Berufungsverfahren von Interesse, im Wesentlichen wie folgt begründet:

32 Die internationale Anmeldung WO 02/056535 (D1) nehme sämtliche Merkmale des Patentanspruchs 1 vorweg. Merkmal 1.2a sei auch dann offenbart, wenn man ein engeres Verständnis des Begriffs der Authentifizierung zugrunde lege. Der in D1 offenbarte enabling key block (EKB) stelle eine der Voraussetzungen für das Abspielen der Daten beim Benutzer dar. Er werde von einem externen reliable key distribution center (KDC) für ein valid user device zur Verfügung gestellt und enthalte damit die Angabe eines vertrauenswürdigen Verteilers als Quelle.

33 Das nach Hilfsantrag 1 zusätzlich vorgesehene Merkmal, dass die Steuerungsinformationen in frames durch eine Eingabeverbindung von einem zentralen Inhalteanbieter empfangen werden, sei entgegen der Auffassung der Beklagten nicht dahin auszulegen, dass eine direkte internetbasierte Verbindung zu einem Medienserver erforderlich sei. Mit diesem Verständnis sei das Merkmal in D1 offenbart. Lege man das Verständnis der Beklagten zugrunde, werde es durch D1 nahegelegt. Das weitere Merkmal, wonach eine Eingangsschnittstelle für einen IC und ein Anschluss an bzw. für einzulesende Daten vorhanden sein müssen, sei in D1 offenbart.

34 Das in Hilfsantrag 2 zusätzlich vorgesehene Merkmal eines Authentisierungsblocks im IC sei insbesondere aus Figur 18 der D1 bekannt. Das nach Hilfsantrag 3 vorgesehene Merkmal, wonach ein Schlüssel die Steuerungsdaten mit Quell- und Zielpunkten verknüpfe, sei ebenfalls in D1 offenbart. Entsprechendes gelte für die zusätzlichen Merkmale nach den Hilfsanträgen 4 bis 6.

35 III. Diese Beurteilung hält der Überprüfung im Berufungsrechtszug stand.

36 1. Der mit dem Hauptantrag verteidigte Gegenstand von Patentanspruch 1 wird durch D1 vollständig vorweggenommen.

37 a) D1 betrifft unter anderem die Verarbeitung von Inhaltsdaten, die mit einer Nutzungsbeschränkung versehen sind (D1' S. 1 Abs. 2 Mitte).

38 aa) Nach den Ausführungen in D1 war zum Schutz der Rechte des Urhebers vor unerlaubten Kopien das Serial Copy Management System (SCM) bekannt (D1' S. 2/3). Dabei werde mittels eines aufgezeichneten Codes auf dem Medium angezeigt, ob eine Kopie möglich sei oder nicht. Dieser Code könne jedoch manipuliert werden (D1' S. 4, Abs. 1).

39 Es gebe darüber hinaus verschiedene Verschlüsselungstechniken (D1' S. 4-8). Auch bei diesen bestehe das Problem, dass die Informationen auf einem Medium wie CD und DVD, die die Kopierregel enthielten, durch einen unredlichen Benutzer manipuliert werden könnten (D1' S. 8 Abs. 3).

40 Vor diesem Hintergrund macht es sich die D1 zur Aufgabe, Vorrichtungen und Verfahren zum Aufzeichnen oder Wiedergeben von Informationen bereitzustellen, die eine unberechtigte Datennutzung ausschließen (D1' S. 9 Abs. 1).

41 Hierzu schlägt D1 vor, den Inhalt eines Aufzeichnungsträgers oder Mediums (z.B. DVD, CD) durch Verschlüsselung zu schützen. Der Schlüssel zum Aufheben der Verschlüsselung werde durch ein sicheres Verfahren zusammen mit dem Inhalt auf das Medium aufgezeichnet. Gleichzeitig erfolge die Aufzeichnung der Kennung (ID) dieses Inhalts und der Rechtedaten (Rights Data), die Regeln für die Art und Weise der Verwendung dieses Inhalts angäben. Die Aufzeichnung erfolge in einer Form, deren Legitimität durch einen Integritätsprüfwert (ICV) garantiert sei. In den Rechtedaten seien zum Beispiel die Anzahl der erlaubten Wiedergaben oder Kopien aufgezeichnet. Der Integritätsprüfwert ICV und die Schlüsseldaten für die Erzeugung des ICV seien physisch geschützt aufgezeichnet. Geheime Daten wie der ICV und die Schlüsseldaten für dessen Erzeugung könnten

nur mittels eines speziellen Verfahrens aufgezeichnet und wiedergegeben werden. Hierzu könne ein integrierter Schaltkreis eingesetzt werden, der nur in einer legitimen Vorrichtung eingerichtet und dem Benutzer zur Verfügung gestellt werde (D1' S. 55-57).

42 bb) Der Integritätsprüfwert ICV werde zum Beispiel für den Inhalt und die Kopierkontrollinformationen erzeugt und ermögliche eine Prüfung von deren Integrität.

43 Zur Erzeugung eines solchen Werts könne eine Nachricht in Blöcke von je 8 Bit aufgeteilt werden, die nacheinander einer exklusiv-oder-Verknüpfung und einer Verschlüsselung unterzogen werden. Zur Überprüfung würden die vorliegenden Daten in gleicher Weise verarbeitet und ein Prüfwert ICV' erzeugt. Wenn dieser mit dem ICV übereinstimme, sei gewährleistet, dass der ICV nicht manipuliert worden sei. Damit stehe zugleich fest, dass die DRM-Daten nicht manipuliert seien (D1' S. 58 f.).

44 cc) Jede Vorrichtung, die eine Verarbeitung des Inhalts vornehme, wie etwa eine Aufzeichnungs-Wiedergabevorrichtung, enthalte einen Schlüssel, der mit Hilfe einer Baumstruktur verteilt werde. Diese Baumstruktur zeige die nachfolgend wiedergegebene Figur 4 (D1' S. 60).

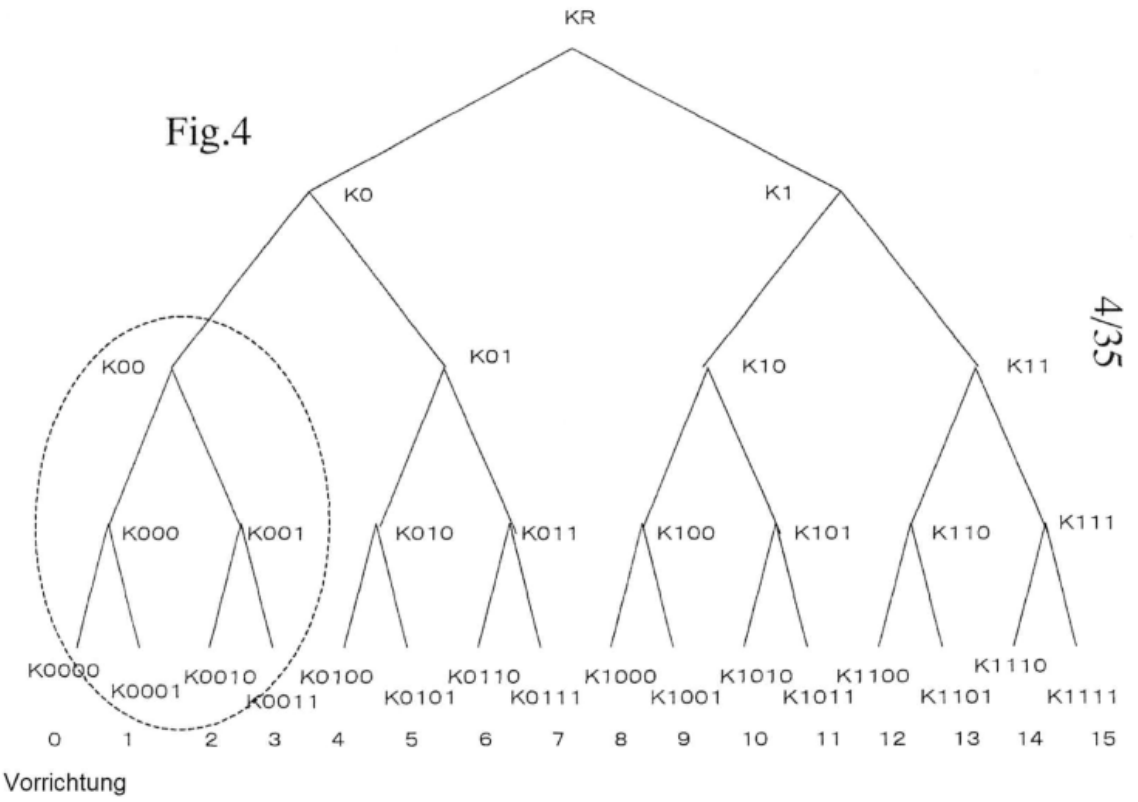


Fig.4

4/35

45 Dies ermögliche die Einteilung in Gruppen, wie sie beispielhaft durch die gestrichelte Linie in Figur 4 dargestellt seien. An Vorrichtungen einer solchen Gruppe könne beispielsweise ein gemeinsamer verschlüsselter Inhalt gesendet werden (D1' S. 62 Abs. 3). Der Datenaustausch mit den Vorrichtungen könne beispielsweise durch einen Inhaltsprovider erfolgen (D1' S. 63).

46 Die Knotenschlüssel und die Blattschlüssel könnten durch ein Zentrum verwaltet werden. Im Falle eines kompromittierten (gehackten) Schlüssels werde eine Modifizierung des Schlüssels beispielsweise durch das Schlüsselverwaltungszentrum oder den Provider vorgenommen (D1' S. 64 Abs. 1). Werde zum Beispiel entdeckt, dass die der Vorrichtung 3 zugeordneten Schlüssel K0011, K001, K00, K0, KR durch einen Hacker aufgedeckt worden seien, sei es nötig, die Vorrichtung 3 vom System zu trennen, die Knotenschlüssel K001, K00, K0 und KR zu neuen Schlüsseln K(t)001, K(t)00, K(t)0, K(t)R zu aktualisieren und den Vorrichtungen 0, 1, 2 diese neuen Schlüssel zu übermitteln (D1' S. 65 Abs. 2).

47 Die Verteilung der aktualisierten Schlüssel könne über ein Netzwerk oder ein Aufzeichnungsmedium erfolgen. Übermittelt werde ein Aktivierungsschlüsselblock (enabling key block, EKB). Die darin enthaltenen aktualisierten Schlüssel könnten mit dem der Vorrichtung bekannten Blattschlüssel entschlüsselt werden (D1' S. 66-68). Damit sei gewährleistet, dass die Schlüssel nur Vorrichtungen zur Verfügung stünden, die über legitime Rechte verfügten (D1' S. 75).

48 dd) Ein Medium zur Verteilung von Inhalten sei in einen Benutzerbereich und einen geschützten Bereich unterteilt. Im Benutzerbereich würden ein EKB, der verschlüsselte Inhalt und DRM-Daten abgelegt. Im geschützten Bereich seien ein ICV-Schlüssel und ein ICV gespeichert (D1' S. 80 f.).

49 ee) Die Erzeugung solcher Daten könne durch eine Authoring-Vorrichtung erfolgen (D1' S. 81), mit der zum Beispiel ein zur Herstellung von CDs oder DVDs einsetzbares Original erzeugt werden könne (D1' S. 83), oder durch eine zum Aufzeichnen von Inhalten geeignete Benutzervorrichtung (D1' S. 91).

50 Eine Authoring-Vorrichtung beziehe einen EKB von einem verlässlichen Verwaltungszentrum (key distribution center, KDC, D1' S. 83 f.) und speichere diesen auf dem Medium ab (D1' S. 85).

51 Eine Benutzervorrichtung verwende gegebenenfalls den zu den aufgezeichneten Inhalten gehörenden EKB, anderenfalls einen in der Vorrichtung selbst gespeicherten EKB für eigene Aufzeichnungen (D1' S. 92).

52 ff) Bei der Wiedergabe von Inhalt könne eine Aktualisierung von DRM-Daten erforderlich werden, etwa wenn nur eine beschränkte Anzahl von Wiedergaben oder Kopien zugelassen sei. Dann müsse auch der ICV aktualisiert werden (D1' S. 107 Abs. 2). Durch Verschlüsselung eines Zufallswerts mit dem EKB-Schlüssel entstehe ein neuer Schlüssel zur Erzeugung und Prüfung des ICV. Mit diesem Schlüssel werde anhand der neuen DRM-Daten in der oben beschriebenen Weise der neue ICV erzeugt (D1' S. 112 f.).

53 b) Damit sind, wovon zutreffend auch das Patentgericht ausgegangen ist, die Merkmale 1.1, 1.2, 1.2b und 1.2c offenbart.

54 c) Vorweggenommen ist auch das Merkmal 1.2a.

55 aa) Insoweit genügt, dass bei dem in D1 offenbarten System durch Vergleich des berechneten ICV' mit dem ICV aus dem geschützten Bereich des Mediums eine Integritätsprüfung durchgeführt wird.

56 bb) Eine Überprüfung auf die Herkunft aus einer sicheren Quelle ist, wie oben dargelegt wurde, nach Merkmal 1.2a nicht erforderlich. Unabhängig davon erfüllt der in D1 offenbarte Vergleich von ICV' und ICV auch diese Funktion.

57 Die Verwendung des EKB für die Berechnung des Vergleichswerts ICV' stellt sicher, dass die empfangenen DRM-Daten von einer befugten Stelle erstellt worden sind. Damit ist die Herkunft aus einer sicheren Quelle gewährleistet.

58 Wie die Berufung im Ansatz zutreffend geltend macht, kann bei dieser Vorgehensweise zwar nicht beurteilt werden, von welcher befugten Stelle die überprüften Daten stammen. Wie bereits oben dargelegt wurde, ist dies zur Verwirklichung von Merkmal 1.2b aber auch dann nicht erforderlich, wenn dieses Merkmal eine Überprüfung der sicheren Herkunft zwingend vorsähe.

59 Dass die Lehre in D1 in dem Fall eines kompromittierten (gehackten) Schlüssels zu dem Ergebnis führt, dass nur Datenträger mit aktualisierter EKB wiedergegeben werden können und damit auch Datenträger ungesperrter Vorrichtungen derselben Gruppe mit noch nicht aktualisiertem EKB von der Wiedergabe ausgeschlossen sind, ist entgegen der von der Beklagten in der mündlichen Verhandlung vor dem Senat geäußerten Auffassung ohne Belang.

60 Das Streitpatent enthält keine näheren Angaben dazu, unter welchen Voraussetzungen eine Quelle als vertrauenswürdig angesehen werden kann. Da im Streitpatent nicht festgelegt ist, dass die Quelle zwingend eine individuelle Per-

son oder ein Gerät ist, kann auch nach dem Streitpatent eine Gruppe von Geräten insgesamt als nicht vertrauenswürdige Quelle eingestuft werden, und zwar unabhängig davon, ob sämtliche Geräte gehackt worden sind.

61 2. Im Ergebnis ohne Erfolg wendet sich die Berufung gegen die Auffassung des Patentgerichts, der Gegenstand des Hilfsantrags 1 sei nicht patentfähig.

62 a) Nach Hilfsantrag 1 soll Patentanspruch 1 folgende zusätzlichen bzw. modifizierten Merkmale enthalten:

63

| | | |
|---|---|---|
| 1.2' | an integrated circuit (30) operable to receive content and associated control information, included in frames carried through the input connection (100) from a central content provider, | eine integrierte Schaltung (30), die betreibbar ist, um Inhalte und zugeordnete Steuerungsinformation zu empfangen, die in Rahmen enthalten sind, die von einem zentralen Inhalteanbieter an die Eingangsverbindung (100) übermittelt werden, |
| 1.3 | an input interface (50) coupled to the integrated circuit and adapted to be coupled to an input connection. | eine Eingangsschnittstelle (50), die mit der integrierten Schaltung gekoppelt und dazu eingerichtet ist, mit dem Eingang verbunden zu werden. |

64 b) Zu Recht wendet sich die Berufung nicht gegen die Auffassung des Patentgerichts, dass Merkmal 1.3 durch D1 offenbart ist.

65 Figur 1 der D1 zeigt ein Blockdiagramm des Aufbaus einer Aufzeichnungs- und Wiedergabevorrichtung, die Inhalte wie Musikdaten, Bilddaten oder dergleichen verwendet (D1' S. 52 Abs.3). Diese weist unter anderem eine Medienschnittstelle (190) als Schnittstelle für ein Aufzeichnungsmedium oder einen Auf-

zeichnungsträger (MEDIA) auf. Diese ist mit dem Verschlüsselungsverarbeitungsmittel (150) verbunden, bei dem es sich nach den vorstehenden Ausführungen um eine integrierte Schaltung handelt (D1' S. 52/53).

66 c) Merkmal 1.2' ist ausgehend von D1 jedenfalls nahegelegt.

67 Dabei kann dahingestellt bleiben, ob sich aus der Anforderung, dass die Rahmen von einem zentralen Diensteanbieter übermittelt werden, ergibt, dass die Übertragung über ein Netzwerk wie etwa das Internet erfolgen muss. Eine solche Ausgestaltung beruht jedenfalls nicht auf erfinderischer Tätigkeit.

68 aa) Wie das Patentgericht zutreffend ausgeführt hat, lag es angesichts der in D1 geschilderten und aus dem Stand der Technik bekannten Übertragung von verschlüsselten Inhalten im Internet (D1' S. 4 Abs. 3) nahe, Inhalts- und Steuerungsinformationen auch über das Internet zu übertragen.

69 bb) Ohne Erfolg macht die Beklagte geltend, D1 setze zwingend voraus, dass ein Datenträger mit einem besonders geschützten Bereich verwendet werde, in dem ICV und ICV-Schlüssel gespeichert werden könnten, und lehre deshalb von einer internetbasierten Kommunikation weg.

70 Das Speichern des für die Prüfung auf Integrität und vertrauenswürdige Herkunft herangezogenen EKB in einem geschützten Bereich ist zwar eines der zentralen Lösungselemente in D1 für die Wiedergabe von Inhalten, die auf einem Datenträger gespeichert sind. D1 lehrt jedoch auch, dass sensible Daten wie der Aktivierungsschlüsselblock (EKB), der Inhaltsschlüssel und der verschlüsselte Inhalt sicher über ein Netzwerk verteilt werden können (D1' S. 76). Grund hierfür ist, dass eine Entschlüsselung und Verwendung des Inhalts nur für Vorrichtungen, die über legitime Rechte verfügen, möglich ist (D1' S. 75/76).

71 Hieraus ergab sich ein konkreter Hinweis, wie das in D1 offenbarte Verfahren auch für die gesicherte Wiedergabe von Inhalten aus dem Internet eingesetzt werden kann - nämlich dadurch, dass die bei Einsatz von Datenträgern in

einem geschützten Bereich abgelegten Daten bei Übertragung über ein Netzwerk in derselben Weise geschützt werden, die D1 für die Übertragung anderer sensibler Daten vorschlägt.

72 Dass dies möglicherweise einen geringeren Grad an Sicherheit bietet, ist schon deshalb unerheblich, weil das Streitpatent keinen bestimmten Mindestgrad an Sicherheit vorschreibt und nicht einmal für die Wiedergabe von Datenträgern ein Schutzniveau aufzeigt, wie es D1 beschreibt.

73 3. Das Patentgericht hat zutreffend auch den Gegenstand des Hilfsantrags 2 als nicht patentfähig angesehen.

74 a) Nach Hilfsantrag 2 soll Patentanspruch 1 in der Fassung des Hilfsantrags 1 folgendes zusätzliche Merkmal enthalten:

75

| | | |
|---|---|---|
| 1.2d | an authentication application block (160) adapted to authenticate the modified control information. | einen Authentifizierungsanwendungsblock (160), der dazu eingerichtet ist, die geänderte Steuerungsinformation zu authentifizieren |

76 b) Der Begriff "Authentifizierung" ist in diesem Zusammenhang nicht anders auszulegen als im Zusammenhang von Merkmal 1.2a.

77 c) Wie das Patentgericht zutreffend angenommen hat, zeigt das in Figur 18 der D1 gezeigte Verschlüsselungsverarbeitungsmittel (810) einen Authentifizierungsanwendungsblock im Sinne dieses Merkmals.

78 Dass die Abspielgeräte bei dem in D1 offenbarten System nur ICV und DRM-Daten modifizieren, nicht aber den EKB, führt entgegen der Auffassung der Berufung nicht zu einer abweichenden Beurteilung. Dieser Unterschied wäre allenfalls dann relevant, wenn eine Authentifizierung zwingend dazu geeignet sein müsste, die Herkunft von einem bestimmten Individuum zu gewährleisten. Letzteres trifft aus den oben zu Merkmal 1.2a dargelegten Gründen nicht zu.

79 4. Keine andere Beurteilung ergibt sich hinsichtlich des mit Hilfsantrag 3 verteidigten Gegenstands.

80 a) Nach Hilfsantrag 3 soll die erteilte Fassung von Patentanspruch 1 um folgendes Merkmal ergänzt werden:

81

| | | |
|---|---|---|
| 1.2a.0 | the control information includes a key that links the control information to source and destination points | die Steuerungsinformationen enthalten einen Schlüssel, der sie mit Quell- und Zielpunkten verknüpft |

82 b) Auch aus diesem Merkmal ergibt sich nicht, dass die verknüpfte Quelle zwingend ein bestimmtes Individuum sein muss. Vielmehr genügt es, wenn eine Verknüpfung zu einer nach fachlich geeigneten Kriterien als vertrauenswürdig eingestuften Quelle möglich ist.

83 Der Schlüssel muss darüber hinaus eine Verknüpfung der Steuerungsdaten mit einem Zielpunkt vornehmen. Wie das Patentgericht zutreffend angenommen hat, bedeutet dies, dass der Schlüssel angibt, ob Daten an einem Ziel entschlüsselt werden können oder nicht.

84 c) Ein solcher Schlüssel ist, wie das Patentgericht zutreffend dargelegt hat, in D1 in Gestalt des ICV und des EKB offenbart.

85 5. Die Berufung hat auch keinen Erfolg, soweit das Berufungsgericht den Gegenstand des Hilfsantrags 4 als nicht patentfähig angesehen hat.

86 a) Nach Hilfsantrag 4 soll die erteilte Fassung von Patentanspruch 1 wie folgt ergänzt werden:

87

| | | |
|---|---|---|
| 1.2a.1 | wherein validating the authenticity includes | Die Validierung der Authentizität umfasst: |
| 1.2a.1a | authenticating a link between the control information and the associated content to verify that the control information has not been modified | die Authentifizierung einer Verbindung zwischen den Steuerungsinformationen und dem zugehörigen Inhalt, um zu bestätigen, dass die Steuerungsinformationen nicht verändert wurden, |
| 1.2a.1b | and a key that links the control information to the authentication of the source and destination points | einen Schlüssel, der die Steuerungsinformationen zur Authentifizierung von Quell- und Zielpunkten verknüpft, |
| 1.2a.1c | as well as the means to unlock access to the corresponding content, | die Mittel, um den Zugriff auf den zugeordneten Inhalt freizugeben. |

88 b) Merkmal 1.2a.1a erfordert eine Integritätsprüfung, die wie oben ausgeführt in D1 offenbart ist.

89 c) Merkmal 1.2a.1b enthält trotz der in Einzelheiten abweichenden Formulierung keine weitergehenden Vorgaben als das nach Hilfsantrag 3 vorgesehene Merkmal 1.2a.0, welches aus den oben dargelegten Gründen durch D1 vorweggenommen wird.

90 d) Merkmal 1.2a.1c ist erfüllt, wenn der Schlüssel dazu dient, die Mittel, die den Zugriff auf den zugeordneten Inhalt freigeben, zu aktivieren.

91 Letzteres ist in Figur 18 von D1 ebenfalls bereits gezeigt. Dort wird im Schritt S510 der verschlüsselte Inhaltsschlüssel aus den DRM-Daten erlangt und in einer Einheit (824) unter Verwendung des in Schritt S503 erlangten EKB-Schlüssels verarbeitet. Im darauffolgenden Schritt S511 wird der verschlüsselte Inhalt in einer Einheit (825) für die Wiedergabe entschlüsselt (D1' S. 114 Abs. 1).

92 6. Die Verteidigung mit Hilfsantrag 5 bleibt ebenfalls ohne Erfolg.

93 a) Nach Hilfsantrag 5 soll die erteilte Fassung von Patentanspruch 1 wie folgt ergänzt werden:

94

| | | |
|---|---|---|
| 1.2a.2 | wherein the control data is validated according to an authentication algorithm in the control processing block | die Steuerungsinformationen können durch einen Authentifizierungsalgorithmus im Steuerungsverarbeitungsblock validiert werden |
| 1.2a.3 | wherein the authentication also includes a key that links it to the authentication of the source and destination points | Die Authentifizierung umfasst einen Schlüssel, der sie mit der Authentifizierung von Quell- und Zielpunkten verknüpft |

95 b) Merkmal 1.2a.3 entspricht sinngemäß dem Merkmal 1.2a.0 gemäß Hilfsantrag 3, welches aus den oben genannten Gründen vorweggenommen ist.

96 Wie das Patentgericht zutreffend ausgeführt hat, ist mit dem Austausch von "control information" durch "authentication" in der Sache keine Änderung verbunden.

97 c) Ein Authentifizierungsalgorithmus im Sinne von Merkmal 1.2a.2 ist eine Regel zur Authentifizierung.

98 Der zuletzt genannte Begriff ist auch in diesem Zusammenhang nicht anders auszulegen als im Zusammenhang mit Merkmal 1.2a.

99 d) Ein solcher Authentifizierungsalgorithmus ist in D1 aus den oben dargelegten Gründen offenbart.

100 7. Für Hilfsantrag 6 gilt nichts anderes.

101 a) Nach Hilfsantrag 6 soll Patentanspruch in der Fassung von Hilfsantrag 5 um das Merkmal 1.2a.1c aus Hilfsantrag 4 ergänzt werden.

102 b) Auch in dieser Kombination sind die genannten Merkmale aus den bereits oben dargelegten Gründen in D1 offenbart.

103 IV. Die Kostenentscheidung beruht auf § 121 Abs. 2 Satz 2 PatG sowie § 97 Abs. 1 ZPO.

Bacher Hoffmann Marx

Rombach Crummenerl

Vorinstanz:
Bundespatentgericht, Entscheidung vom 10.03.2021 - 5 Ni 28/18 (EP) -