Unified Patent Court
Einheitliches Patentgericht
Juridiction unifiée du brevet

Ortsverband Paris

UPC_CFI_530/2025 & UPC-CFI-0002281/2025 & UPC-CFI-0002285/2025 & UPC-CFI-0000003/2026 & UPC-CFI-0002274/2025

Entscheidung in der Sache des Gerichts erster Instanz des Einheitlichen Patentgerichts, erlassen am 17.11.2026

Kopfzeile:

Der Patentinhaber hat die Möglichkeit, die Beschreibung so zu ändern, dass sie mit dem geänderten Anspruch übereinstimmt (vgl. Regel 30.1 (a) der Verfahrensordnung). Es ist jedoch nicht möglich, die Beschreibung so zu ändern, dass sich die Bedeutung des Patents und seines Anspruchs 1 ändert. Es ist zwar möglich, den Schutzumfang des Patents einzuschränken, jedoch nicht, dem Patent durch eine derart umfassende Änderung der Beschreibung eine neue Bedeutung zu verleihen. Dies wäre im Übrigen mit dem Grundsatz der Rechtssicherheit für Dritte unvereinbar.

Stichwörter:

R. 30.1 (a) RdP. Änderung des Patents. Grundsatz der Rechtssicherheit für Dritte

ANMELDER

KEEEX SAS
5 rue de Lissandre
13013 – MARSEILLE – FR

Vertreten durch Thibaud LELONG sowie weitere Vertreter der Kanzlei FIDAL, der Kanzlei FIDAL INNOVATION sowie der Kanzlei GERMAIN MAUREAU

BEKLAGTE

1) **ADOBE SYSTEMS SOFTWARE IRELAND LIMITED**
4–6 Riverwalk, Citywest Business Campus, Saggart
D24DCWO – Dublin 24 – IE

2) **ADOBE INC**
345 Park Avenue
CA 95110-2704 – San Jose – US

Vertreten durch Thomas CUCHE und weitere Vertreter der Kanzlei

DTMV, der Kanzlei POWELL GILBERT und der Kanzlei PAUSTIAN & PARTNER

3) OPEN AI OPCO LLC
1455 3rd Street
CA 94158 – San Francisco – USA

4) OPEN AI IRELAND LTD
117–126 Sheriff Street Upper, The Liffey Trust Centre, 1. Stock
D01 YC43 – Dublin 1 – IE

Vertreten durch David POR und weitere Vertreter der Kanzlei CLIFFORD CHANCE

5) TRUEPIC INC.
402 W. Broadway, Suite 400/PMB#5021
CA 92101 – San Diego – US

Vertreten durch Benjamin MAY und weitere Vertreter der Kanzlei JEANTET

6) JOINT DEVELOPMENT FOUNDATION PROJECTS LLC
548 Market Street, Postfach 57724
CA 94101-5401 – San Francisco – USA

7) COALITION FOR CONTENT PROVENANCE AND AUTHENTICITY (C2PA)
3500 South Dupont Highway, Suite AA101,
DE 19901 – Dover – USA

Vertreten durch Philipp Cepl und weitere Vertreter der Kanzlei Herbert Smith Freehills Kramer Paris LLP

STREITIGES PATENT

Patentnummer	*Patentinhaber*
EP2949070	KEEEX SAS

ZUSAMMENSETZUNG DER KAMMER – PLENARSITZUNG:

Vorsitzende und Berichterstatterin	**Camille Lignieres**
Juristisch qualifizierte Richterin	**Carine Gillet**
Juristisch qualifizierte Richterin	**Peter Tochtermann Alessandro**
Technisch qualifizierte Richterin	**Sanchini**

VERFAHRENSSPRACHE: Französisch

ENTSCHEIDUNG

Beteiligte Parteien

1. Die Gesellschaft KEEEX SAS ist eine französische Gesellschaft, die 2014 von Laurent HENOCQUE, dem Erfinder des im vorliegenden Rechtsstreit streitgegenständlichen Patents, gegründet wurde. Der Sitz von KEEEX befindet sich in Marseille. Diese Gesellschaft hat den Status eines KMU (Kleines und Mittelständisches Unternehmen) und hat die Entwicklung von Softwareprogrammen und IT-Lösungen zum Gegenstand. Die Gesellschaft KEEEX ist auf Lösungen für digitale Vertrauens- und Sicherheitssysteme spezialisiert.
   KEEEX ist seit der endgültigen Übertragung zu seinen Gunsten am 26. März 2025 (Anlage KEEEX A4) Inhaber des europäischen Patents EP 2 949 070 B1 (im Folgenden „EP 070“), nachdem es seit 2014 dessen exklusiver Lizenznehmer war (Klagebegründung, Seite 12). Das Gericht stellt fest, dass die Anfechtung der Inhaberschaft des Patents und damit der Zulässigkeit der Patentverletzungsklage von KEEEX in dieser Verfahrensphase von ADOBE nicht mehr aufrechterhalten wird.

2. Die Unternehmen ADOBE (Beklagte 1 und 2):

   Die Beklagte 1) ist eine Gesellschaft nach US-amerikanischem Recht, die Muttergesellschaft der vor über 40 Jahren gegründeten ADOBE-Gruppe mit Sitz in Kalifornien, die auf Software und andere digitale Tools spezialisiert ist. ADOBE hat insbesondere das generative KI-Tool „ADOBE Firefly“ entwickelt.

   Die Beklagte 2) ist eine Gesellschaft nach irischem Recht, die zur ADOBE-Gruppe gehört (Klageerwiderung von ADOBE, Seite 16).

3. Die Beklagten 3 bis 4 OpenAI: (Klageerwiderung von OpenAI, Seite 14)

   Einleitend ist anzumerken, dass die Klage gegen die Gesellschaft OpenAI LP durch Beschluss vom 19.12.2025 zurückgenommen wurde.

   Die Beklagten 3 und 4 sind Gesellschaften nach US-amerikanischem Recht, die zur 2015 gegründeten OpenAI-Gruppe gehören, die sich auf die Forschung und Entwicklung von Technologien der künstlichen Intelligenz („KI“) spezialisiert hat. Die Haupttätigkeit der OpenAI-Gruppe besteht in der Entwicklung, dem Training und dem Einsatz fortschrittlicher KI-Modelle, wie beispielsweise des Modells „ChatGPT“.

4. Das 2016 gegründete Unternehmen TRUEPIC (Beklagte 5) präsentiert sich als amerikanisches Technologie-KMU, das auf die Überprüfung und

Authentifizierung digitaler Bilder und Videos spezialisiert hat. Ihr Hauptsitz befindet sich in San Diego, Kalifornien. (Klageerwiderung von TRUEPIC, Seite 9)

5. Die Beklagten 6 und 7:

   Joint Development Foundation Projects LLC (Beklagte 6) ist eine spezielle Gesellschaft mit beschränkter Haftung (vom Typ „Series“ LLC) mit Sitz in San Francisco (Kalifornien). Die Beklagte 6 wurde in erster Linie gegründet, um die Gründung sogenannter „Serien“-Einheiten zu ermöglichen, mit dem Ziel, die Festlegung von Normen und technischen Spezifikationen zu erleichtern und so die Entwicklung von Aktivitäten durch Dritte zu fördern.

   Ihr einziges Mitglied ist die C2PA (Beklagte 7), eine gemeinnützige Gesellschaft mit Sitz im Bundesstaat Delaware.

6. Es ist unstreitig, dass ADOBE, OpenAI und TRUEPIC an der Entwicklung der sogenannten „C2PA“-Technologie beteiligt sind. Diese Technologie wird von KEEEX als „ein Mittel zur Entwicklung eines offenen Standards zur Zertifizierung der Echtheit und Herkunft digitaler Inhalte (Bilder, Videos, Dokumente)“ beschrieben. (Zusammenfassung der Klagegründe von KEEEX, Seite 3)

TATSACHEN UND VERFAHREN

7. KEEEX hat am 17. Juni 2025 vor der Pariser Zweigstelle der Einheitlichen Patentgerichtsbarkeit (im Folgenden „JUB“) eine Klage wegen Verletzung des Patents EP 2 949 070 B1 (sogenanntes „EP 070“) gegen die Unternehmen ADOBE, OpenAI, TRUEPIC, JOINT DVT und C2PA.

8. Im Rahmen eines Einwands in der Vorverhandlung haben die Beklagten die Zuständigkeit des Gerichts hinsichtlich der nationalen Teile des streitigen Patents, die außerhalb des Hoheitsgebiets der Vertragsstaaten der AJUB liegen, bestritten, was zu einem Beschluss des Luxemburger Berufungsgerichts vom 13.03.2026 führte, in dem entschieden wurde, dass „das Gericht nicht zuständig ist, über die behauptete Verletzung der schweizerischen, spanischen, britischen, irischen, norwegischen und polnischen Teile des Patents EP 2 949 070 zu entscheiden“. Daraus folgt, dass das Gericht im Rahmen dieses Rechtsstreits mit den von KEEEX geltend gemachten Verletzungshandlungen befasst ist, die sich auf die nationalen Teile des Patents ausschließlich in den im Patent benannten und in diesen Gebieten geltenden AJUB-Mitgliedstaaten beziehen.

9. Die Klagebeantwortungen mit Widerklagen auf Nichtigkeit des Patents wurden am 30. und 31. Dezember 2025 eingereicht.
   Am 5. März 2026 hat der Kläger auf die Klagebeantwortungen erwidert und eine bedingte Änderung des Patents mit 11 Hilfsanträgen beantragt. KEEEX hat seinen letzten Schriftsatz am 5. Juni 2026 eingereicht, die Beklagten am 6. Juli 2026.
   Das schriftliche Verfahren wurde am 27. August 2026 abgeschlossen, und das Vorverfahrensverfahren wurde am 22. September dieses Jahres beendet.

10. Der Berichterstatter wurde in dieser Sache mit zahlreichen Verfahrensanträgen befasst und erließ Beschlüsse, gegen die ihrerseits zahlreiche Anträge auf Überprüfung und/oder Berufung eingereicht wurden.
Es wurden mehrere Online-Bereitstellungssitzungen organisiert, um sich mit den Vertretern der Parteien über die Vorbereitung dieses Verfahrens und die Organisation der mündlichen Verhandlung abzustimmen.

11. Die Verfahrensentscheidungen, abgesehen von der Entscheidung über die Zuständigkeit im Rahmen der Einrede der Unzuständigkeit, die sich auf den Umfang des dem Gremium vorgelegten Rechtsstreits im Stadium der noch zu erlassenden Endentscheidung auswirken, sind folgende:

- der Verzicht von KEEEX auf ihren ursprünglichen Antrag, bereits im Rahmen der Entscheidung in der Hauptsache über die Festsetzung des Schadenersatzes zu entscheiden, zugunsten einer Entscheidung zu diesem Punkt im Rahmen eines gesonderten Verfahrens;

- die Zulässigkeit des Antrags von KEEEX auf Zahlung eines Vorschusses auf Schadensersatz in Höhe von 100 Millionen (materieller Schaden) und 20 Millionen Euro (immaterieller Schaden);

- bestimmte Teile des von KEEEX am 5. Juni 2026 eingereichten Schriftsatzes wurden als verspätet aus dem Verfahren ausgeschlossen; und der Antrag von KEEEX auf eine nachträgliche Änderung ihres Patents gemäß R. 30.2 RdP wurde vom Berichterstatter nicht genehmigt (vgl. Beschluss vom 25. Juni 2026 und dessen Bestätigung durch das Gremium am 29. Juli 2026);

- Eine Sicherheitsleistung für die Prozesskosten (Reg. 158 RdP) in Höhe von insgesamt 200.000 Euro wurde vom Kläger auf Antrag der Beklagten geleistet (endgültiger Beschluss vom 19. Dezember 2025), anschließend wurde auf Antrag von ADOBE am 11. September 2026 eine zusätzliche Sicherheit in Höhe von 100.000 Euro geleistet (Beschluss vom 20. Juli 2026, bestätigt durch das Gremium am 27. August 2026).

12. Schließlich sei noch hinzugefügt, dass ADOBE am 17. Juli 2026 zur Information des Gerichts im CMS das vorläufige Gutachten des Bundespatentgerichts zur Gültigkeit des deutschen Teils des Patents EP 070 eingereicht hat. Dieses Schriftstück wurde vom Berichterstatter in die Akte aufgenommen, der die Parteien aufforderte, ihre schriftlichen Stellungnahmen zu diesem neuen Schriftstück in der Akte einzureichen. Diese vorläufige Stellungnahme betrifft eine Nichtigkeitsklage gegen den deutschen Teil des geltend gemachten Patents, die am 10. Dezember 2025 von der Firma ADOBE Systems GmbH, die nicht Partei des vorliegenden Verfahrens ist, beim Bundespatentgericht in Deutschland eingereicht wurde.

ANTRÄGE DER PARTEIEN

13. **KEEEX, der Kläger im Hauptverfahren, beantragt im Wesentlichen:**

Zur Verletzungsklage:

festzustellen, dass die Beklagten eine direkte (Artikel 25 AJUB) und eine indirekte (Artikel 26 AJUB) Verletzung des Anspruchs 1 des Patents EP 070 begangen haben,

indem sie:

- technische Spezifikationen C2PA zur Verfügung gestellt haben;
- die Software C2PATOOL sowie die Prüfprogramme VERIFY und TRUEPIC zur Verfügung gestellt haben;
- durch die Bereitstellung überprüfbarer Dateien;
- die Software C2PATOOL, ADOBE FIREFLY und CHATGPT (OPENAI) zur Verfügung stellen, mit denen überprüfbare Dateien erstellt werden können;

14. KEEEX wirft den Beklagten zudem direkte und indirekte Verletzungen der Ansprüche 2, 4, 7, 8, 10, 11, 14, 16 und 18 des erteilten Patents EP 070 sowie der in der geänderten Fassung des streitigen Patents gemäß dem Hauptantrag und den Hilfsanträgen geltend gemachten Ansprüche vor. Der Anspruch 15 des erteilten Patents wird nicht entgegengehalten.

15. Dementsprechend beantragt KEEEX beim Gericht, dass es:

- die Einstellung der Verletzungshandlungen anzuordnen und die Unterlassungsverfügung mit einem Zwangsgeld zu verbinden (Art. 63 AJUB)
- die Gewährung einer vorläufigen Entschädigung in Form eines Schadensersatzes *in solidum* durch die Beklagten in Höhe von 100 Millionen Euro (materieller Schaden) und 20 Millionen Euro (immaterieller Schaden) anzuordnen
- die Veröffentlichung des Tenors der zu erlassenden Entscheidung anzuordnen (Art. 80 AJUB)
- Verurteilt die Beklagten zur Tragung der Gerichtskosten und der dem Kläger sowohl im Hauptsacheverfahren als auch im Widerklageverfahren auf Nichtigkeit entstandenen Kosten,
- Weist die von jeder der Beklagten gestellten Anträge auf vorläufige Kostenerstattung gemäß Regel 150.2 RdP in Höhe von 1,25 Millionen zurück;
- ordnet die sofortige Vollstreckung an (Art. 82 AJUB).

16. ***Zur Widerklage auf Nichtigkeit:***

- die Abweisung sämtlicher Anträge der Beklagten, die darauf abzielen, die Änderung des Patents gemäß Regel 30.1 RdP für unzulässig zu erklären,
- die Abweisung der Anträge auf Nichtigkeit der angefochtenen Patentansprüche,
- die Abweisung der Anträge, die darauf abzielen, die Vollstreckung jeglicher Unterlassungsverfügung oder finanziellen Verurteilung von der Hinterlegung einer Sicherheit durch das Unternehmen abhängig zu machen,
- die Ablehnung der Gewährung einer Nachfrist von 6 Monaten vor jeglicher Vollstreckung,
- die Abweisung der Anträge auf vorläufige Erstattung der Kosten, die von jeder der Beklagten gemäß Regel R 150.2 RdP gestellt wurden.

17. **<u>Alle Beklagten beantragen im Wesentlichen:</u>**

1) ***In Bezug auf die Anträge auf Änderung des Patents:***
die vom Antragsteller beantragten Änderungen des Patents gemäß dem Hauptantrag und den Hilfsanträgen für unzulässig zu erklären und sie in jedem Fall zurückzuweisen;

2) ***Bezüglich der Widerklage auf Nichtigkeit des Patents:***

A. In erster Linie,
die Ansprüche 1, 2, 4, 7, 8, 10, 11, 14, 16 und 18 des Patents (wobei Anspruch 15 nicht von dem Nichtigkeitsantrag betroffen ist) in ihrer Gesamtheit für nichtig zu erklären, wie es im Hoheitsgebiet der folgenden Vertragsstaaten der JUB erteilt wurde: Frankreich, Italien, Deutschland, Österreich, Belgien, Dänemark, den Niederlanden und Schweden;

B. die angefochtenen Ansprüche des europäischen Patents EP 2 949 070 B1 gemäß dem Hauptantrag und den von der Klägerin gestellten Hilfsanträgen im Hoheitsgebiet der folgenden Vertragsstaaten der JUB vollständig für nichtig zu erklären: Frankreich, Italien, Deutschland, Österreich, Belgien, Dänemark, die Niederlande und Schweden.

C. In jedem Fall:
a. die Klägerin zur Tragung aller Kosten der Widerklage auf Nichtigkeit zu verurteilen;
b. die Klägerin zu verurteilen, vorläufig (gemäß Artikel 150 Absatz 2 der Verfahrensordnung) einen Betrag in Höhe von 1,25 Millionen Euro als Kosten im Zusammenhang mit der Nichtigkeits-Widerklage zu erstatten.

18. ***3) Bezüglich der Klage wegen Patentverletzung:***

A. Hauptantrag:
a. die Klage der Klägerin wegen Patentverletzung abzuweisen;
b. den Antrag der Klägerin auf vorläufigen Schadensersatz ABZUWEISEN;
c. die Klägerin in allen ihren Anträgen, Rügen und Ansprüchen abzuweisen;
d. die Klägerin zur Übernahme aller Kosten der Klage wegen Patentverletzung zu verurteilen;
e. die Klägerin zu verurteilen, vorläufig (Regel 150.2 der Verfahrensordnung) einen Betrag von 1,25 Millionen Euro als Kosten für das Verletzungsverfahren zu erstatten.6

B. Hilfsweise,
a. den Antrag der Klägerin auf Verurteilung der Beklagten in solidum abzuweisen;
b. die Vollstreckung jeder Entscheidung, mit der einer Unterlassungsklage stattgegeben wird, von der Leistung einer Sicherheit in Höhe von 50 Millionen Euro durch die Klägerin zugunsten der Beklagten 1) und der Beklagten 2) abhängig zu machen;

c. eine Nachfrist von sechs Monaten zu gewähren, bevor eine Unterlassungsverfügung vollstreckbar wird;
d. den Antrag der Klägerin auf sofortige Vollstreckung der Entscheidung in jedem Fall zurückzuweisen;
e. die Vollstreckung jeglicher Geldstrafe und/oder (vorläufiger) Schadensersatzverurteilung von der Hinterlegung eines entsprechenden Betrags abhängig zu machen.

HINTERGRUND DES RECHTSSTREITS (vor der Klageerhebung)

19. KEEEX gibt an, die im Patent EP 070 offen gelegte Lösung im Jahr 2020 der New York Times in Anwesenheit eines der Gründer des Unternehmens C2PA vorgestellt zu haben, das anschließend den gleichnamigen Standard entwickelt hat. Nach Ansicht von KEEEX kopiere der C2PA-Standard jedoch die Lehren aus seinem Patent EP 070. KEEEX wirft daher den Unternehmen JOINT DVP und C2PA vor, den C2PA-Standard entwickelt zu haben, sowie den Unternehmen ADOBE, OpenAI und TRUEPIC als Mitentwickler zu haben und diesen Standard in Europa über ihre Verifizierungs-Tools kostenlos verbreitet zu haben, wobei sie die Rechte aus dem Patent EP 070 missachtet hätten, was es KEEEX unmöglich gemacht habe, seine Technologie zu vermarkten.

20. Daher wurde am 6. Februar 2025 von den Rechtsbeiständen von KEEEX ein 35-seitiges, ausführlich begründetes Mahnschreiben an ADOBE, OpenAI und TRUEPIC gerichtet (Betreff:
„Aufforderungsschreiben – Verletzung der Patente EP 070 und US 10.218.714“), in dem geltend gemacht wurde, dass C2PA sowie seine Mitgliedsunternehmen die durch EP 070 und US 10.218.714 gewährten ausschließlichen Rechte verletzten, wobei man sich auf das von einem Gerichtsvollzieher (Rechtsanwalt Legrain) vom 15. Januar 2025 sowie auf die technischen Gutachten eines Sachverständigen (Herr Aymar), um die funktionale Ähnlichkeit zwischen den C2PA-Tools und den Patentansprüchen von EP 070 nachzuweisen. Die Unternehmen JOINT DVT und C2PA erhielten ebenfalls eine Aufforderung zur Stellungnahme, und zwar am 31. Januar 2025 bzw. am 22. April 2025 (Aktenstücke KEEEX 9 bis 14).

BEGRÜNDUNG DER ENTSCHEIDUNG

21. **Einleitend zur internationalen Zuständigkeit und zur Zuständigkeit der örtlichen Abteilung in Paris**

Die internationale Zuständigkeit und die innerstaatliche Zuständigkeit wurden von allen Beklagten im Rahmen von Einreden gemäß Regel 19 der Verfahrensordnung (RdP) angefochten. Diese Einreden wurden vom Berichterstatter durch Beschluss vom 27. November 2025 zurückgewiesen. Mit einem Beschluss vom 13. März 2026 hob das Berufungsgericht der JUB den erstinstanzlichen Beschluss auf und entschied, dass das Gericht nicht zuständig sei, über die von den Parteien aus der Schweiz, Spanien, Großbritannien, Irland, Norwegen und Polen geltend gemachte Verletzung des Patents EP 070 zu entscheiden.

22. Zu den übrigen Punkten, zu denen der Berichterstatter auf der Grundlage von R.19 RdP in seinem Beschluss vom 27. November 2025 entschieden hatte, insbesondere die

bezüglich der internen Zuständigkeit der Lokalen Abteilung Paris, wurden in der Berufungsinstanz bestätigt (Auszug aus dem Beschluss des Berufungsgerichts vom 13. März 2026, § 45: *„Die interne Zuständigkeit der Lokalen Abteilung Paris für die Entscheidung in dieser Sache ist im vorliegenden Fall durch die in Frankreich bestehende Zugänglichkeit von Software zur Überprüfung der Integrität von Inhalten gerechtfertigt, die von den Beklagten kostenlos im Internet zur Verfügung gestellt wird. Das Unternehmen Truepic hat im Übrigen in der mündlichen Verhandlung bestätigt, dass es im Rahmen des Berufungsverfahrens die Entscheidung bezüglich der internen Zuständigkeit nicht anficht. Ebenso hat sie bestätigt, dass ihr Antrag auf Aussetzung des Verfahrens durch die Entscheidung vom 12. Januar 2026, mit der der Antrag auf Überprüfung des angefochtenen Beschlusses zurückgewiesen wurde, gegenstandslos geworden ist.“*)

23. Daraus folgt, dass die vorliegende Kammer für die Entscheidung über diesen Rechtsstreit bezüglich der Teile des Patents ausschließlich in den Vertragsstaaten des JUB-Abkommens zuständig ist, d. h.: Frankreich, Italien, Deutschland, Österreich, Belgien, Dänemark, die Niederlande und Schweden.

VORSTELLUNG DES BETROFFENEN PATENTS

24. Das Patent EP 070 trägt den Titel „Verfahren zur Überprüfung der Integrität eines digitalen Datenblocks“ [Anlage 2.1 von KEEEX].
Das Patent geht auf eine internationale Anmeldung PCT/FR2014/050073 zurück, die am 15. Januar 2014 von der Universität Aix-Marseille und dem CNRS (Centre National de la Recherche Scientifique) eingereicht wurde [Anlage ADOBE, DTMV 3.3].
Als Erfinder ist Herr Laurent HENOCQUE genannt.

25. Die internationale Anmeldung und damit das Patent EP 070 beansprucht die Priorität einer französischen Patentanmeldung FR 13 50549, die am 22. Januar 2013 eingereicht und am 12. Februar 2016 unter der Nummer FR 3 001 313 erteilt wurde. Die internationale Anmeldung wurde am 31. Juli 2014 unter der Nummer WO 2014/114861 veröffentlicht.

26. Es ist unstreitig, dass das Patent zum Zeitpunkt der von KEEEX geltend gemachten Patentverletzung in den folgenden Vertragsstaaten in Kraft ist: Frankreich, Italien, Deutschland, Österreich, Belgien, Dänemark, den Niederlanden und Schweden.

27. EP 070 betrifft allgemein Verfahren zur Überprüfung der Integrität und Authentizität digitaler Datenblöcke sowie zum Zugriff auf diese Datenblöcke, unabhängig davon, ob diese über ein Netzwerk verteilt oder auf einem Speichermedium gespeichert sind ([0001] des Patents).

28. Das Patent enthält Definitionen mehrerer Begriffe oder Ausdrücke [0002] und führt insbesondere aus, dass „Datenblock“ [0003] jede digitale Datei oder jedes digitale Dokument bzw. jeden Teil einer solchen Datei oder eines solchen Dokuments bezeichnet, wobei der Begriff „Datei“ nicht als auf eine Datei eines Dateiverwaltungssystems beschränkt zu verstehen ist.

29. Darüber hinaus wird der Ausdruck „digitaler Fingerabdruck“ in [0005] wie folgt definiert: „ein durch eine Funktion erzeugtes Datum, das die Integrität

des Datenblocks zu gewährleisten, sodass sich der digitale Fingerabdruck ändert, wenn ein Bit des Datenblocks verändert wird. Diese Funktion kann eine Hash-Funktion sein, muss es aber nicht. Ein digitaler Fingerabdruck wird manchmal auch als Hash-Schlüssel, Prüfsumme, Fingerabdruck, Hash, Nachrichtenzusammenfassung, Kondensat oder kryptografischer Fingerabdruck bezeichnet“.

30. Schließlich wird der Begriff „digitale Signatur“ in [006] wie folgt definiert: „Ein digitaler Fingerabdruck, der mit Hilfe eines privaten Schlüssels eines öffentlichen/privaten Schlüsselpaars und eines asymmetrischen kryptografischen Programms wie ‚pgp
“ (Pretty Good Privacy) oder dessen freies Pendant „gpg“ (Gnu Privacy Guard) verschlüsselt wurde.
Eine digitale Signatur ermöglicht es, die Integrität eines Datenblocks zu gewährleisten und dessen Unterzeichner zu authentifizieren, analog zur handschriftlichen Unterschrift auf einem Papierdokument. Es ist anzumerken, dass eine digitale Signatur mit den Eigenschaften eines digitalen Fingerabdrucks erhalten werden kann, indem ein asymmetrisches Verschlüsselungsprogramm direkt auf den Datenblock angewendet wird.“

31. Im Stand der Technik ist es bekannt, zur Gewährleistung der Integrität einer Datei Hash-Funktionen zu verwenden, wie sie in der Patentschrift in den Absätzen [0009] bis [0025] beschrieben sind.

32. In der Patentschrift wird darauf hingewiesen, dass die Lösungen des Standes der Technik den folgenden Nachteil aufweisen [0027]:

- *„Derzeit kann ein Fingerabdruck oder eine Signatur nicht in einen Datenblock eingefügt werden, ohne dass sich dessen Wert dadurch ändert. Ein Datenblock kann keine eigenen gültigen Fingerabdrücke oder Signaturen enthalten. Ein Fingerabdruck oder eine Signatur (…) kann daher nicht gleichzeitig als Identifikations- oder Authentifizierungselement und als Suchkriterium für einen von Suchmaschinen indizierten Datenblock verwendet werden. (…) Es gibt keine Möglichkeit, den Datenblock, der dieser Signatur entsprechen könnte, sofort zu ermitteln. Darüber hinaus ist es, sobald ein Datenblock gefunden wurde, ein aufwendiger Vorgang, zu überprüfen, ob dieser Block mit der Signatur übereinstimmt*.“

33. Das Patent erläutert, dass diese Schwierigkeiten darauf zurückzuführen sind, dass „die zur Identifizierung oder Authentifizierung eines Datenblocks erforderlichen Informationen außerhalb dieses Blocks verbleiben müssen“. Die außerhalb des Blocks befindlichen Informationen „können daher von einem Dritten verfälscht oder durch Tricks betrügerisch zugänglich gemacht werden“ [0028].

34. Das Patent EP 070 weist darauf hin, dass ein Bedarf an einer Lösung besteht, die „das Einfügen eines Fingerabdrucks oder einer Signatur in einen Datenblock auf kontrollierte und gegebenenfalls zerstörungsfreie Weise“ ermöglicht. Darüber hinaus besteht ein Bedarf an einem Verfahren, „das in der Lage ist, diesen Fingerabdruck oder diese Signatur automatisch zu überprüfen und/oder zu aktualisieren“. [0029]

35. Das Patent EP 070 schlägt vor, diese Schwierigkeiten zu beheben, indem es ein Verfahren zur Überprüfung der Integrität eines digitalen Datenblocks offenlegt, wie es in Absatz [0030] dargelegt ist. Dieses im Patent offen gelegte Verfahren läuft in

zwei Schritten ab:

- Zunächst wird aus einer Ausgangsdatei ein Fingerabdruck berechnet und anschließend in diese Datei eingefügt, um eine „überprüfbare“ Datei zu erzeugen.
- In einem zweiten Schritt, wenn die Integrität der Datei überprüft werden soll, sucht das System nach dem in der Datei gespeicherten Fingerabdruck, berechnet einen neuen Fingerabdruck, wobei der Bereich, der diesen Fingerabdruck enthält, aus der Berechnung ausgeschlossen wird, und vergleicht dann die beiden Werte. Stimmen diese überein, gilt die Datei als intakt; andernfalls gilt sie als verändert. Verschiedene Ausführungsformen dieses Verfahrens werden in den Absätzen [0031] bis [0044] vorgestellt.

36. Das Patent lehrt zudem verschiedene Ausführungsformen bezüglich eines Computerprogrammprodukts, das auf einem computerlesbaren Träger gespeicherte Programmdateiteile umfasst (vgl. [0045] bis [0050]).

37. Schließlich werden in der Beschreibung des Patents die verschiedenen Figuren des Patents von Absatz [051] bis Absatz [103] vorgestellt.

38. So stellt Abbildung 1 Schritte eines Verfahrens dar, das gegebenenfalls eine Einfügephase (a), eine Überprüfungsphase (b) und eine Aktualisierungsphase (c) eines Fingerabdrucks in einem digitalen Datenblock in einer Ausführungsform umfasst: [0051]

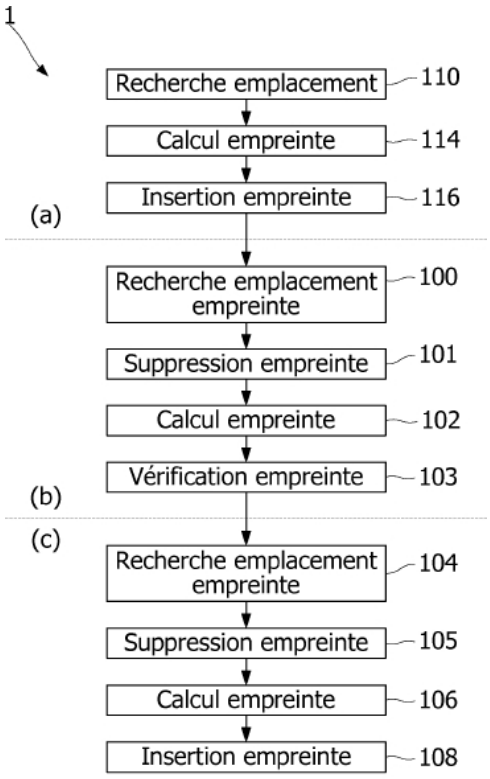


Fig. 1

39. Abbildung 3 des Patents zeigt den Datenblock vor und während einer Fingerabdruckprüfung eines Datenblocks [0058]:

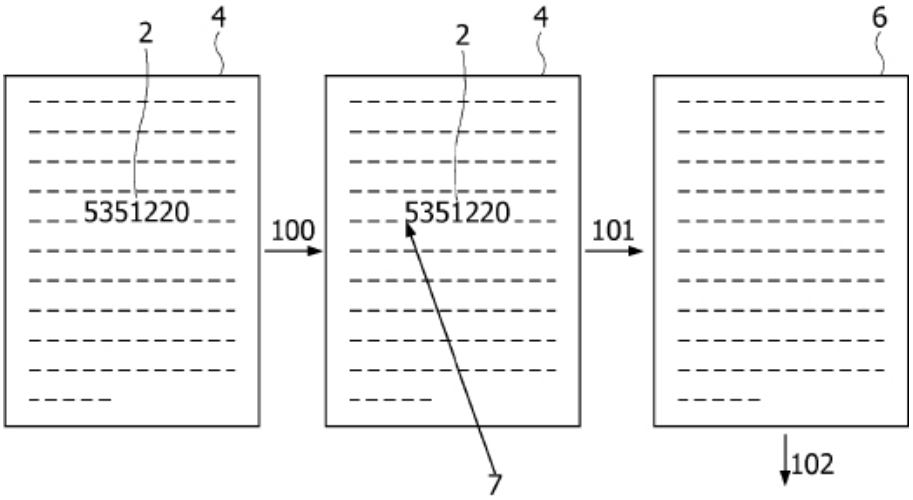


Fig. 3

40. Das Patent umfasst 20 Ansprüche. Die Ansprüche 1, 16 und 18 sind unabhängig. Die Ansprüche 2 bis 15 sind von Anspruch 1 (R1) ab. Anspruch 17 ist von Anspruch 16 abhängig. Die Ansprüche 19 und 20 sind von Anspruch 18 abhängig. Nur die Ansprüche 1, 2, 4, 7, 8, 10, 11, 14, 16 und 18 des erteilten Patents werden den Beklagten wegen der behaupteten Patentverletzung entgegengehalten (vgl. Klageschrift und Zusammenfassung der Anträge von KEEEX vom 7. September 2026).

41. Die geltend gemachten Ansprüche des erteilten Patents lauten in französischer Sprache wie folgt:

„1. Verfahren zur Überprüfung der Integrität eines digitalen Datenblocks, wobei das Verfahren folgende Schritte umfasst:

in einem ersten Datenblock (4) mittels eines ersten Markers (7) nach einem digitalen Identifikationsfingerabdruck des ersten Datenblocks (4) zu suchen,

wenn der Identifikationsfingerabdruck (2) des ersten Datenblocks im ersten Datenblock gefunden wird, Berechnen eines digitalen Fingerabdrucks des ersten Datenblocks durch Anwenden einer Fingerabdruck-Berechnungsfunktion auf den ersten Datenblock, wobei der berechnete Fingerabdruck des ersten Datenblocks einen Wert aufweist, der von jedem der Bits des ersten Datenblocks abhängt, mit Ausnahme der Bits des im ersten Datenblock gefundenen Identifikations-Fingerabdrucks (2), und

den im ersten Datenblock gefundenen Identifikationsfingerabdruck durch Vergleich mit dem berechneten Fingerabdruck des ersten Datenblocks zu überprüfen, wobei ein fehlgeschlagener Vergleich anzeigt, dass der erste Datenblock verändert wurde, seit der Identifikationsfingerabdruck in den ersten Datenblock eingefügt wurde,

oder dass der Identifikations-Fingerabdruck durch Anwendung einer anderen Fingerabdruck-Berechnungsfunktion auf den ersten Datenblock berechnet wurde“.

42. **Die von R 1 abhängigen Ansprüche 2, 4, 7, 8, 10, 11 und 14 lauten wie folgt:**

2. Verfahren nach Anspruch 1, wobei der erste Datenblock einen Referenzlink umfasst, der aus einem weiteren Identifikations-Fingerabdruck gebildet ist, der in einem zweiten Datenblock vorhanden ist, und dessen Wert von jedem der Bits des zweiten Datenblocks abhängt, wobei die Bits des anderen Identifikations-Fingerabdrucks ausgeschlossen sind.

4. Verfahren nach einem der Ansprüche 1 bis 3, umfassend Schritte zum Erzeugen eines überprüfbaren Datenblocks, bestehend aus:

Suchen einer Fingerabdruck-Einfügestelle in einem ursprünglichen Datenblock (3) mittels einer dritten Markierung,

Berechnen eines dritten digitalen Fingerabdrucks (2) des überprüfbaren Datenblocks durch Anwenden der Fingerabdruck-Berechnungsfunktion auf den ursprünglichen Datenblock, wobei der berechnete dritte Fingerabdruck des überprüfbaren Datenblocks einen Wert aufweist, der von jedem der Bits des ursprünglichen Datenblocks abhängt, und

Erzeugen des überprüfbaren Datenblocks durch Einfügen des berechneten dritten Fingerabdrucks des überprüfbaren Datenblocks als Identifikationsfingerabdruck des überprüfbaren Datenblocks an der im Ausgangsdatenblock gefundenen Einfügestelle.

7. Verfahren nach einem der Ansprüche 3 bis 5, umfassend mehrere Schritte zum Berechnen eines Fingerabdrucks eines Datenblocks und zum Einfügen des berechneten Fingerabdrucks in den Datenblock unter Beibehaltung der bereits in den Datenblock eingefügten Fingerabdrücke.

8. Verfahren nach einem der Ansprüche 1 bis 7, umfassend einen Schritt zum Auslesen einer Information, die für die Lokalisierung und/oder die Berechnung eines Identifikationsfingerabdrucks (2) nützlich ist und in einem Datenblock (4) enthalten ist, der den Identifikationsfingerabdruck enthält.

10. Verfahren nach einem der Ansprüche 1 bis 9, wobei einer der Datenblöcke Metadaten umfasst, die einen variablen Teil enthalten, der von der auf den Datenblock angewandten Fingerabdruckberechnung zur Berechnung des Identifikationsfingerabdrucks des Datenblocks ausgeschlossen ist.

11. Verfahren nach Anspruch 10, wobei sich der Identifikationsfingerabdruck des Datenblocks im variablen Teil von Identifikations-Metadaten befindet.

14. Verfahren nach einem der Ansprüche 1 bis 13, wobei das Einfügen jedes Identifikations-Fingerabdrucks (2) in einen Datenblock (4) an einer Stelle im Datenblock erfolgt, die so gewählt ist, dass die erwarteten Nutzungsbedingungen des Datenblocks (4) durch ein Softwareprogramm nicht verändert werden.“

43. **Der unabhängige Anspruch 16** lautet wie folgt:

16. Computerprogrammprodukt, das auf einem computerlesbaren Träger gespeicherte Programmdateiteile umfasst, um die Schritte des Verfahrens gemäß einem der Ansprüche 1 bis 15 auszuführen.

44. Schließlich lautet **der unabhängige Anspruch 18** wie folgt:

18. Eine Sammlung von Dateien, die jeweils auf einem computerlesbaren Datenträger gespeichert sind, wobei jede Datei einen digitalen Identifikationsfingerabdruck der Datei enthält, wobei der Identifikationsfingerabdruck der Datei mittels eines Verweises in der Datei auffindbar ist, wobei der Identifikationsfingerabdruck der Datei einen Wert aufweist, der durch Anwenden einer Fingerabdruck-Berechnungsfunktion auf die Datei berechnet wird, wobei der Wert des Identifikations-Fingerabdrucks von jedem der Bits der Datei abhängt, mit Ausnahme der Bits des in der Datei enthaltenen Identifikations-Fingerabdrucks der Datei, wobei die Integrität jeder Datei des Dateisatzes mithilfe des Verfahrens gemäß einem der Ansprüche 1 bis 15 überprüfbar ist und jede Datei als Datenblock betrachtet wird“

AUSLEGUNG UND AUSWERTUNG DER ANSPRÜCHE

45. ***Der Fachmann***

Die Merkmale der Ansprüche sind aus der Sicht eines Fachmanns auszulegen.

Rechtlicher Rahmen

Der Fachmann ist eine fiktive Person, die keiner realen Person auf dem technischen Gebiet der Erfindung zugeordnet werden kann. Ausschlaggebend ist nicht die Gesamtheit der individuellen Kenntnisse und Fähigkeiten einer Person, sondern vielmehr das allgemeine Fachwissen, die durchschnittliche Erfahrung und die normalen Fähigkeiten, die zum Zeitpunkt der Einreichung auf dem betreffenden technischen Gebiet zu erwarten sind (UPC_CoA_768/2024, 30. April 2025, Insulet Corporation gegen EOFlow Co).

KEEEX schlägt folgende Definition vor: Unter Berücksichtigung des technischen Problems der vorgestellten und beanspruchten Lösung ist der Fachmann ein Techniker, der auf die Nutzung von Systemen zur elektronischen Verwaltung digitaler Dokumente, zur Datenfreigabe und zur Archivierung spezialisiert ist. Er befasst sich mit den Anforderungen der Indizierung und Kennzeichnung von Inhalten. Als einfacher Nutzer von Hash- und Signaturalgorithmen benötigt er hingegen keine fundierten Kenntnisse in Kryptografie (vgl. Seite 11 der Zusammenfassung seiner Klagegründe).

Die Beklagten (Klageerwiderung von ADOBE, § 24, bzw. die von OPENAI, Seite 5 der Zusammenfassung ihrer Klagegründe) schlagen folgende Definition vor: Der Fachmann ist als Informatikingenieur zu definieren, der auf die

Sicherheit von Informationssystemen, insbesondere in angewandter Kryptografie und im Management der Integrität digitaler Daten, der über mehrjährige Erfahrung in diesem Bereich verfügt.

46. Standpunkt des Gerichts:
Das Gericht ist überzeugt, dass die von den Beklagten vorgeschlagene Definition am zutreffendsten ist, da das Verständnis des Patents die Kenntnis kryptografischer Konzepte erfordert, die über die bloße Anwendung von Hash-Algorithmen und digitalen Signaturen hinausgehen.

Es wird daher folgende Definition zugrunde gelegt: Der Fachmann ist im vorliegenden Fall ein Informatiker oder ein auf Informatik spezialisierter Ingenieur, der über mehrjährige Berufserfahrung im Bereich der IT-Sicherheit und der kryptografischen Verfahren zur Gewährleistung der Datenintegrität verfügt.

47. ***Die Grundsätze der Auslegung***

Die für die Auslegung der Ansprüche geltenden Grundsätze wurden vom Berufungsgericht der Einheitlichen Patentgerichtsbarkeit in seinem Beschluss in der Rechtssache UPC_CoA_335/2023 vom 26. Februar 2024, NanoString gegen 10x Genomics, in der berichtigten Fassung, dargelegt; siehe auch Berufungsgericht, UPC_CoA_1/2024 vom 13. Mai 2024, VusionGroup gegen Hanshow; UPC_CoA_768/2024 vom 30. April 2025, Insulet
gegen EOFlow. Ein Patentanspruch bildet nicht nur den Ausgangspunkt, sondern auch die maßgebliche Grundlage für die Bestimmung des Schutzumfangs eines europäischen Patents gemäß Artikel 69 EPÜ in Verbindung mit dem Auslegungsprotokoll zu Artikel 69 EPÜ. Die Auslegung eines Patentanspruchs darf sich nicht auf die enge und wörtliche Bedeutung der verwendeten Begriffe beschränken. Vielmehr sind die Beschreibung und die Zeichnungen stets als Erläuterungsmittel zur Auslegung des Anspruchs heranzuziehen und nicht nur dazu, etwaige Unklarheiten des Anspruchs zu beseitigen. Ein Patentanspruch ist stets aus der Sicht eines Fachmanns auszulegen. Dieser legt die Merkmale eines Anspruchs stets im Lichte der Gesamtheit der Ansprüche aus (UPC_CoA_1/2024, 13. Mai 2024, VusionGroup
gegen Hanshow; UPC_CoA_768/2024, 30. April 2025, Insulet gegen EOFlow; UPC_CoA_646/2024, 25. November 2025, Meril gegen Edwards). Diese Grundsätze zur Auslegung eines Patentanspruchs gelten sowohl für die Frage der Patentverletzung als auch für die Frage der Gültigkeit des Patents (NanoString gegen 10x Genomics).

Bei der Anwendung dieser Grundsätze besteht das Ziel darin, einen angemessenen Schutz für den Patentinhaber mit ausreichender Rechtssicherheit für Dritte zu verbinden.

48. **Hinsichtlich Anspruch 1 sind sich die Parteien über die Auslegung der Begriffe „digitale Signaturen und Fingerabdrücke“ uneinig:**

49. Nach Ansicht von KEEEX kann der Identifikationsfingerabdruck nicht durch eine digitale Signatur erstellt werden, wobei sich das Unternehmen auf folgende Argumente stützt (vgl. Seite 13, Zusammenfassung seiner Klagegründe):

Gemäß Absatz [0006] des Patents EP'070 bezeichnet eine digitale Signatur einen digitalen Fingerabdruck, der mithilfe eines privaten Schlüssels eines öffentlichen/privaten Schlüsselpaars und eines asymmetrischen kryptografischen Programms verschlüsselt wurde.

Die Begriffe „Fingerabdruck" und „digitale Signatur" bezeichnen somit eindeutig unterschiedliche Objekte, wobei die Signatur aus einem Fingerabdruck gewonnen wird, der durch ein asymmetrisches kryptografisches Programm und einen privaten Schlüssel eines Unterzeichners in eine Signatur umgewandelt wird.

Absatz [0074] des erteilten Patents stellte eindeutig eine weitere Ausführungsform dar (eingeleitet mit „In einer zweiten Ausführungsform"), bei der der Fingerabdruck in Form einer digitalen Signatur in den Datenblock eingefügt wird, was nichts anderes bedeutet, als dass die Position des Fingerabdrucks im Datenblock durch eine digitale Signatur eingenommen wird.

Im Übrigen gibt es in der gesamten Beschreibung keinerlei Unklarheiten hinsichtlich der Verwendung der Begriffe „Fingerabdruck" und „Signatur". Zu keinem Zeitpunkt wird einer dieser Begriffe anstelle des anderen verwendet, und wenn beide Objekte betroffen sind, werden sie beide in der Form „Fingerabdruck und/oder Signaturen" erwähnt (vgl. Absätze [0087], [0089] und [0095]). Folglich bezeichnen die Begriffe „Fingerabdruck" und „Signatur"
" im Patent EP 070 eindeutig unterschiedliche Objekte."

Laut KEEEX ist eine Signatur das Ergebnis eines kryptografischen Vorgangs, bei dem ein Datenblock (oder dessen Fingerabdruck) mit einer Kennung eines Unterzeichners (dem privaten Schlüssel des Unterzeichners) kombiniert wird. Folglich identifiziert eine Signatur nicht einen Datenblock, sondern ein Objekt, das einen Datenblock mit einem Unterzeichner verknüpft, der eine vom Datenblock völlig getrennte Einheit darstellt. Daraus folgt, dass ein und derselbe Datenblock unendlich viele Unterzeichner und somit unendlich viele verschiedene Signaturen haben kann. Eine Signatur kann daher nicht in gleicher Weise eine Identifizierungsfunktion für einen Datenblock erfüllen wie ein Identifikationsfingerabdruck des Datenblocks, dessen Berechnung nur eine einzige Eingabe erhält, nämlich den Inhalt des Datenblocks. Schließlich verweist KEEEX auf das Gutachten von Professor Quisquater (seine Anlage 37), wonach: „Der Wert einer Signatur ist keineswegs eine (Art) von Fingerabdruck, da er mit einem Absender verbunden ist, der über einen geheimen Schlüssel verfügt, der seiner persönlichen Identität entspricht. Es handelt sich also um einen kontextabhängigen Wert, der per Definition variabel ist. Es muss unbedingt sichergestellt werden, dass dieser Kontext korrekt ist." (vgl. das Verhandlungsheft – oder Booklet – von KEEEX zur Unterstützung der Plädoyers in der mündlichen Verhandlung, Seite 4).

50. <u>Nach Ansicht der Beklagten, insbesondere von ADOBE und OPENAI, berücksichtigt das Patent EP 070 nicht die Unterschiede zwischen dem digitalen Fingerabdruck und der digitalen Signatur</u>:

Die Beklagten fassen diese beiden Konzepte unter dem allgemeineren Begriff „digitaler Fingerabdruck" zusammen. Dieser Begriff ist sehr weit gefasst und umfasst auch digitale Signaturen, wie in den Absätzen [0006] und [0044] des Patents dargelegt (Klageerwiderung von Adobe, §13 und 14, Seite 19). Die Beklagten führen diesen Standpunkt in allen ihren Schriftsätzen aus und bekräftigen

ihn

mündlichen Verhandlung bei der Vorstellung des Patents durch den Vertreter von OpenAI. Dieser verweist auf die im Patent selbst unter [0005] gegebene Definition und weist darauf hin, dass bereits in [0006], das den Begriffsdefinitionen des Patents gewidmet ist, ausdrücklich erwähnt wird, dass „eine digitale Signatur einen ‚digitalen Fingerabdruck' bezeichnet, der verschlüsselt ist (…). Daraus folgt, dass eine Signatur eine Unterkategorie des digitalen Fingerabdrucks ist. Dies wird in [0062] des Patents bestätigt: „(…) das Verfahren 1 entspricht einem Verfahren zur Identifizierung, Überprüfung und Authentifizierung eines Datenblocks, in den ein Fingerabdruck auf kontrollierte Weise eingefügt wurde (…)". Dies wird auch durch verschiedene im Patent offen gelegte Ausführungsformen bestätigt, wie beispielsweise in Absatz [0074]: „Der Fingerabdruck 2 wird in Form einer digitalen Signatur (…) in den Datenblock 4 eingefügt, was bedeutet, dass es sich bei der Verwendung eines verschlüsselten Fingerabdrucks um eine ‚digitale Signatur' handelt." Aus Absatz [0076] geht hervor, dass

„gemäß einer Ausführungsform Metadaten, die in den Datenblock eingefügt werden, den Fingerabdruck oder die Signatur eines anderen Datenblocks enthalten, um eine Referenzverbindung herzustellen (…)" und durch weitere in den Absätzen 92, 93 oder 95 offen gelegte Ausführungsformen; so heißt es im letztgenannten Absatz

„dass diese Ausführungsform die Verarbeitung von Datenblöcken mit mehreren Vorkommen von Fingerabdrücken und/oder Signaturen ermöglicht (…). Schließlich ist Anspruch 15 des Patents entscheidend, da er besagt: „ein Verfahren gemäß einem der Ansprüche 1 bis 14, bei dem der in einen Datenblock eingefügte Identifikationsfingerabdruck eine digitale Signatur ist (…)". Nach Ansicht der Beklagten seien die Ausführungen in der Bescheinigung von Professor Quisquater, auf die sich KEEEX bezieht (Anlage 37 von KEEEX), für die Auslegung der Begriffe des Patents nicht relevant, da sie außerhalb des Kontexts des Patents erwähnt würden, diese Begriffe jedoch im Kontext des Patents auszulegen seien.

51. Standpunkt des Gerichts:

Das Gericht ist von der vom Kläger vorgebrachten Argumentation hinsichtlich einer Beschränkung des Anspruchs 1 ausschließlich auf Fingerabdrücke vom Typ „Hash" (oder „Hashwert") beschränkt sei. Im Gegenteil, aus dem gesamten Patent geht hervor, dass Anspruch 1 auch digitale Signaturen umfasst.

52. Zwar trifft es zu, dass in der Beschreibung konzeptionell zwischen dem digitalen Fingerabdruck und der digitalen Signatur unterschieden wird. In Absatz [0005] wird der digitale Fingerabdruck als Datenangabe definiert, die es insbesondere ermöglicht, die Integrität eines Datenblocks zu überprüfen, während in Absatz [0006] die digitale Signatur als ein mit einem privaten Schlüssel verschlüsselter digitaler Fingerabdruck dargestellt wird. Das Patent identifiziert also zwei unterschiedliche technische Gegenstände, und aus technischer und kryptografischer Sicht ist eine Signatur nicht mit einem einfachen Hashwert identisch. Darüber hinaus bestätigt Absatz [0006], dass eine digitale Signatur die Integrität eines Datenblocks gewährleisten kann, ebenso wie ein einfacher Fingerabdruck.

53. Die Frage ist jedoch nicht, ob ein Hash und eine Signatur technisch unterschiedlich sind, sondern zu beurteilen, wie ein Fachmann

den beanspruchten Ausdruck „digitaler Identifikationsfingerabdruck“ im Rahmen von Anspruch 1 des streitigen Patents verstehen würde. Nichts in Anspruch 1 schließt digitale Signaturen ausdrücklich aus. Der Anspruch erwähnt weder eine Hash-Funktion noch einen Hash noch einen bestimmten Algorithmus. Er bezieht sich lediglich auf einen „digitalen Identifikationsfingerabdruck“. Hätte der Anmelder den Anspruch ausschließlich auf nicht signierte Fingerabdrücke beschränken wollen, wäre ihm dies ohne Weiteres möglich gewesen. Eine solche Beschränkung geht aus dem beanspruchten Wortlaut nicht hervor.

54. Diese Auslegung wird durch die Beschreibung in ihrer Gesamtheit bestätigt. Das Patent stellt Signaturen zu keinem Zeitpunkt als der Erfindung fremd dar. Im Gegenteil: Mehrere Passagen der Beschreibung sehen ausdrücklich die Verwendung digitaler Signaturen im Rahmen des beanspruchten Verfahrens vor. Absatz [0074] beschreibt genau den Fall, in dem der Identifikationsfingerabdruck aus einer digitalen Signatur besteht, und erläutert, wie die Überprüfung erfolgt.

- [0074] *In einer zweiten Ausführungsform des Verfahrens 1, 1’ wird der Fingerabdruck 2 in den Datenblock 4 in Form einer digitalen Signatur eingefügt, die durch Verschlüsselung des Fingerabdrucks des Datenblocks mit einem privaten Schlüssel eines öffentlichen/privaten Schlüsselpaars erzeugt wird. Die Überprüfung 102 der digitalen Signatur kann darin bestehen, die Signatur mit dem öffentlichen Schlüssel des öffentlichen/privaten Schlüsselpaars zu entschlüsseln, um einen entschlüsselten Fingerabdruck des Datenblocks zu erhalten, und darin zu überprüfen, ob der entschlüsselte Fingerabdruck mit demjenigen übereinstimmt, der aus dem geänderten Datenblock 6 berechnet wurde, in dem der Fingerabdruck 2 im Schritt des Löschens 101 oder des Ersetzens 101' entfernt wurde. Es ist zu beachten, dass der Fingerabdruck 2 auch eine Signatur sein kann, die berechnet wird, indem nicht ein Fingerabdruck des Datenblocks, sondern direkt der Datenblock selbst mit dem privaten Schlüssel verschlüsselt wird. In diesem Fall kann die Überprüfung der Signatur erfolgen, indem die Signatur mit Hilfe des entsprechenden öffentlichen Schlüssels entschlüsselt wird und der so erhaltene entschlüsselte Datenblock mit dem modifizierten Datenblock verglichen wird.*

55. Auch die Absätze [0075], [0077], [0092] und [0093] befassen sich mit der Verwendung von Signaturen im Rahmen der Funktionsweise der Erfindung. Ein objektiver Leser des Patents, wie es ein Fachmann ist, versteht daher, dass der Verfasser digitale Signaturen als Teil der von seiner Lehre abgedeckten Ausführungsformen betrachtete.

56. Das Vorhandensein des abhängigen Anspruchs 15 erscheint noch bedeutender:

- 15. *Verfahren nach einem der Ansprüche 1 bis 14, wobei der in einen Datenblock eingefügte Identifikationsfingerabdruck (2) eine digitale Signatur ist, die durch eine asymmetrische kryptografische Berechnung unter Verwendung eines privaten Schlüssels eines öffentlichen/privaten Schlüsselpaars erzeugt wird, und die Fingerabdruckprüfung (102) einen Schritt zum Entschlüsseln der im Datenblock gefundenen digitalen Signatur mit dem öffentlichen Schlüssel des öffentlichen/privaten Schlüsselpaars umfasst, wobei sich der öffentliche Schlüssel in Metadaten des Datenblocks befinden kann.*

57. Dieser Anspruch sieht ausdrücklich vor, dass der Identifikationsfingerabdruck eine digitale Signatur ist, d. h., die Signatur wird nicht beispielsweise dem Fingerabdruck hinzugefügt: Die Signatur ist der Fingerabdruck. Gemäß den üblichen Grundsätzen der Auslegung von Ansprüchen fügt ein abhängiger Anspruch normalerweise eine bestimmte Einschränkung zu einem Gegenstand hinzu, der bereits durch den Anspruch abgedeckt ist, von dem er abhängt. Würde Anspruch 1 digitale Signaturen grundsätzlich ausschließen, wäre Anspruch 15 technisch unsinnig, da er einen Gegenstand einführen würde, der außerhalb des Geltungsbereichs des unabhängigen Anspruchs liegt. Die naheliegendste Auslegung ist hingegen, dass Anspruch 1 allgemein Identifikations-Hashwerte abdeckt, zu denen auch digitale Signaturen gehören, während sich Anspruch 15 darauf beschränkt, diese bestimmte Ausführungsform ausdrücklich zu schützen.

58. Das Gericht ist auch nicht von dem Argument von KEEEX überzeugt, wonach das Merkmal 1.5 zwangsläufig einen direkten Vergleich zweier „Hashes“ vorschreiben würde. Der Anspruch verlangt, dass eine Überprüfung durch den Vergleich des gefundenen Fingerabdrucks mit dem berechneten Fingerabdruck erfolgt, präzisiert jedoch nicht, welche Zwischenschritte vor diesem Vergleich erforderlich sein können. Wird eine digitale Signatur verwendet, kann das Verfahren durchaus einen vorbereitenden Schritt umfassen, bei dem der der Signatur zugrunde liegende Fingerabdruck ermittelt wird, bevor der Vergleich durchgeführt wird. Genau diese Auslegung wird in den Absätzen [0074] und [0075] beschrieben.

59. Aus diesen Gründen ist das Gericht der Ansicht, dass es mit dem Wortlaut der Ansprüche, der Struktur des Patents und der Lehre der Beschreibung im Einklang steht, davon auszugehen, dass Anspruch 1 sowohl nicht signierte Fingerabdrücke als auch digitale Signaturen umfasst. Die Tatsache, dass in der Beschreibung zwischen diesen beiden Begriffen unterschieden wird, führt nicht dazu, dass Signaturen aus dem Geltungsbereich des Anspruchs ausgeschlossen werden; sie führt lediglich dazu, anzuerkennen, dass eine Signatur eine besondere Form eines Identifikationsfingerabdrucks darstellt, der in bestimmten Ausführungsformen des Patents zum Einsatz kommt.

60. Das Gericht stellt ferner fest, dass KEEEX im Rahmen seiner auf Regel 30 der Verfahrensordnung gestützten Änderungsanträge versucht hat, Anspruch 15 zu streichen und entsprechend mehrere Passagen der Beschreibung, insbesondere die Absätze [0044] und [0074], zu ändern.

61. Das erklärte Ziel dieser Änderungen bestand darin, klarzustellen, dass der im Patent genannte „digitale Identifikationsabdruck“ nicht als digitale Signatur, sondern als Hash-Abdruck zu verstehen ist. KEEEX macht somit geltend, dass Anspruch 15 und bestimmte Passagen der Beschreibung eine Verwechslung zwischen zwei unterschiedlichen technischen Konzepten aufrechterhalten und nicht korrekt widerspiegeln, was sie als die eigentliche Lehre der Erfindung ansieht. Dieses letzte Argument, das von KEEEX erst in ihrer Erwiderung auf die Klagebeantwortung vorgebracht wurde, ist nicht überzeugend.

62. Das Gericht stellt ferner fest, dass der Antragsteller auf Nachfrage des Berichterstatters ausdrücklich angegeben hat, dass seine Anträge auf Änderung des Patents bedingt im Sinne von Regel 30.1 RdP seien (Mitteilung über CMS vom 24.06.2026). Dies bedeutet, dass der Kläger seinen Antrag auf Änderung des Patents nur dann aufrechterhält, wenn die erteilte Fassung im Rahmen dieses Rechtsstreits für ungültig erklärt wird. Dies wird in der aktualisierten Zusammenfassung der Anträge bestätigt, die KEEEX auf Ersuchen des Berichterstatters am 7. September 2026 über das CMS eingereicht hat, und zwar wie folgt:

DECLARER recevable la société KEEEX en tant que titulaire du Brevet européen EP 2 949 070 B1 ;

DECLARER valable l'ensemble des revendications du Brevet européen EP 2 949 070 B1, **à défaut**,

FAIRE DROIT à la requête principale de modification du Brevet européen EP 2 949 070 B1 concernant la suppression de la revendication 15, **à défaut**,

FAIRE DROIT successivement aux requêtes subsidiaires, dans l'ordre dans lequel elles sont présentées (de la première requête à la onzième requête subsidiaire) ;

MODIFIER le Brevet européen EP 2 949 070 B1 conformément aux requêtes retenues, afin de clarifier la portée du Brevet et de préserver sa validité ;

63. Folglich beabsichtigte KEEEX nicht, das Patent in seiner erteilten Fassung aufzugeben, sondern beantragte lediglich hilfsweise eine Änderung für den Fall, dass die ursprüngliche Fassung vom Gericht für ungültig erklärt werden sollte. Das Gericht hat daher die strittigen Begriffe im Hinblick auf die erteilte Fassung ausgelegt.

64. **Der Ausdruck „digitaler Datenblock“**

Was den Begriff „digitaler Datenblock“ betrifft, so wird dessen Definition in der Beschreibung unter [0003] des Patents wie folgt angegeben: „bezeichnet jede digitale Datei oder jedes digitale Dokument oder jeden Teil einer solchen Datei oder eines solchen Dokuments, wobei der Begriff ‚Datei‘ nicht als auf eine Datei eines Dateiverwaltungssystems beschränkt zu verstehen ist“.

Nichts in Anspruch 1.1 beschränkt den Datenblock auf ein bestimmtes Format.

Es kann sich insbesondere um ein PDF-Dokument, ein Bild, eine Audio- oder Videodatei, eine XML-Datei, ein Archiv oder ganz allgemein um jede digitale Datenmenge handeln, die einen Identifikationsfingerabdruck enthalten kann.

65. **Auswirkungen der Auslegung auf die Ausgestaltung der Ansprüche**

Der Anspruch 1 in französischer Sprache lautet gemäß der von ADOBE vorgeschlagenen (und von den anderen Parteien nicht bestrittenen) Aufgliederung der Merkmale, die das Gericht wie folgt übernimmt:

- Verfahren zur Überprüfung der Integrität eines Blocks digitaler Daten, wobei das Verfahren folgende Schritte umfasst:
- in einem ersten Datenblock (4) mittels eines ersten Markers (7) nach einem digitalen Identifikationsfingerabdruck des ersten Datenblocks (4) zu suchen,
- falls der Identifikationsfingerabdruck (2) des ersten Datenblocks im ersten Datenblock gefunden wird, Berechnen eines digitalen Fingerabdrucks des ersten Datenblocks durch Anwenden einer Fingerabdruck-Berechnungsfunktion auf den ersten Datenblock,
- wobei der berechnete Fingerabdruck des ersten Datenblocks einen Wert aufweist, der von jedem der Bits des ersten Datenblocks abhängt, mit Ausnahme der Bits des im ersten Datenblock gefundenen Identifikations-Fingerabdrucks (2), und
- den im ersten Datenblock gefundenen Identifikationsfingerabdruck durch Vergleich mit dem berechneten Fingerabdruck des ersten Datenblocks zu überprüfen, wobei ein fehlgeschlagener Vergleich zeigt, dass der erste Datenblock verändert wurde, seit der Identifikations-Fingerabdruck in den ersten Datenblock eingefügt wurde, oder dass der Identifikations-Fingerabdruck durch Anwendung einer anderen Fingerabdruck-Berechnungsfunktion auf den ersten Datenblock berechnet wurde.

66. **Merkmal 1.1**: ***Verfahren zur Überprüfung der Integrität eines digitalen Datenblocks, wobei das Verfahren folgende Schritte umfasst:***

    Das Merkmal 1.1 bildet die Einleitung des Anspruchs und definiert den allgemeinen Gegenstand der Erfindung als ein Verfahren zur Überprüfung der Integrität eines digitalen Datenblocks.

67. Ein Fachmann würde verstehen, dass das Ziel des Verfahrens („Überprüfung der Integrität“) darin besteht, festzustellen, ob der Inhalt eines Datenblocks seit der Erstellung oder dem Einfügen des Identifikationsfingerabdrucks verändert wurde.

68. Der Begriff „Integrität“ ist in seiner üblichen Bedeutung in der Informatik zu verstehen, d. h. als die Eigenschaft, dass die Daten nicht verfälscht oder verändert wurden.

69. Diese Auslegung steht im Übrigen im Einklang mit dem Ende von Anspruch 1.5, der vorsieht, dass ein negativer Vergleich ergibt, dass „der erste Datenblock verändert wurde“. Der primäre Zweck des Verfahrens ist somit die Überprüfung der Integrität des Inhalts (nicht die Authentifizierung eines Urhebers, der Herkunftsnachweis oder die Zertifizierung eines Unterzeichners usw.).

70. Hingegen verlangt der Anspruch nicht, dass die Lösung unabhängig vom verwendeten Format ist. Der Datenblock kann durchaus eine für ein bestimmtes Format spezifische Struktur aufweisen.

71. Wie in der Auslegung der beanstandeten Begriffe dargelegt, sei daran erinnert, dass der Ausdruck „Datenblock“ im Kontext des Patents im weiteren Sinne zu verstehen ist.

72. Zusammenfassend ist das Merkmal 1.1 so zu verstehen, dass es ein Verfahren definiert, mit dem festgestellt werden soll, ob ein digitaler Datenblock – verstanden als jede Datei, jedes Dokument oder jeder digitale Datensatz – seine Integrität bewahrt hat, d. h. nicht verändert wurde.

73. **<u>Merkmal 1.2</u>: *Suchen eines digitalen Identifikationsfingerabdrucks des ersten Datenblocks (4) in einem ersten Datenblock (4) mittels eines ersten Markers***

Das Merkmal 1.2 verlangt, dass ein digitaler Identifikationsfingerabdruck innerhalb des Datenblocks selbst gesucht wird und dass diese Suche mittels eines Referenzwerts erfolgt.

74. Dieser Schritt erfolgt vor jeder Berechnung eines Fingerabdrucks. Der Fachmann versteht daher, dass der Identifikationsfingerabdruck bereits im Datenblock vorhanden ist, wenn er den Überprüfungsvorgang beginnt, da das Verb „suchen" einen Lokalisierungsvorgang impliziert.

75. Der Schritt besteht nicht einfach darin, einen Wert auszulesen, dessen Speicherort im Voraus bekannt wäre. Das Verfahren sieht vielmehr vor, den Speicherort des Fingerabdrucks anhand eines im Datenblock vorhandenen Markierungselements („Marker") zu identifizieren.

76. Der Begriff „Marker" („repère") ist ein allgemeiner Begriff, der im Patent nicht speziell definiert ist.

77. Der Fachmann versteht daher, dass ein vorbereitender Schritt erforderlich ist, um festzustellen, wo sich der Identifikationsfingerabdruck befindet, der anschließend überprüft werden muss, wobei der gesuchte Fingerabdruck innerhalb des Datenblocks selbst vorhanden sein muss. Dieses Merkmal unterscheidet die Erfindung von Systemen des Standes der Technik, bei denen der Fingerabdruck in einer externen Datenbank oder in einer separaten Datei gespeichert ist, oder von Systemen, bei denen der Fingerabdruck zum Zeitpunkt der Überprüfung von einem Dritten bereitgestellt wird.

78. Der Fachmann versteht, dass ein Marker eine Information ist, die es ermöglicht, den Fingerabdruck im Datenblock zu lokalisieren, doch der Anspruch schreibt keine bestimmte Form vor.

79. Der Beschreibung zufolge kann der Marker daher eine Zeichenfolge, ein Tag, ein strukturiertes Feld, eine Positionsangabe oder jede andere Information sein, die den Zugriff auf den Speicherort des Fingerabdrucks ermöglicht.

80. Der Wortlaut des Anspruchs verlangt hingegen einen funktionalen Zusammenhang zwischen dem Marker und dem Speicherort des Fingerabdrucks: Der Marker muss es ermöglichen, den gesuchten Fingerabdruck zu finden.

81. Das Merkmal 1.2 verlangt nicht, dass sich die Kennung unmittelbar neben dem Fingerabdruck befindet, dass die Kennung Teil des Fingerabdrucks ist, dass die Kennung eine bestimmte Form hat oder dass die Kennung unabhängig vom Dateiformat ist.

82. Zusammenfassend ist Merkmal 1.2 so zu verstehen, dass es verlangt, dass ein zuvor in den Datenblock eingefügter digitaler Identifikationsfingerabdruck innerhalb dieses Blocks mittels einer Markierungsinformation lokalisiert wird, die es ermöglicht, dessen Position zu bestimmen. Die „erste Markierung“ ist eine Information, die dazu dient, den Identifikationsfingerabdruck zu lokalisieren, ohne dass der Anspruch eine bestimmte Form dieser Markierung oder deren genaue Position im Datenblock vorschreibt.

83. **Merkmal 1.3**: ***Wenn der Identifikationsfingerabdruck (2) des ersten Datenblocks im ersten Datenblock gefunden wird, Berechnung eines digitalen Fingerabdrucks des ersten Datenblocks durch Anwendung einer Fingerabdruckberechnungsfunktion auf den ersten Datenblock,***

Das Merkmal 1.3 beschreibt den Schritt der Neuberechnung des Fingerabdrucks, der anschließend zur Überprüfung dient. Nach dem Auffinden des Identifikations-Fingerabdrucks gemäß Merkmal 1.2 berechnet das Verfahren mittels einer Fingerabdruck-Berechnungsfunktion einen neuen Fingerabdruck des Datenblocks.

84. Die bedingte Formulierung „sofern der Identifikationsfingerabdruck gefunden wird“ besagt, dass die in Merkmal 1.3 vorgesehene Berechnung nur dann erfolgt, wenn im Suchschritt gemäß Merkmal 1.2 ein Identifikationsfingerabdruck im Datenblock lokalisiert werden konnte.

85. Der Anspruch beschreibt somit eine logische Abfolge von Schritten: Suche nach dem Fingerabdruck; Lokalisierung des Fingerabdrucks; Berechnung eines neuen Fingerabdrucks; Vergleich.

86. Der Anspruch verlangt die Berechnung eines neuen Fingerabdrucks („Berechnung eines digitalen Fingerabdrucks des ersten Datenblocks“). Der Fachmann versteht, dass es sich dabei um einen Wert handelt, der während des Überprüfungsverfahrens ermittelt wird, um als Referenz für den in Merkmal 1.5 vorgesehenen Vergleich zu dienen.

87. Durch die Angabe „unter Anwendung einer Fingerabdruck-Berechnungsfunktion“ beschränkt sich der Anspruch nicht ausdrücklich auf eine bestimmte Funktion oder die Art dieser Funktion.

88. Der Anspruch erwähnt lediglich eine „Fingerabdruck-Berechnungsfunktion“ und bleibt in dieser Phase technologisch offen. Zusammenfassend ist Merkmal 1.3 so zu verstehen, dass es verlangt, dass, sobald ein Identifikationsfingerabdruck im Datenblock lokalisiert wurde, ein neuer Fingerabdruck des Datenblocks durch Anwendung einer Fingerabdruck-Berechnungsfunktion auf den Datenblock berechnet wird. Dieser Schritt liefert den Referenzwert, der bei der in Merkmal 1.5 vorgesehenen nachfolgenden Überprüfung verwendet werden soll. Der Anspruch schreibt weder einen bestimmten Algorithmus vor, noch beschränkt er die Berechnungsfunktion ausdrücklich auf eine bestimmte Hash-Funktion. Dies wird in [0005] des Patents bestätigt, wo ausdrücklich darauf hingewiesen wird, dass „diese Funktion eine Hash-Funktion sein kann, aber nicht notwendigerweise“.

89. **<u>Merkmal 1.4</u>: *Der berechnete Fingerabdruck des ersten Datenblocks hat einen Wert, der von jedem der Bits des ersten Datenblocks abhängt, wobei die Bits des Identifikationsfingerabdrucks (2), der im ersten Datenblock gefunden wurde, ausgeschlossen werden.***

Das Merkmal 1.4 präzisiert, wie der berechnete Fingerabdruck aus Merkmal 1.3 zu ermitteln ist.

90. Es verlangt, dass der Wert des berechneten Fingerabdrucks vom gesamten Inhalt des Datenblocks abhängt, mit Ausnahme der Bits, die dem zuvor im Datenblock gefundenen Identifikationsfingerabdruck entsprechen.

91. „wobei der berechnete Fingerabdruck […] einen Wert hat, der von jedem einzelnen Bit des ersten Datenblocks abhängt“: Der Fachmann versteht, dass der Fingerabdruck aus dem Inhalt des Datenblocks so berechnet werden muss, dass eine Änderung eines in die Berechnung einbezogenen Bits den erhaltenen Wert verändern kann.

92. Der Ausdruck „abhängig von jedem der Bits“ bedeutet jedoch nicht zwangsläufig, dass eine mathematische Beziehung „jedes einzelne Bit“ berücksichtigen muss. Er drückt vielmehr aus, dass sich die Berechnung auf die Gesamtheit der berücksichtigten Daten bezieht, „unter Ausschluss der Bits des Identifikationsabdrucks“.

93. Diese letzte Einschränkung ist wesentlich: Der Anspruch schreibt vor, dass die Bits, aus denen sich der in Schritt 1.2 ermittelte Identifikationsfingerabdruck zusammensetzt, nicht in die Berechnung des in Schritt 1.3 ermittelten Fingerabdrucks einfließen dürfen.

94. Der Fachmann versteht sofort den Grund für diesen Ausschluss: Würde der Identifikationsfingerabdruck in die Berechnung einbezogen, würde das Einfügen dieses Fingerabdrucks selbst den Inhalt verändern, von dem der berechnete Fingerabdruck abhängt, was den in Merkmal 1.5 vorgesehenen späteren Vergleich verhindern würde. Der Anspruch löst somit das Problem der Selbstreferenz, indem er den Bereich, der den eingefügten Fingerabdruck enthält, aus der Berechnung ausschließt.

95. Die wichtigste Frage ist, was genau ausgeschlossen wird, d. h. der Umfang des Ausschlusses.

96. Der Wortlaut von Anspruch 1 bezieht sich ausdrücklich auf die Bits des gefundenen Identifikationsfingerabdrucks, und für sich genommen bezeichnet dieser Wortlaut ausschließlich die Bits, die dem Fingerabdruck selbst entsprechen. Er erwähnt keinen weiter gefassten Bereich, keine zugehörigen Metadaten, keine zusätzlichen Felder oder Strukturen, die den Fingerabdruck enthalten.

97. Um diesen Punkt besser zu verstehen, sollte man ihn im Lichte der abhängigen Ansprüche 10 und 11 lesen, ohne Anspruch 1 einzuschränken, sowie im Zusammenhang mit bestimmten Abschnitten der Beschreibung.

98. Tatsächlich sehen die Ansprüche 10[1]und 11[2]ausdrücklich Metadaten vor, die einen variablen Teil umfassen, der von der Berechnung ausgeschlossen werden kann und in dem der Fingerabdruck gespeichert werden kann.

99. Ein Fachmann, der das gesamte Patent liest, versteht daher, dass der Ausschluss nicht notwendigerweise in allen Ausführungsformen allein auf den binären Wert des Fingerabdrucks beschränkt ist. Die Ansprüche 10 und 11 lehren vielmehr, dass auch größere Bereiche variabler Daten von der Berechnung ausgeschlossen werden können.

100. Das Merkmal 1.4 ist unter Berücksichtigung sowohl seines Wortlauts, der ausdrücklich auf den Ausschluss der Bits des Identifikationsfingerabdrucks abzielt, als auch der Beschreibung und der abhängigen Ansprüche 10 und 11 auszulegen, aus denen hervorgeht, dass das Patent auch Ausführungsformen mit umfangreicheren variablen Bereichen vorsieht.

101. Das Merkmal 1.4 darf daher nicht so ausgelegt werden, dass es zwangsläufig einen Ausschluss vorschreibt, der sich ausschließlich auf die Zeichenkette beschränkt, die den Fingerabdruck darstellt.

102. Zusammenfassend verlangt Merkmal 1.4, dass der berechnete Fingerabdruck aus dem Inhalt des Datenblocks ermittelt wird, wobei die Bits, die dem zuvor lokalisierten Identifikationsfingerabdruck entsprechen, von der Berechnung ausgeschlossen werden. Dieser Ausschluss ermöglicht die Überprüfung eines in den Datenblock eingefügten Fingerabdrucks, ohne dass dessen Vorhandensein das Berechnungsergebnis beeinflusst. Im Lichte der Beschreibung und der Ansprüche 10 und 11 gelesen, schließt dieses Merkmal nicht aus, dass in bestimmten Ausführungsformen des Patents auch variable Daten, die mit dem Fingerabdruck verbunden sind, von der Berechnung ausgeschlossen werden können. Im Gegenteil, es besteht kein Risiko, andere, nicht variable Daten in die Berechnung einzubeziehen, da diese eben nicht verändert werden können und es – aufgrund ihrer Unveränderlichkeit – daher kein Risiko gibt, dass die Daten beschädigt werden.

103. **Merkmal 1.5**: ***Überprüfung des im ersten Datenblock gefundenen Identifikations-Fingerabdrucks durch Vergleich mit dem berechneten Fingerabdruck des ersten Datenblocks, wobei ein falscher Vergleich darauf hindeutet, dass der erste Datenblock seit dem Einfügen des Identifikations-Fingerabdrucks in den ersten Datenblock verändert wurde oder dass der Identifikations-Fingerabdruck unter Anwendung einer anderen Fingerabdruck-Berechnungsfunktion berechnet wurde.***

Merkmal 1.5 definiert den letzten Schritt des Verfahrens. Nachdem der Identifikations-Fingerabdruck lokalisiert (Merkmal 1.2) und ein neuer Fingerabdruck berechnet wurde (Merkmale 1.3 und 1.4), führt das System eine Überprüfung durch, indem

[1] *10.1 Verfahren nach einem der Ansprüche 1 bis 9, wobei einer der Datenblöcke Metadaten*
10.2, der einen variablen Teil umfasst, der bei der auf den Datenblock angewendeten Fingerabdruckberechnung zur Berechnung des Identifikationsfingerabdrucks des Datenblocks ausgeschlossen wird.

[2] *11. Verfahren nach Anspruch 10, wobei sich der Identifikationsfingerabdruck des Datenblocks im variablen Teil*

eines Identifikations-Metadatenblocks befindet.

durch Vergleichen der beiden Werte. Dieser Schritt stellt das Ergebnis des in dem Anspruch beschriebenen Integritätsprüfmechanismus dar.

104. Der Anspruch sieht weder eine Überprüfung des Dokuments im Allgemeinen noch eine Überprüfung de_ s Autors des Dokuments vor: Überprüft wird speziell der im Datenblock enthaltene Identifikationsfingerabdruck.

105. Der Fachmann versteht, dass sich die Überprüfung auf die Übereinstimmung zwischen dem in der Datei gespeicherten Fingerabdruck und dem aktuellen Inhalt der Datei bezieht.

106. Der zentrale Begriff dieses Merkmals ist das Verb „vergleichen". Im üblichen Sinne bedeutet „vergleichen", zwei Werte miteinander abzugleichen, um festzustellen, ob sie übereinstimmen oder nicht.

107. Der Anspruch präzisiert weder die genaue Form des Vergleichs noch die gegebenenfalls erforderlichen vorbereitenden Schritte oder den zur Durchführung dieses Vergleichs verwendeten Algorithmus. Das erwartete Ergebnis ist hingegen klar definiert: Es geht darum festzustellen, ob der gefundene Fingerabdruck mit dem neu berechneten Fingerabdruck übereinstimmt (d. h. derselbe ist wie dieser).

108. Ein Fachmann würde dieses Merkmal so interpretieren, dass lediglich das Vorhandensein von zwei Werten gefordert wird:
den im Datenblock gefundenen Fingerabdruck; den bei der Überprüfung berechneten Fingerabdruck.
Diese beiden Werte werden anschließend miteinander verglichen, um ihre Übereinstimmung zu überprüfen.

109. Zusammenfassend verlangt Merkmal 1.5, dass eine Überprüfung durchgeführt wird, bei der der im Datenblock gefundene Identifikationsfingerabdruck mit dem gemäß den Merkmalen 1.3 und 1.4 neu berechneten Fingerabdruck abgeglichen wird, um festzustellen, ob diese beiden Werte übereinstimmen. Eine Abweichung zwischen den beiden Werten deutet entweder auf eine Änderung des Datenblocks nach dem Einfügen des Identifikations-Fingerabdrucks oder auf die Verwendung einer anderen Berechnungsfunktion hin. Der Anspruch verlangt einen Vergleich zwischen dem gefundenen und dem berechneten Fingerabdruck, ohne die gegebenenfalls vor diesem Vergleich erforderlichen vorbereitenden Schritte ausdrücklich zu definieren.

GÜLTIGKEIT DES PATENTS

1) Anspruch 1 (Patent in der erteilten Fassung)

110. **Zur Gegenstandserweiterung (Art. 123 (2) EPÜ)**

Rechtlicher Rahmen:

Eine Gegenstandserweiterung liegt vor, wenn sich der Anspruch in der erteilten Fassung über den Inhalt der eingereichten Anmeldung hinaus erstreckt. Um festzustellen, ob eine Gegenstandserweiterung vorliegt, muss das Gericht daher zunächst ermitteln, was ein Fachmann unter Rückgriff auf sein Allgemeinwissen und aus objektiver Sicht zum Zeitpunkt der Einreichung unmittelbar und eindeutig aus der Gesamtheit der eingereichten Anmeldung ableiten würde. Der Gegenstand

implizit offenbart, d. h. derjenige, der eine klare und eindeutige Folge des ausdrücklich Erwähnten darstellt, muss ebenfalls als Teil dieses Inhalts betrachtet werden (UPC_CoA_764/2024, 2. Oktober 2025, expert klein GmbH gegen Seoul Viosys Co).

111. Argumente der Beklagten:

Die Beklagten machen geltend, dass das erteilte Patent EP'070 über den Inhalt der eingereichten Anmeldung hinausgeht, und stützen sich dabei auf folgende Argumente:

- Ein Teilmerkmal des Merkmals 1.5 von Anspruch 1 (am Ende von 1.5 erwähnt und unten unterstrichen) wurde erst im Laufe der Patentprüfung vor der Erteilung in Anspruch 1 aufgenommen und war ursprünglich nicht offenbart. (vgl. Anlage DTMV 3.2):

- „den im ersten Datenblock gefundenen Identifikationsfingerabdruck durch Vergleich mit dem berechneten Fingerabdruck des ersten Datenblocks zu überprüfen, wobei ein fehlgeschlagener Vergleich darauf hindeutet, dass der erste Datenblock seit dem Einfügen des Identifikations-Fingerabdrucks in den ersten Datenblock verändert wurde oder dass der Identifikations-Fingerabdruck durch Anwendung einer anderen Fingerabdruck-Berechnungsfunktion auf den ersten Datenblock berechnet wurde."

112. Dieses Untermerkmal des Merkmals 1.5, das in der ursprünglichen Anmeldung fehlte und in 1.5 hinzugefügt wurde, stellt nach Ansicht der Beklagten eine Ausweitung des Gegenstands des Patents EP'070 über den Inhalt der Anmeldung in der eingereichten Fassung hinaus dar.

113. Nach Ansicht von KEEEX wurden die beiden Merkmale hinzugefügt, um die Wirkung des genannten Vergleichs zu präzisieren, der sich auf den im Datenblock gefundenen Identifikationsfingerabdruck und den aus diesem Datenblock berechneten Fingerabdruck bezieht, nämlich:

„ein falscher Vergleich, der zeigt, dass der erste Datenblock verändert wurde, seit der Identifikationsfingerabdruck in den ersten Datenblock eingefügt wurde",

„ein falscher Vergleich, der zeigt, dass der Identifikationsfingerabdruck durch Anwendung einer anderen Fingerabdruckberechnungsfunktion auf den ersten Datenblock berechnet wurde".

114. KEEEX vertritt die Auffassung, dass diese beiden Merkmale lediglich die Möglichkeiten verdeutlichen, die zu einem falschen Vergleich führen können. Es scheint keine weiteren zu geben. Denn die elementare Logik gebietet, dass man zur Überprüfung einer Berechnung diese wiederholt und die Konsistenz der Ergebnisse überprüft. Treten bei diesen Ergebnissen Abweichungen auf, bedeutet dies, dass die beiden Berechnungen nicht identisch sind. Damit zwei Berechnungen identisch sind, müssen zudem zwei Bedingungen erfüllt sein: Die Daten, auf die sich diese Berechnungen beziehen, müssen identisch sein (Merkmal 1), und die bei diesen beiden Berechnungen angewandte Vorgehensweise muss dieselbe sein (Merkmal 2).

115. In Absatz [0062] wird auf andere Weise beschrieben, wie die beanspruchte Überprüfung durchgeführt wird: „Das Verfahren ermöglicht es, durch Entfernen des im Datenblock enthaltenen Fingerabdrucks den Wert des Datenblocks wiederherzustellen, aus dem der Fingerabdruck vermutlich berechnet wurde, und anschließend durch Vergleich des entfernten Fingerabdrucks mit dem berechneten Fingerabdruck zu überprüfen, ob diese Annahme richtig oder falsch ist."

116. Diese Überprüfung entspricht genau dem Anwendungsbereich der im vorigen Absatz erwähnten elementaren Logik, da es darum geht, dieselbe Berechnung auf vermeintlich identische Daten anzuwenden und die erhaltenen Ergebnisse zu vergleichen.

117. Merkmal 1 taucht fast wörtlich am Ende des Absatzes [0062] auf : „Ist der Vergleich falsch, ist der Datenblock 4 beschädigt oder wurde einfach verändert." Es lässt sich ebenfalls feststellen, dass, wenn der Datenblock beschädigt wurde, dies bedeutet, dass er verändert wurde.

118. Was Merkmal 2 betrifft, so beziehen sich die Absätze [0071] und [0072] des Patents EP 070 auf die Bedingung hinsichtlich des Verfahrens, da sie die Speicherung und Bereitstellung einer Information betreffen, die das Verfahren spezifiziert, mit dem der Überprüfungsvorgang gewährleistet wird. Tatsächlich heißt es in Absatz [0071], dass verschiedene Berechnungen oder Algorithmen zur Berechnung des Fingerabdrucks eingesetzt werden können und dass der Fingerabdruck mit dem Namen des Berechnungsalgorithmus verknüpft werden kann, der zur Erzeugung des Fingerabdrucks verwendet wurde. In Absatz [0072] wird präzisiert, dass, wenn der Fingerabdruck 2 an sich nicht die Art der Berechnung oder des Berechnungsalgorithmus angibt, mit dem er erzeugt wurde, diese Information in Metadaten bereitgestellt werden kann, die in den Datenblock eingefügt sind.

119. Somit leiten sich nach Ansicht des Anmelders die beiden Merkmale, die dem Anspruch 1 hinzugefügt wurden, unmittelbar und eindeutig aus dem eingereichten Wortlaut des Patents EP 070, aus allgemeinem Fachwissen und aus elementarer Logik ab.

120. <u>Standpunkt des Gerichts:</u>

Es ist unstreitig, dass die Hinzufügung des letzten Untermerkmals von Anspruch 1.5 mit folgendem Wortlaut: *„oder dass der Identifikationsfingerabdruck durch Anwendung einer anderen Fingerabdruck-Berechnungsfunktion berechnet* wurde", während der Erteilungsphase vorgenommen wurde. Es handelt sich aus den in der Verteidigung angeführten Gründen um eine unzulässige Hinzufügung, da sie eine Erweiterung des Schutzumfangs gegenüber der eingereichten Anmeldung bewirkt. Tatsächlich wurde in der eingereichten Anmeldung nicht offenbart, dass ein falscher Vergleich an sich die Verwendung einer anderen Berechnungsfunktion offenbaren könnte. Anspruch 1 geht somit über den Inhalt der eingereichten Anmeldung hinaus.

121. Daraus folgt, dass Anspruch 1 des erteilten Patents gemäß Art. 123 (2) des Münchner Übereinkommens (EPÜ) nichtig ist.

122. Das Gericht stellt jedoch fest, dass der von KEEEX vorgeschlagene Hilfsantrag Nr. 11 (RS 11) zur Änderung des Patents (Schriftstück KEEEX 29.11) diesen

Mangel behoben hat, indem der Zusatz des beanstandeten Untermerkmals gestrichen wurde. RS 11 lautet nämlich wie folgt:

REVENDICATIONS

1. Procédé de vérification de l'intégrité d'un bloc de données numériques, le procédé comprenant des étapes consistant à :

rechercher, dans un premier bloc de données (4), une empreinte numérique d'identification du premier bloc de données (4), au moyen d'un premier repère (7),

si l'empreinte (2) d'identification du premier bloc de données est trouvée dans le premier bloc de données, calculer une empreinte numérique du premier bloc de données en appliquant une fonction de calcul d'empreinte au premier bloc de données, l'empreinte calculée du premier bloc de données ayant une valeur dépendant de chacun des bits du premier bloc de données en excluant les bits de l'empreinte d'identification (2) trouvée dans le premier bloc de données, et

vérifier l'empreinte d'identification trouvée dans le premier bloc de données en la comparant à l'empreinte calculée du premier bloc de données, une comparaison fausse révélant que le premier bloc de données a été modifié depuis que l'empreinte d'identification a été insérée dans le premier bloc de données~~, ou que l'empreinte d'identification a été calculée en appliquant au premier bloc de données une autre fonction de calcul d'empreinte~~.

123. Vorsorglich beabsichtigt das Gericht, die Gültigkeit des erteilten Patents im Hinblick auf die Neuheit (Art. 54 EPÜ) zu prüfen.

124. Die Beklagten haben verschiedene Dokumente geltend gemacht, insbesondere das mit dem Titel
„KANAI“ (oder „D5“, gemäß den Schriftsätzen von ADOBE).

125. **<u>Zur Neuheit (Art. 54 Abs. 1 EPÜ)</u>**

126. <u>Rechtlicher Rahmen:</u>

Gemäß Artikel 54 (1) EPÜ gilt eine Erfindung als neu, wenn sie nicht zum Stand der Technik gehört. Eine technische Lehre gehört nicht zum Stand der Technik, wenn sie sich durch mindestens eines ihrer bekannten Merkmale von dem unterscheidet, was im Stand der Technik bereits bekannt ist. Als durch ein Dokument des Stands der Technik vorweggenommen gilt nur das, was der Fachmann unter Rückgriff auf sein allgemeines Wissen zum Zeitpunkt der Einreichung oder der maßgeblichen Priorität direkt und eindeutig aus diesem einzigen Dokument ableiten würde (vgl. UPC_CoA_182/2024, 25. September 2024, Mammut gegen Ortovox; UPC_CoA_382/2024, 14. Februar 2025, Abbott gegen Sibio).

127. <u>In Bezug auf KANAI:</u>

Vorstellung des als „KANAI“ bezeichneten Dokuments aus dem Stand der Technik

Es handelt sich um die am 28. Juni 2005 veröffentlichte Patentanmeldung US 2005/0166044 A1 mit dem Titel „Digital measurement apparatus and image measurement apparatus“. (vgl. Anlage DMTV 4.5, D5), in deren Zusammenfassung es heißt: *„Eine digitale Messvorrichtung misst ein physikalisches Messobjekt, versieht die Messdaten einer so gemessenen physikalischen Größe mit einer digitalen Signatur der Public-Key-Kryptografie und verwaltet die Messdaten. Die Vorrichtung generiert mindestens ein Schlüsselpaar aus einem öffentlichen*

Schlüssel und eines privaten Schlüssels, die für die digitale Signatur der Public-Key-Kryptografie verwendet werden sollen, mittels eines Schlüsselgenerierungsalgorithmus“.

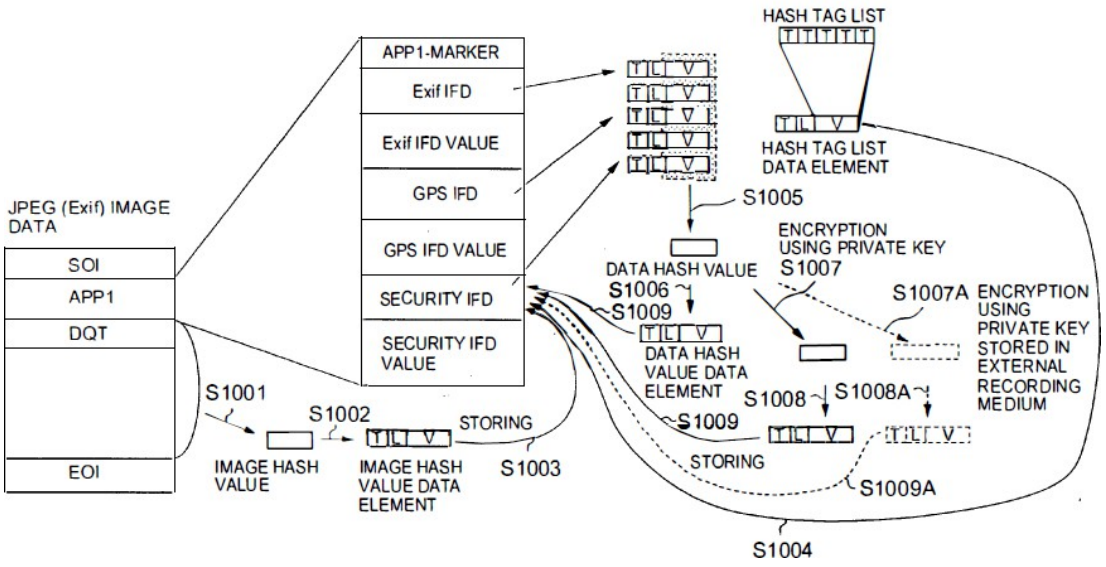
Dieses Dokument betrifft ein System, das dazu dient, die Integrität und Authentizität digitaler Messdaten zu gewährleisten, insbesondere von Bildern, die von Geräten wie Digitalkameras, Scannern oder medizinischen Geräten erzeugt werden. Die Erfindung zielt darauf ab, die Nachteile von Systemen zu beheben, bei denen die digitale Signatur in einer von der Datendatei getrennten Datei gespeichert wird, was zu einer Entkopplung zwischen beiden führen kann.

128. Die Kernidee von KANAI besteht darin, die für die Überprüfung erforderlichen Hash-Werte und digitalen Signaturen direkt in die Datei zu integrieren. Das System berechnet zunächst einen Hash-Wert der zu schützenden Daten, insbesondere des Hauptinhalts des Bildes. Dieser Hash-Wert wird anschließend in einer speziellen, in die Datei integrierten Datenstruktur gespeichert. Ein zweiter Hashwert kann aus mehreren Elementen berechnet werden, die als wichtig für die Glaubwürdigkeit des Dokuments angesehen werden, wie beispielsweise das Erstellungsdatum, die Identität des Benutzers, verschiedene Metadaten oder auch der erste Hashwert. Dieser zweite Wert wird anschließend mit einem privaten Schlüssel verschlüsselt, um eine digitale Signatur zu erzeugen.

129. Im speziellen Fall des JPEG/Exif-Formats sieht KANAI die Erstellung eines Sicherheits-Metadatenbereichs („Security IFD“) innerhalb der Bilddatei vor. Dieser Bereich enthält insbesondere einen Hash-Wert des Bildes („Image Hash Value“), eine Liste der geschützten Elemente („Hash Tag List“), einen globalen Hash-Wert („Data Hash Value“) sowie eine oder mehrere digitale Signaturen. Alle diese Informationen werden direkt in der Bilddatei gespeichert**.**

130. In Abbildung 10 veranschaulicht das KANAI-Dokument, wie die Sicherheitsinformationen in eine Bilddatei im JPEG/Exif-Format integriert werden:

FIG.10



131. Abbildung 10 zeigt, dass die Bilddatei neben den eigentlichen Bilddaten eine spezielle Struktur namens Security IFD (Security Image File Directory) enthält, die dazu dient, die Informationen aufzunehmen, die zum Schutz der Integrität der Datei verwendet werden. Diese Struktur ist direkt in die JPEG/Exif-Datei innerhalb des APP1-Segments integriert.

132. Der Vorgang beginnt mit der Berechnung eines ersten Hash-Werts, des sogenannten „Image Hash Value“, der aus dem Hauptdatenstrom des Bildes ermittelt wird. Dieser Wert wird in einem speziellen Datenelement namens „Image Hash Value Data Element“ gespeichert. Die Abbildung zeigt anschließend die Erstellung einer „Hash Tag List“, d. h. einer Liste, die die Elemente der Datei identifiziert, die bei späteren Überprüfungen berücksichtigt werden müssen.

133. Anhand der in dieser Liste aufgeführten Elemente berechnet das System einen zweiten Hash-Wert, den sogenannten „Data Hash Value“. Dieser Wert wird anschließend in einem „Data Hash Value Data Element“ gespeichert. Der „Data Hash Value“ wird dann mit einem privaten Schlüssel verschlüsselt, um eine „Data Signature“ zu erzeugen, die ebenfalls in der „Security IFD“-Struktur gespeichert wird.

134. Die Abbildung verdeutlicht somit, dass die Datei gleichzeitig einen eigenständigen Hashwert (Image Hash Value), einen globalen Hashwert (Data Hash Value) und eine digitale Signatur (Data Signature) enthält, wobei all diese Informationen in einer Metadatenstruktur zusammengefasst sind, die in die Datei selbst integriert ist.

135. Diese Abbildung ist von besonderer Bedeutung, da sie explizit die Einbettung eines Hash-Werts in die Datei zeigt, der den geschützten Inhalt repräsentiert – unabhängig von der digitalen Signatur.
Somit scheint es, dass KANAI bereits einen Mechanismus offenlegt, der einen in die Datei integrierten Hashwert beinhaltet, der in einem dafür vorgesehenen Bereich gespeichert und anschließend beim Integritätsprüfungsverfahren verwendet wird. Die Absätze [0049] bis [0057] beschreiben die Erzeugung und Speicherung dieser Werte, während die Absätze [0062] und [0063] deren Auslesen, Neuberechnung und Vergleich während der Überprüfung darlegen.

136. Dieses Dokument misst der Frage des Einfügens der Signatur in die Datei besondere Bedeutung bei. Es erläutert, dass das Hinzufügen einer Signatur den Inhalt der Datei verändert und somit die Berechnung des Fingerabdrucks beeinflussen könnte. Um dieses Problem zu lösen, sieht KANAI insbesondere vor, dass vorab ein Bereich für die Signatur oder bestimmte Sicherheitsdaten reserviert wird, der bei der Berechnung der Hash-Werte ignoriert oder speziell behandelt wird.

137. **Laut ADOBE:** (vgl. Seiten 23 bis 26 der Zusammenfassung der Klagegründe)

ADOBE stützt seine Darlegung auf bestimmte Absätze der Beschreibung der KANAI-Anmeldung, und zwar auf folgende:

- [0063] *Zunächst wird der Wert im Wertbereich des Daten-Signatur-Datenelements aus den JPEG- (Exif-) Bilddaten ausgelesen. Anschließend wird die so erhaltene Datensignatur mit dem öffentlichen Schlüssel der Digitalkamera entschlüsselt. Dadurch wird der Daten-Hashwert ermittelt. (…) Dann wird festgestellt, ob der so erhaltene Daten-Hashwert übereinstimmt (…)*
- *Der geschützte Bilddatenstrom wird gelesen … und mittels des Hash-Algorithmus (SHA-1, MD5 oder dergleichen) komprimiert. Auf diese Weise wird der Hash-Wert berechnet. (…) Stimmen sie nicht miteinander überein, wird festgestellt, dass die Bilddaten in irgendeiner Weise verändert wurden. (…)*

Freie Übersetzung ins Deutsche:

- [0063] Zunächst wird der im Wertteil des Signaturdatenelements enthaltene Wert aus den JPEG-Bilddaten (Exif) ausgelesen. Anschließend wird die so erhaltene Signatur mit Hilfe des öffentlichen Schlüssels der Digitalkamera entschlüsselt. Dadurch wird der Hashwert der Daten ermittelt. (…) Anschließend wird geprüft, ob der so erhaltene Hashwert (...)
- Der geschützte Bilddatenstrom wird eingelesen … und mithilfe des Hash-Algorithmus (SHA-1, MD5 oder ähnliches) komprimiert. Der Hashwert wird somit berechnet. (...) Stimmen diese nicht überein, wird festgestellt, dass die Bilddaten in irgendeiner Weise verändert wurden. (…)

138. ADOBE vertritt die Auffassung, dass die auf einem „Marker“ basierende Position des integrierten digitalen Identifikationsabdrucks über einen Tag-/Typ-Indikator offengelegt wird:

- [0056] *Ein TLV-Datenelement wird (in Schritt S1008) unter Verwendung einer Tag-Nummer (im Tag-Teil „T“ geschrieben) erzeugt, die angibt, dass dieses TLV-Datenelement zur Datensignatur gehört. Dieses TLV-Datenelement enthält die Datensignatur in seinem Wertteil. Das so erzeugte TLV-Datenelement wird als Datensignatur-Datenelement bezeichnet.*

Freie Übersetzung ins Deutsche:

- [0056] Ein TLV-Datenelement wird (in Schritt S1008) mithilfe einer Tag-Nummer (die im Tag-Teil „T“ steht) erzeugt, die angibt, dass dieses TLV-Datenelement zur Datensignatur gehört. Dieses TLV-Datenelement enthält die Datensignatur in seinem Wertteil. Das so erzeugte TLV-Datenelement wird als „Datensignatur“-Datenelement bezeichnet.

139. Dementsprechend weist ADOBE darauf hin, dass US'044 – KANAI – D5 ebenfalls die Erzeugung eines überprüfbaren Datenblocks offenbart, indem zunächst ein Einfügeplatz im ursprünglichen Datenblock reserviert/identifiziert und anschließend die berechnete Signatur/der Hashwert an dieser Stelle eingebettet wird:

- [0038] *(…) ein Bereich zum Einbetten der digitalen Signatur wird zuvor in der Bilddatendatei reserviert, dieser Bereich wird zuvor mit vorgegebenen Werten gefüllt, ein Hash-Wert der gesamten Daten wird berechnet, die digitale Signatur wird erzeugt, und anschließend wird die erzeugte digitale Signatur in den zuvor reservierten Bereich eingebettet.*

Freie Übersetzung ins Deutsche:

- [0038] (…) In der Bilddatendatei wird zuvor ein Bereich für die Einbettung der digitalen Signatur reserviert; dieser Bereich wird zuvor mit vorgegebenen Werten gefüllt, ein Hashwert der gesamten Daten wird berechnet, die digitale Signatur wird erzeugt, und anschließend wird die erzeugte digitale Signatur in den zuvor reservierten Bereich eingebettet.

140. Laut ADOBE stellt KANAI einen Stand der Technik für Anspruch 1 dar, selbst nach der unzulässig restriktiven Auslegung der Klägerin, die den „Identifikationsabdruck" auf einen rohen, unverschlüsselten Hash-Wert reduziert. In seiner zweiten Ausführungsform berechnet KANAI einen „Bild-Hashwert" mittels eines Algorithmus wie SHA-1 oder MD5, fügt ihn in die JPEG/Exif-Datei innerhalb eines speziell gekennzeichneten TLV-Datenelements ein und überprüft ihn anschließend durch Vergleich mit einem neu berechneten Hashwert des geschützten Bilddatenstroms. KANAI unterscheidet diesen Bild-Hashwert vom „Daten-Hashwert" und von der übergeordneten „Datensignatur". Das Vorhandensein dieser zusätzlichen Mechanismen beeinträchtigt daher in keiner Weise die vollständige Offenlegung des Roh-Hash-Teilprozesses. [Quellen: Schriftsatz Nr. 1, § 4.2.2.1.5, S. 77–81, Abs. 149–159. Schriftsatz Nr. 2, § 3.6, S. 71–80, Abs. 257–306.
Schriftsatz Nr. 3, § 2.4.6, S. 50–52, Abs. 140–145.]

141. ADOBE weist zudem darauf hin, dass die eigene Analyse von KANAI durch die Klägerin den wesentlichen Inhalt dieser Korrespondenz bestätigt: Sie räumt ein, dass der Hashwert „mithilfe eines Index im SOI-EOI-Datenblock gesucht und gefunden werden kann" und dass diese Suche dazu dient, den für den Vergleich bestimmten Wert zu erhalten. Ihre Einwände konzentrieren sich somit auf den Ausschluss der Bits aus dem gefundenen Fingerabdruck (Merkmal 1.4). [Quellen: Schriftsatz Nr. 2, § 3.6, S. 71–
80, Abs. 257–306. Schriftsatz Nr. 3, § 2.4.6, S. 50–51, Abs. 140–142. Einwand der Klägerin: Erwiderung vom 5. Juni 2026, § III.4.4.1.5.]

142. **Nach Angaben von OPENAI:** (vgl. § 74 bis 84, Seite 27, Zusammenfassung der Klagegründe)

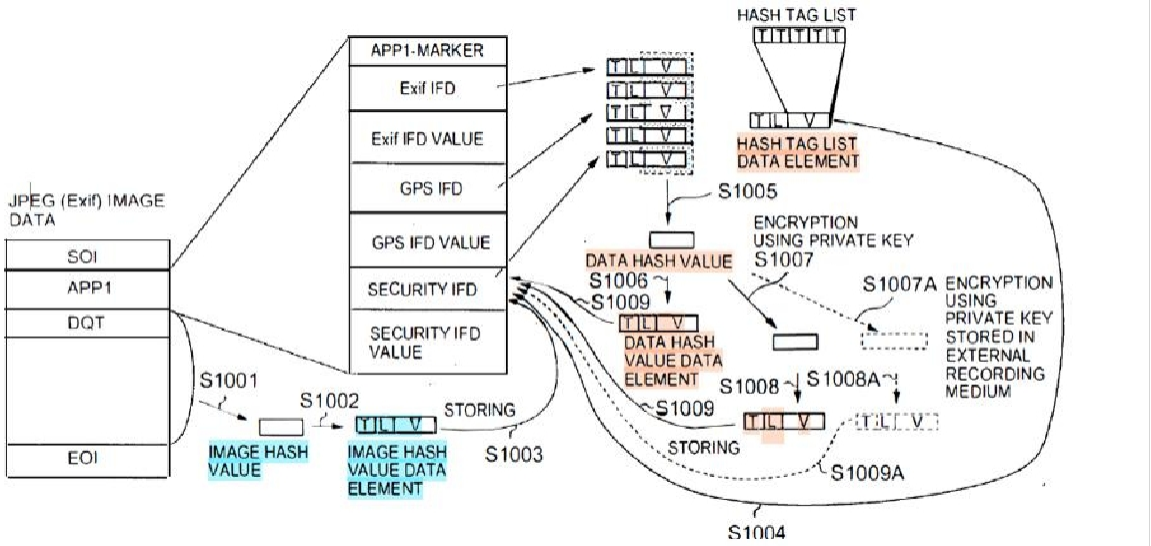
Das Dokument KANAI, das sich insbesondere auf Digitalkameras bezieht, erläutert, dass es im Stand der Technik bekannt war, einen im Gerät gespeicherten privaten Schlüssel zur Berechnung einer digitalen Signatur des Fotos zu verwenden, wobei die Signatur anschließend zusammen mit dem Foto auf einem Datenträger gespeichert wurde und der entsprechende öffentliche Schlüssel die Überprüfung des Fotos ermöglichte. Da jedoch die Bilddatei und die Signatur getrennt waren (vgl. Abs. [0005] und [0006]), konnte es vorkommen, dass die Zuordnung zwischen diesen beiden Elementen nicht gewährleistet war, was wiederum dem gleichen Problem wie im Patent entspricht.

143. OpenAI bezieht sich auf die zweite beschriebene Ausführungsform im Hinblick auf das Exif-Bildformat (siehe Abb. 9), das verschiedene Bereiche definiert: (i) einen Bereich, der sich vom Anfang des als DQT bezeichneten Bereichs bis zum Ende des Bereichs erstreckt, der dem EOI-Bereich vorausgeht; dies ist der Bereich, in dem die zu schützenden Informationen gespeichert sind; (ii) einen APP-Bereich, der bestimmte Metadaten enthält, darunter insbesondere einen „Security-IFD"-Bereich,

der aus einer Sammlung von Tags zur Beschreibung der Informationen von

Sicherheit sowie die Exif-IFD- und GPS-IFD-Felder, die Informationen enthalten, die zur Verbesserung der Glaubwürdigkeit der Daten dienen, beispielsweise die Aufnahmebedingungen und den Aufnahmeort des Fotos (vgl. US 044, Abs. [0047])

144. Nach Angaben der Beklagten wird das Verfahren zur Erzeugung und Signierung eines Bildes im Exif-Format in Abb. 10 von D5 (KANAI) veranschaulicht, die von OPENAI wie folgt kommentiert wird:



145. Laut OPENAI beschreibt US 044 angesichts dieser in Abb. 10 von KANAI dargestellten Ausführungsform beschreibt US 044 die Erzeugung eines Bilddatenblocks (rot umrandet), der zu schützende Daten (blau umrandet) enthält, für die ein Hash (blau hervorgehoben) berechnet und in ein TLV-Element (orange hervorgehoben) eingefügt wird, das ein „T"-Tag enthält. Dieses TLV-Element wird in den Bereich „security IFD" (orange umrandet) eingefügt, der wiederum im Bereich APP1 (grün umrandet) enthalten ist, der wiederum im Datenblock (rot) enthalten ist. Die Überprüfung besteht darin, den Hash aus dem TLV-Element zu extrahieren, einen Hash der zu schützenden Daten zu berechnen und die beiden Hash-Werte zu vergleichen. (§ 79 Zusammenfassung der Klagegründe von OPENAI)

146. **Antwort von KEEEX zur Anfechtung des Mangels an Neuheit im Hinblick auf KANAI:** (vgl. Seiten 25 und 26, Zusammenfassung der Klagegründe von KEEEX)

KEEEX legt zunächst eine allgemeine Stellungnahme zu den Angriffen auf die Gültigkeit seines Patents vor. In seiner Erwiderung auf die Klagebeantwortung macht KEEEX für jeden der ihm entgegengehaltenen Stand der Technik geltend, dass die angeführten Dokumente alle auf digitalen Signatursystemen beruhen und nicht auf Identifikations-Fingerabdrücken im Sinne des Patents. Nach Ansicht des Klägers verwenden diese Referenzen Signaturen, die der Authentifizierung eines Urhebers oder eines Dokuments dienen, während seine Erfindung auf einem eigenständigen Mechanismus beruht, der es ermöglicht, in eine Datei eine aus ihrem eigenen Inhalt berechnete Kennung einzufügen und diesen Inhalt durch eine einfache Neuberechnung zu überprüfen. Das zentrale Argument der Erwiderung auf die Klagebeantwortung stützt sich darauf, dass die angeführten Stand der Technik weder die Verwendung eines echten, in das Dokument integrierten Identifikationsfingerabdrucks

in das Dokument noch den im Patent beanspruchten direkten Vergleich offenlegen, sodass die Neuheit und die erfinderische Tätigkeit gewahrt bleiben

147. ***Insbesondere hinsichtlich der Gültigkeit im Hinblick auf das Dokument KANAI*** entgegnet KEEEX**,** dass KANAI ein komplexes Sicherheitssystem ist, das auf einer für das JPEG/Exif-Format spezifischen Architektur, auf speziellen Metadatenstrukturen und auf Mechanismen der digitalen Signatur beruht. Nach Ansicht des Klägers offenbart dieses Dokument nicht den generischen Mechanismus zur Suche nach einem Identifikationsfingerabdruck mittels eines Referenzwerts und anschließender Überprüfung durch Neuberechnung und Vergleich, wie er im Patent EP070 beansprucht wird.

148. KEEEX führt aus, dass die Beklagten beim Vergleich zwischen dem Gegenstand von Anspruch 1 und dem Dokument D5 bestimmte Merkmale von Anspruch 1 außer Acht lassen. Daher kann die von ihnen gezogene Schlussfolgerung, dass keine Neuheit vorliegt, nur angefochten werden.

149. a) Identifizierungsabdruck

Tatsächlich berücksichtigen die Beklagten die Identifizierungsfunktion des beanspruchten Fingerabdrucks nicht, die jedoch für die Lösung des im Patent aufgeworfenen technischen Problems von wesentlicher Bedeutung ist.

Das Dokument D5 beschreibt einen Hash-Wert, der aus Bilddaten berechnet wird, die sich zwischen den Tags DQT und EOI einer JPEG-Datei befinden, und der in einen APP1-Block zwischen den Tags SOI und DQT der JPEG-Datei eingefügt wird, wobei dieser Block durch die Tags SOI und EOI begrenzt ist.

Tatsächlich wird im Dokument D5 an keiner Stelle präzisiert, dass diesem Hashwert die Funktion eines Identifikators für die JPEG-Datei zukommen soll. Allgemeiner gesagt geht das Dokument D5 nicht auf das Problem der Identifizierung der JPEG-Datei ein. Es wird daher stillschweigend davon ausgegangen, dass die gemäß dem Dokument D5 erzeugte JPEG-Datei eine herkömmliche Kennung erhält, wie beispielsweise einen Dateinamen im Windows- oder OSX-Betriebssystem.

150. b) Suche nach einem Identifikationsfingerabdruck mithilfe eines Markers

Die Beklagten weisen darauf hin, dass der Hashwert in ein TLV-Feld eingefügt wird, das aus einem Tag, einer Länge und einem Wert besteht, der dem Hashwert entspricht.

Auch wenn dem Hashwert ein Tag zugeordnet ist, wird im Dokument D5 an keiner Stelle angegeben, wie der Hashwert in der Datei gefunden wird, geschweige denn, dass das dem Hashwert zugeordnete Tag verwendet wird, um diesen in der JPEG-Datei wiederzufinden, oder dass dieses Tag überhaupt zu diesem Zweck verwendet werden kann.

151. c) Berechnung des Fingerabdrucks unter Ausschluss des gefundenen Identifikationsfingerabdrucks

Dieses Merkmal ist wichtig, da es zusammen mit dem Schritt der Suche anhand eines Markers dazu beiträgt, das beanspruchte Überprüfungsverfahren universell zu gestalten, genauer gesagt unabhängig von einem möglicherweise vordefinierten Format oder einer vordefinierten Struktur des Datenblocks.

Auch dieses Merkmal des Anspruchs wurde von den Beklagten bei ihrer Beurteilung der Relevanz des Dokuments D5 nicht berücksichtigt. Tatsächlich haben sie geltend gemacht, dass dieses Merkmal des Anspruchs 1 durch das Dokument D5 offenbart sei, allein aufgrund der Tatsache, dass der Bilddatenbereich DQT-EOI, auf den sich die Berechnung des Hashwerts bezieht, den Hashwert nicht enthält.

Das Dokument D5 sieht jedoch nicht vor, den Bereich für die Hash-Berechnung anhand des Ergebnisses der Hash-Suche im Datenblock zu bestimmen. Tatsächlich ist dieser Berechnungsbereich bereits vor dem Einfügen eines Hash-Werts oder einer Signatur in den Datenblock vordefiniert:

- *„Insbesondere müssen die Informationen, die mit dem DQT-Marker beginnen und vor dem EOI-Marker enden, geschützt werden*." (Absatz 0047)

152. Somit existieren die DQT- und EOI-Marker, die den Umfang des durch einen Fingerabdruck und eine Signatur zu schützenden Bildbereichs begrenzen, bereits vor einer eventuellen Suche nach dem Fingerabdruck. Die Bestimmung dieses Bildbereichs erfordert daher keineswegs, die Position des Fingerabdrucks im Datenblock zu kennen oder eine vorherige Suche nach dem Fingerabdruck im Datenblock durchzuführen.

153. Im Gegenteil: Das in Anspruch 1 formulierte Verifizierungsverfahren erfordert die Suche nach dem Identifikations-Fingerabdruck, bevor der Fingerabdruck berechnet werden kann, da die Fingerabdruckberechnung unter Ausschluss der Bits des gefundenen Identifikations-Fingerabdrucks erfolgt.

154. Darüber hinaus kann im Gegensatz zum Gegenstand des Anspruchs 1 die Berechnung des Hashwerts der Bilddaten nicht durch Ausschluss des Hashwerts erfolgen, da der Bereich für die Berechnung dieses Hashwerts positiv zwischen zwei vordefinierten Markierungen DQT und EOI festgelegt ist. Es handelt sich also nicht um einen Mechanismus, der auf dem Ausschluss des lokalisierten Fingerabdrucks oder allgemeiner auf dem Ausschluss bestimmter Daten beruht, sondern um einen Mechanismus, der auf der vorherigen Auswahl eines bestimmten Teils der Datei basiert, der bei der Berechnung berücksichtigt werden soll.

155. **Antworten auf die Kritik von KEEEX:** (vgl. insbesondere die Argumente von OPENAI in den Absätzen 85 bis 89, in denen seine Einwendungen zusammengefasst sind)

OpenAI entgegnet, dass KEEEX eine übermäßig komplexe Auslegung des KANAI-Dokuments vornimmt, indem es sich auf alle darin beschriebenen Ausführungsformen und Sicherheitsmechanismen stützt, während sich die Neuheitsanalyse der Beklagten ausschließlich auf die zweite Ausführungsform und, genauer gesagt, allein auf den „Bild-Hash-Wert" (*Image Hash Value*) konzentriert. Nach Ansicht von OpenAI stellt dieses Element für sich genommen einen in die Datei integrierten Fingerabdruck dar, der anhand eines Markers lokalisiert, anhand der geschützten Daten neu berechnet und bei der Überprüfung mit dem gespeicherten Wert verglichen wird. OpenAI macht außerdem geltend, dass der Ausschluss zusätzlicher Elemente außer dem Fingerabdruck selbst bei der Berechnung keine Unterscheidung von Anspruch 1 zulässt, da die Ansprüche 10 und 11 des Patents selbst

den Ausschluss größerer Teile der Datei vorsehen. Schließlich ist OpenAI der Ansicht, dass der beanspruchte Marker durch die in KANAI verwendeten Tags und Strukturen offenbart wird, die es ermöglichen, den Fingerabdruck in der Datei zu lokalisieren. Die anderen in KANAI beschriebenen Mechanismen, insbesondere digitale Signaturen oder Strukturen zum Schutz anderer Daten, werden als unabhängig von dem ausschließlich auf dem „Image Hash Value“ basierenden Überprüfungsunterprozess dargestellt, der bereits die wesentlichen Merkmale von Anspruch 1 wiedergeben würde

156. Standpunkt des Gerichts:

Das Gericht ist von den Argumenten von KEEEX nicht überzeugt und ist der Ansicht, dass Anspruch 1 offenbart ist, da der Fachmann unter Rückgriff auf sein zum Zeitpunkt der Patentanmeldung vorhandenes Allgemeinwissen allein aus dem Dokument KANAI die Lehre jedes einzelnen Merkmals wie folgt unmittelbar und eindeutig abgeleitet hätte:

157. **Merkmal 1.1**: Das Dokument KANAI offenbart ein Verfahren zur Überprüfung der Integrität digitaler Daten, insbesondere von im JPEG/Exif-Format gespeicherten Bildern. Bei der Überprüfung wird ein zuvor in der Datei gespeicherter Hash-Wert mit einem neuen Wert verglichen, der aus den Bilddaten berechnet wird. Eine Diskrepanz zwischen diesen Werten weist auf eine Veränderung der geschützten Daten hin. Das digitale Foto stellt somit einen „digitalen Datenblock“ im Sinne von Anspruch 1 dar.

158. Das Gericht lässt sich von dem Argument der Klägerin nicht überzeugen, dass das Dokument nicht unter den Geltungsbereich des Anspruchs falle, da es auf ein bestimmtes Format beschränkt sei. Wie bereits in der Analyse der Auslegung der Ansprüche dargelegt, verlangt Anspruch 1 weder eine besondere Allgemeingültigkeit noch Unabhängigkeit vom Format der verarbeiteten Datei. Es reicht aus, dass das Dokument für die betreffende Datei das beanspruchte Überprüfungsverfahren offenbart.

159. **Merkmal 1.2**: KANAI offenbart einen „Bild-Hash-Wert“ (*Image Hash Value*), der in der Exif-Datei innerhalb der Sicherheitsstruktur (*Security IFD*) gespeichert ist. Dieser Wert stellt einen digitalen Fingerabdruck im Sinne des Anspruchs dar.

160. Das Gericht stellt ferner fest, dass die in KANAI verwendete TLV-Struktur einen Teil „T“ (*Tag*), einen Teil „L“ (*Length*) und einen Teil „V“ (*Value*) umfasst. Der Teil „T“ ermöglicht es, das Datenelement zu identifizieren, das den Bild-Hashwert enthält, und somit diesen Wert in der Datei zu lokalisieren. Er erfüllt damit die Funktion des „ersten Markers“ im Sinne des Anspruchs 1.2.

161. Das Gericht teilt nicht die Auffassung der Klägerin, wonach der beanspruchte Marker zwangsläufig eine Textsuche oder einen von der logischen Struktur der Datei unabhängigen Marker erfordern würde. Das Patent definiert den Marker

funktional definiert, als Mittel zum Auffinden des Fingerabdrucks. Eine auf einem Daten-Tag basierende Lokalisierung erfüllt diese Anforderung.

162. **Merkmal 1.3**: Sobald der Hashwert lokalisiert ist, weist KANAI die Neuberechnung eines neuen Hashwerts auf der Grundlage der geschützten Bilddaten an. Die Offenbarung sieht ausdrücklich die Anwendung eines Hash-Algorithmus wie SHA-1 oder MD5 auf den Bilddatenstrom vor, um einen Wert zur Überprüfung zu erhalten.

163. Das Gericht ist der Ansicht, dass dieser Vorgang der Berechnung eines digitalen Fingerabdrucks des Datenblocks mittels einer Fingerabdruckfunktion entspricht, wie es Merkmal 1.3 verlangt.

164. Das Gericht ist von dem Argument, KANAI betreffe lediglich digitale Signaturen, nicht überzeugt. Das Dokument unterscheidet klar zwischen dem „Hashwert des Bildes“, dem „Hashwert der Daten“ und der „Signatur der Daten“. Das Vorhandensein einer zusätzlichen Signatur-Ebene hebt die eigenständige Offenlegung des Hashwerts des Bildes nicht auf.

165. **Merkmal 1.4**: Der Bild-Hashwert wird im Sicherheits-IFD gespeichert, der in die JPEG/Exif-Datei integriert ist. Bei der Neuberechnung des Hashwerts werden hingegen nur die Bilddaten zwischen den Markern DQT und EOI dem Hash-Algorithmus unterzogen.

166. Daraus folgt, dass der Bereich, der den gespeicherten Hashwert enthält, bei der Berechnung des neu berechneten Fingerabdrucks nicht berücksichtigt wird. Die Bits, die dem gespeicherten Fingerabdruck entsprechen, tragen daher nicht zum erzielten Ergebnis bei. Die Tatsache, dass die Daten des DQT-Feldes in Schritt 1001 berücksichtigt werden, wie aus Abbildung 10 von KANAI hervorgeht, ist unerheblich, da dieses Feld nur unveränderliche Daten enthält, die teilweise die Struktur des JPEG-Bildes bestimmen, wie die Beklagten in der mündlichen Verhandlung unwidersprochen geltend gemacht haben.

167. Das Gericht ist von dem Argument der Klägerin nicht überzeugt, wonach KANAI festlege, was in die Berechnung einbezogen werden müsse, während der Anspruch festlege, was davon auszuschließen sei. Merkmal 1.4 schreibt keine bestimmte Methode vor, mit der der Identifikationsfingerabdruck aus der Berechnung ausgeschlossen werden kann. Es verlangt lediglich, dass der Wert des neu berechneten Fingerabdrucks ermittelt wird, ohne die Bits zu berücksichtigen, die dem gespeicherten Fingerabdruck entsprechen. Aus funktionaler Sicht werden Daten, die außerhalb des der Hash-Funktion unterworfenen Datenabschnitts liegen, tatsächlich aus der Berechnung ausgeschlossen, unabhängig davon, ob dieser Ausschluss durch eine aktive Löschung oder durch die vorherige Festlegung des zu verarbeitenden Bereichs erfolgt.

168. Das Gericht ist auch nicht von dem Argument überzeugt, wonach der Anspruch zwangsläufig die Berücksichtigung aller Bits des Datenblocks erfordern würde, die nicht zum Fingerabdruck gehören. Wie bei der Auslegung des Anspruchs dargelegt, bedeutet der Ausdruck „abhängig von jedem der Bits“

bedeutet, dass der Fingerabdruck von der Gesamtheit der für die Berechnung herangezogenen Daten abhängt und nicht, dass keine anderen Daten ausgeschlossen werden dürfen. Eine solche Auslegung wäre im Übrigen kaum mit den abhängigen Ansprüchen 10 und 11 vereinbar, die ausdrücklich vorsehen, dass Metadaten einen variablen Teil umfassen können, der von der Berechnung des Fingerabdrucks ausgeschlossen ist, und dass sich der Fingerabdruck selbst in diesem variablen Teil befinden kann.

169. Selbst wenn KANAI den Bereich der Datei, der der Hash-Berechnung unterzogen wird, konkret festlegt, während Anspruch 1 den Vorgang im Sinne eines Ausschlusses des lokalisierten Fingerabdrucks beschreibt, dienen beide Ansätze demselben technischen Ziel, nämlich zu verhindern, dass die in der Datei gespeicherten Verifizierungsdaten das Ergebnis der für die Verifizierung verwendeten Berechnung beeinflussen. Das Gericht ist daher der Ansicht, dass der Fachmann aus KANAI zumindest – wenn schon nicht wörtlich, so doch zumindest unmittelbar und eindeutig – die Lehre einer Fingerabdruckberechnung unter Ausschluss des Bereichs, der den Identifikationsfingerabdruck enthält, entnehmen würde.

170. In beiden Fällen besteht das Ziel darin, einen Fingerabdruck zu berechnen, der für die geschützte Nutzlast (Payload) der Datei repräsentativ ist, wobei die Verifizierungsdaten und gegebenenfalls andere vordefinierte Daten, die das Berechnungsergebnis nicht beeinflussen dürfen, ausgeschlossen werden, um die Erkennung einer Änderung des tatsächlich geschützten Inhalts zu ermöglichen.

171. Folglich wird das Merkmal 1.4 von KANAI offenbart.

172. **Merkmal 1.5**: KANAI beschreibt anschließend den Vergleich zwischen dem zuvor aus der Datei gelesenen Hashwert und dem neu berechneten Hashwert. In der Offenbarung wird ausdrücklich darauf hingewiesen, dass eine Differenz zwischen diesen beiden Werten auf eine Veränderung der Bilddaten hindeutet.

173. Das Gericht ist der Ansicht, dass diese Abfolge aus Einlesen, Neuberechnung und Vergleich der in Merkmal 1.5 beanspruchten Überprüfung entspricht.

174. Der Umstand, dass KANAI auch andere Überprüfungsmechanismen vorsieht, ist irrelevant. Anspruch 1 ist offen formuliert und schließt das Vorhandensein zusätzlicher Schritte nicht aus. Es reicht aus, dass die Schrift den beanspruchten Vergleichsmechanismus offenbart, was der Fall ist.

175. **Fazit:**

Das Gericht ist der Auffassung, dass keiner der von der Klägerin vorgebrachten Einwände eine Abgrenzung des beanspruchten Gegenstands vom KANAI-Dokument ermöglicht. Dieses Dokument offenbart unmittelbar und eindeutig jedes der Merkmale 1.1 bis 1.5 des Anspruchs 1.

Anspruch 1 des erteilten Patents ist daher im Hinblick auf das Dokument KANAI nicht neu.

2) Gültigkeit der von KEEEX entgegengehaltenen, von Anspruch 1 abhängigen Ansprüche (2, 4, 7, 8, 10, 11 und 14)

176. Rechtlicher Rahmen:

Das Berufungsgericht hat entschieden (UPC_CoA_473/2025, UPC_CoA_474/2025, UPC_CoA_873/2025 und UPC_CoA_881/2026, 13. Juli 2026, Fujifilm gegen Kodak), dass der Patentinhaber nicht verpflichtet ist, einen Änderungsantrag gemäß Regel 30 der Verfahrensordnung allein zu dem Zweck zu stellen, abhängige Ansprüche in der erteilten Fassung oder Kombinationen von Ansprüchen zu verteidigen, die bereits durch das erteilte Patent abgedeckt sind. Wird jedoch die Nichtigkeit mehrerer Ansprüche oder aller Ansprüche beantragt, muss der Patentinhaber hinreichend begründet darlegen, welche abhängigen Ansprüche er für gültig hält, falls der unabhängige Anspruch für nichtig erklärt werden sollte. Beruft er sich auf eine bestimmte Kombination von abhängigen Ansprüchen, so muss diese Kombination ebenfalls hinreichend genau bezeichnet werden (Punkte 2, 3 und 5 der Zusammenfassung).

177. Im vorliegenden Fall:

hat KEEEX in seinen Schriftsätzen nicht dargelegt, welche abhängigen Ansprüche es für gültig hält, falls Anspruch 1 für nichtig erklärt würde, und diese Behauptung noch weniger begründet. Erst in der mündlichen Verhandlung erklärte der Vertreter des Klägers, dass Anspruch 2 auch dann gültig sein könnte, wenn Anspruch 1 für ungültig erklärt würde; der Vertreter von ADOBE wies jedoch zu Recht darauf hin, dass diese Argumentation in den Schriftsätzen nicht enthalten war und daher als verspätet aus dem Verfahren ausgeschlossen werden müsse.

178. Es obliegt dem Patentinhaber nachzuweisen, dass die abhängigen Ansprüche auch dann gültig sein könnten, wenn der Hauptanspruch für nichtig erklärt wird. Im vorliegenden Fall stellt das Gericht fest, dass KEEEX in seinen Schriftsätzen nicht hinreichend begründet dargelegt hat, welche abhängigen Ansprüche es für gültig hält, falls der unabhängige Anspruch für nichtig erklärt würde.

179. Daraus folgt, dass aufgrund der Ungültigerklärung des Anspruchs 1 (aus den Gründen der unzulässigen Erweiterung des Gegenstands und der fehlenden Neuheit) auch die beanstandeten abhängigen Ansprüche Nr. 2, 4, 7, 8, 10, 11 und 14 für ungültig erklärt werden.

3) Weitere unabhängige Ansprüche (16 und 18)

Die unabhängigen Ansprüche 16 und 18 sind spiegelbildlich zum Verfahren des Anspruchs 1 aufgebaut und weisen daher dieselben Ungültigkeitsgründe auf, nämlich eine Ausweitung des Schutzgegenstands und darüber hinaus einen Mangel an Neuheit im Hinblick auf KANAI aus denselben Gründen.

4) Hilfsanträge auf bedingte Änderung des Patents

180. KEEEX schlägt als Antwort auf die Widerklage auf Nichtigerklärung seines Patents 11 Hilfsanträge auf Änderung auf der Grundlage von Regel 30.1 RdP vor, wie sie in den Unterlagen KEEEX 29.1 bis 29.11 dargelegt sind. Der Antragsteller hat in seinem Schriftsatz vom 5. März 2026 eine Tabelle erstellt, in der die eingereichten Hilfsanträge wie folgt zusammengefasst sind:

2.11. Tableau récapitulatif des requêtes

Requête	Descriptif résumé[1]
Principale	Suppression de la revendication 15 incompatible avec la revendication 1
Première requête subsidiaire	Requête principale + La fonction de calcul d'empreinte est une fonction de hachage
Deuxième requête subsidiaire	Première requête subsidiaire + information = fonction de hachage
Troisième requête subsidiaire	Première requête subsidiaire + signature
Quatrième requête subsidiaire	Requête principale + navigateur
Cinquième-neuvième requêtes subsidiaires	Requête principale, première-quatrième requêtes subsidiaires, respectivement + retrait de l'alternative dans la revendication 1
Dixième requête subsidiaire	Brevet tel que délivré
Onzième requête subsidiaire	Brevet tel que délivré + retrait de l'alternative dans la revendication 1

[1] Ce tableau a pour simple objectif de donner une vue synthétique de l'organisation des requêtes, mais ne peut se substituer à la présentation individuelle détaillée de chaque requête.

181. Während der mündlichen Verhandlung bat das Gremium um Klarstellung, um zu prüfen, ob die Hilfsanträge als vollständiges und in sich geschlossenes Ganzes zu betrachten seien oder ob KEEEX die Möglichkeit offenhalten wolle, dass beliebige der Haupt- und abhängigen Ansprüche, die in den in den jeweiligen Hilfsanträgen vorgelegten Anspruchsgruppen enthalten sind, neu kombiniert werden könnten und – als zusätzlicher Hilfsantrag – gemäß einer beliebigen dieser theoretisch möglichen Neukombinationen neu kombiniert werden müssten (vgl. Frage von Richter Tochtermann bei 2:28 des Audioprotokolls der Verhandlung). Die Beklagten antworteten, dass die Hilfsanträge von KEEEX während des gesamten Verfahrens als vollständiges und in sich geschlossenes Anspruchsbündel vorgebracht worden seien, ohne dass mögliche Kombinationen angedeutet oder begründet worden seien. (vgl. Antwort von Rechtsanwalt Por bei 3:33 der Audioaufzeichnung der Verhandlung). In ihrer mündlichen Erwiderung hat KEEEX den Beklagten in dieser Auslegung ihrer Änderungsanträge nicht widersprochen. (vgl. Antwort von Herrn Bourgeois bei 3:45 der Audioaufzeichnung der Verhandlung).

182. Zu RS 1 bis RS 9: Die von KEEEX auf der Grundlage von Regel 30.1 der Verfahrensordnung vorgeschlagenen Anträge auf Änderung der Patente Nr. 1 bis 9 beinhalten die Streichung des Anspruchs 15, der nicht Gegenstand der von den Beklagten erhobenen Nichtigkeitsklagen ist.

183. Zunächst weist das Gericht in verfahrensrechtlicher Hinsicht darauf hin, dass der Streitgegenstand von den Parteien festgelegt wird; die Gültigkeit des Anspruchs 15 wurde jedoch von den Beklagten nicht beanstandet. Folglich ist es dem Patentinhaber, wie von den Beklagten zu Recht geltend gemacht, nicht gestattet, diesen nicht angefochtenen Anspruch zu ändern oder zu streichen.

184. Darüber hinaus hat der Patentinhaber in materieller Hinsicht die Möglichkeit, die Beschreibung so zu ändern, dass sie mit dem geänderten Anspruch übereinstimmt (vgl.
R. 30.1 (a) RdP). Es ist hingegen nicht möglich, die Beschreibung so zu ändern, dass sich die Bedeutung des Patents und seines Anspruchs 1 ändert. Es ist zwar möglich, den Umfang des Patents einzuschränken, aber nicht, dem Patent durch eine derart umfassende Änderung der Beschreibung eine neue Bedeutung zu geben. Dies wäre im Übrigen mit dem Grundsatz der Rechtssicherheit für Dritte unvereinbar. Im vorliegenden Fall stützt sich KEEEX zur Rechtfertigung der Streichung von Anspruch 15 und der betreffenden Teile der Beschreibung darauf, dass diese mit Anspruch 1 unvereinbar seien. In dem Teil der vorliegenden Entscheidung, der sich mit der Auslegung und der Ausgestaltung der Ansprüche befasst, wurde jedoch nachgewiesen, dass das gesamte Patent im Gegenteil lehrt, dass Anspruch 1 auch digitale Signaturen umfasst, wie durch Anspruch 15 bestätigt wird, der somit nicht unvereinbar erscheint, sondern lediglich dessen Geltungsbereich präzisiert. Durch die Streichung von Anspruch 15 und aller stützenden Teile der Beschreibung versucht der Patentinhaber somit, den Umfang und die Bedeutung seines Patents nachträglich zu ändern, um der Vorveröffentlichung durch D5 zu entgehen, was nicht zulässig ist.

185. Das Gremium kommt zu dem Schluss, dass die Anträge RS 1 bis RS 9 zur Änderung des Patents sowohl in verfahrensrechtlicher als auch in materiell-rechtlicher Hinsicht unzulässig sind.

186. Es wird daran erinnert, dass KEEEX den Antrag 10 (SR 10) zurückgenommen hat, der im Übrigen keinen Nutzen hatte, da er das erteilte Patent, dessen Gültigkeit bereits oben geprüft wurde, wörtlich wiederholte (vgl. den Beschluss nach der Vorverhandlung vom 22. September 2026) und dass die nachträgliche Änderung gemäß R. 30.2 RdP vom Gremium nicht genehmigt wurde (vgl. Beschluss vom 25. Juni 2026 und dessen Bestätigung durch das Gremium am 29. Juli 2026).

187. Was SR 11 betrifft, so sieht dieser weder eine Änderung der Beschreibung noch die Streichung des Anspruchs 15 des Patents vor. SR 11 unterliegt daher nicht den von den Beklagten vorgebrachten Einwänden hinsichtlich der Unzulässigkeit von RS 1 bis RS 9. Er besteht, wie bereits dargelegt, in der Streichung des letzten Teils des Merkmals 1.5.

188. Die Beklagten werfen RS 11 die Unzulässigkeit vor, da sie eine Erweiterung des Schutzumfangs gemäß Art. 123 (3) EPÜ bewirke.

189. Stellungnahme des Gerichts zur Unzulässigkeit von RS 11 im Hinblick auf Art. 123 Abs. 3 EPÜ:

190. Der Hilfsantrag 11 (RS11) entspricht im Wesentlichen dem erteilten Patent, mit der Ausnahme, dass Anspruch 1 durch die Streichung des zweiten Teils der am Ende des Merkmals 1.5 aufgeführten Alternative geändert wurde, nämlich der Worte „oder

dass der Identifikationsfingerabdruck durch Anwendung einer

anderen Fingerabdruck-Berechnungsfunktion“. Diese Änderung zielt darauf ab, dem gegen das erteilte Patent erhobenen Einwand der Gegenstandserweiterung zu begegnen, der darauf beruht, dass diese Alternative in der eingereichten Anmeldung keine direkte und eindeutige Grundlage finde. Der Hilfsantrag 11 behält hingegen alle übrigen Merkmale des Anspruchs 1 sowie den allgemeinen Aufbau des erteilten Patents bei, einschließlich der Ausführungsformen, die digitale Signaturen verwenden.

191. Das Gericht muss jedoch noch prüfen, ob die Streichung dieses Merkmals den Anforderungen des Artikels 123 (3) EPÜ entspricht. Denn selbst wenn eine Änderung darauf abzielt, eine mögliche Erweiterung des Schutzgegenstands im Sinne des Artikels 123 (2) EPÜ zu beheben, kann sie nicht zugelassen werden, wenn sie zur Folge hat, dass der durch das Patent gewährte Schutz nach dessen Erteilung erweitert wird. Es ist daher zu prüfen, ob die Streichung der Alternative bezüglich der Verwendung einer anderen Fingerabdruck-Berechnungsfunktion den Umfang des erteilten Anspruchs 1 verändert und dazu führt, dass dem Patentinhaber ein weitergehender Schutz gewährt wird als der, der sich aus dem Wortlaut des erteilten Patents ergibt.

192. Nach Ansicht von ADOBE wurde das Element, dessen Streichung der Beschwerdeführer anstrebt, in den Anspruchsatz vom 13. März 2020 aufgenommen, was die Prüfungsabteilung davon überzeugt hat, ein Patent zu erteilen. Der Antragsteller machte geltend, dass, da beide Varianten im Rahmen des falschen Vergleichs gemeinsam beansprucht worden seien, ein korrekter Vergleich voraussetzen würde, dass der Datenblock nicht verändert worden sei und die verwendeten Hash-Funktionen identisch seien. Durch die Streichung einer der Varianten wird diese daher nicht mehr vom Anspruch verlangt. Folglich verstößt der fünfte Hilfsantrag gegen Artikel 123 (3) EPÜ, da er darauf abzielt, den Schutzumfang zu erweitern.

193. ADOBE macht geltend, dass die Streichung des zweiten Zweigs der in Merkmal 1.5 enthaltenen Alternative im Hinblick auf Artikel 123 (3) EPÜ nicht zulässig sei. Nach Ansicht von ADOBE wurde diese Alternative im Laufe des Prüfungsverfahrens eingeführt und trug zur Erteilung des Patents bei. ADOBE macht geltend, dass im erteilten Anspruch ein korrekter Vergleich zwischen dem gefundenen und dem berechneten Fingerabdruck nicht nur voraussetzt, dass der Datenblock nicht verändert wurde, sondern auch, dass dieselbe Funktion zur Berechnung des Fingerabdrucks verwendet wurde. Die Streichung der Alternative bezüglich der Verwendung einer anderen Hash-Funktion hätte zur Folge, dass diese Bedingung aus dem Anspruch entfällt, und würde somit nach Ansicht von ADOBE zu einer Ausweitung des Schutzumfangs des erteilten Patents führen, was gegen Artikel 123 (3) EPÜ verstößt.

194. Das Gericht ist nicht davon überzeugt, dass die Streichung des zweiten Teils der in Merkmal 1.5 enthaltenen Alternative zwangsläufig zu einer Schutzausweitung im Sinne von Artikel 123 (3) EPÜ führt. Die Änderung betrifft nämlich die einem negativen Vergleich zugewiesenen Konsequenzen und berührt auf den ersten Blick nicht die technischen Schritte des beanspruchten Verfahrens. Es ist daher nicht unmittelbar ersichtlich, dass Handlungen, die nicht unter den Umfang des erteilten Anspruchs fielen, nun in dessen Umfang fallen würden.

195. Das Gericht muss diese Frage jedoch nicht endgültig klären, da RS 11 ohnehin das Problem der mangelnden Neuheit des Patents nicht löst.

196. Standpunkt des Gerichts zur Gültigkeit von RS 11:

197. Der von den Beklagten angeführte Stand der Technik KANAI ist dem in RS 11 geänderten Patent aus denselben Gründen vorrangig, wie sie bereits in Bezug auf die erteilte Patentfassung dargelegt wurden. RS 11 ist daher zudem mangels Neuheit im Hinblick auf den Stand der Technik KANAI ungültig.

198. Schlussfolgerung zur Gültigkeit des Patents:

Die vom Patentinhaber vorgeschlagenen Änderungen sind unzulässig; sie können daher die Patenterlaubnismängel der entgegengehaltenen Ansprüche des Patents EP 070 nicht beheben, die entweder aufgrund einer Erweiterung des Gegenstands oder aufgrund mangelnder Neuheit im Hinblick auf das Dokument KANAI ungültig sind.

DIE PATENTVERLETZUNG:

199. Da sie jeder Grundlage entbehren, sind alle Anträge von KEEEX im Rahmen der Verletzungsklage sowie alle daraus folgenden Anträge zurückzuweisen.

200. Es ist daher nicht erforderlich, über die Begründetheit und die Haftung hinsichtlich der von KEEEX geltend gemachten Patentverletzung zu entscheiden.

GERICHTSKOSTEN (Artikel 69 AJUB):

201. Hinsichtlich der Verteilung der Prozesskosten zwischen den Parteien ist KEEEX als unterlegene Partei zur Tragung aller Kosten des vorliegenden Verfahrens (Verletzungsklage und Widerklage auf Aufhebung) zu verurteilen.

202. Hinsichtlich der Gewährung eines Vorschusses beantragt jede der vier Gruppen von Beklagten die Zahlung eines Vorschusses auf die Kosten in Höhe von 1,25 Millionen Euro für die Kosten im Zusammenhang mit der Klage wegen Patentverletzung sowie denselben Betrag für die Kosten der Widerklage auf Nichtigkeit.

203. Stellungnahme des Gerichts:

Folgende Aspekte sind zu berücksichtigen:

- Die Obergrenze für den Gesamtbetrag der erstattungsfähigen Kosten liegt im vorliegenden Fall bei 2 Millionen Euro,

- Die vom Berufungsgericht empfohlene Rückstellung beträgt 50 % der geschätzten gesamten erstattungsfähigen Kosten.

Darüber hinaus müssen bei der Festsetzung angemessener und verhältnismäßiger Kosten zwei für diesen Rechtsstreit spezifische Kriterien berücksichtigt werden (die vom Berufungsgericht in seinem Beschluss vom 30. April 2026 in dieser Sache anerkannt wurden), nämlich die Synergie der Verteidigungsargumente und der Status von KEEEX als Kleinunternehmen. Diese beiden

besonderen Merkmale des vorliegenden Rechtsstreits rechtfertigen eine Gewichtung im Verhältnis zur vom Verwaltungsausschuss empfohlenen Obergrenze (Beschluss über die Leitlinien zu den Verfahrenskosten und zur Obergrenze der erstattungsfähigen Kosten vom 24. April 2023, geändert am 4. November 2025).

204. Angesichts dieser Umstände ist es angebracht, einen Gesamtbetrag von 300.000 Euro als Sicherheitsleistung zuzuweisen, der bereits von KEEEX als Sicherheit hinterlegt wurde, d. h. jeweils 75.000 Euro für jede der Beklagtengruppen.

AUS DIESEN GRÜNDEN,

beschließt das Gericht erster Instanz der JUB:

1. ordnet an, dass alle entgegengehaltenen Ansprüche des Patents EP2949070 (das „Patent“ oder „EP 070“) in seiner erteilten Fassung für ungültig erklärt werden, und erklärt alle Änderungsanträge für unzulässig,

2. hebt folglich die Ansprüche 1, 2, 4, 7, 8, 10, 11, 14, 16 und 18 des Patents in der erteilten Fassung im Hoheitsgebiet der folgenden Vertragsstaaten der JUB vollständig auf: Frankreich, Italien, Deutschland, Österreich, Belgien, Dänemark, den Niederlanden und Schweden,

3. ordnet an, dass die Geschäftsstelle gemäß Artikel 65 Absatz 5 des JUB-Übereinkommens nach Ablauf der Rechtsmittelfrist vor dem Berufungsgericht eine Kopie dieser Entscheidung an das Europäische Patentamt und an das nationale Patentamt jedes betroffenen Vertragsmitgliedstaats übermittelt,

4. Weist alle auf das Patent EP 070 gestützten Ansprüche von KEEEX wegen Patentverletzung ab,

5. ordnet an, dass die gesamten Prozesskosten des vorliegenden Verfahrens (für die Klage wegen Patentverletzung und die Widerklage auf Nichtigkeit) von KEEEX als unterlegener Partei zu tragen sind,

6. verurteilt KEEEX zur Zahlung eines Vorschusses auf die Prozesskosten in Höhe von insgesamt 300.000 Euro an alle Beklagten wie folgt: jeweils 75.000 Euro an jede der vier Beklagtengruppen ADOBE, OPENAI, TRUEPIC und JOINT DVT/C2PA, und zwar innerhalb von 30 Tagen nach Zustellung dieser Entscheidung.

7. Setzt den Streitwert des vorliegenden Rechtsstreits für jede der Klagen (die Klage wegen Patentverletzung und die Widerklage auf Nichtigkeit) auf mehr als 50.000.000 Euro fest.

Erlassen in Paris am 17. November 2026.

Camille Lignières, vorsitzende Richterin und Berichterstatterin

Camille Lignières
Datum: 17.11.2026 11:25:49 +01'00'

Carine Gillet, rechtlich qualifizierte Richterin



Peter Tochtermann, juristisch qualifizierter Richter



Alessandro Sanchini, fachlich qualifizierter Richter



Marielle Brasseur, Gerichtsschreiberin der Ortsabteilung Paris



Informationen zur Berufung

Jede Partei, deren Anträge ganz oder teilweise zurückgewiesen wurden, kann gegen diese Entscheidung innerhalb von zwei Monaten nach deren Zustellung beim Berufungsgericht Berufung einlegen (Art. 73 Abs. 1 der AJUB, Regeln 220.1(a) und 224.1(a) der Verfahrensordnung der JUB).

Informationen zur Vollstreckung (Art. 82 der AJUB, Art. 37 Abs. 2 der AJUB, Regeln 118.8, 158.2, 354 und 355.4 der Verfahrensordnung)

Eine beglaubigte Abschrift der vollstreckbaren Entscheidung wird vom stellvertretenden Gerichtsschreiber auf Antrag der vollstreckungsberechtigten Partei ausgestellt, Regel 69 der Verfahrensordnung

EINZELHEITEN DER ENTSCHEIDUNG

UPC-Nr.: UPC_CFI_530/2025
sowie UPC-CFI-0002281/2025 – UPC-CFI-0002285/2025 – UPC-CFI-0000003/2026 – UPC-CFI-0002274/2025
Art der Klage: Klage wegen Patentverletzung und Widerklagen auf Nichtigkeit Datum der Entscheidung: 17. November 2026