Unified Patent Court
Einheitliches Patentgericht
Juridiction unifiée du brevet

Lokalkammer Düsseldorf
UPC_CFI_1332/2026

Anordnung

des Gerichts erster Instanz des Einheitlichen Patentgerichts
erlassen am 7. September 2026
betreffend EP 4 285 308

LEITSÄTZE:

1. Um einen reinen Ausforschungsbeweis („fishing expedition“) zu verhindern, setzt die Anordnung einer Inspektion und/oder Beweissicherung voraus, dass es plausibel erscheint, dass das in Rede stehende Patent verletzt wird (Anschluss an UPC_CoA_239/2025, Anordnung v. 26. Mai 2025, Rn. 12 – Centripetal v. Palo Alto).

2. Existieren mögliche Alternativlösungen, ist es gerade eine, wenn nicht die wesentliche Aufgabe des Beweissicherungsverfahrens, ausgehend von dem auf konkrete Anknüpfungstatsachen begründeten Verdacht einer möglichen Patentverletzung weiter aufzuklären und Beweise dafür zu sichern, ob und gegebenenfalls in welchem Umfang die zu untersuchende Ausführungsform von der durch das Antragspatent geschützten technischen Lehre, und eben nicht von einer möglichen Alternativlösung, Gebrauch macht. Mögliche patentfreie Alternativlösungen stehen einer Inspektions- und/oder Beweissicherungsanordnung daher nur entgegen, wenn sie dazu führen, dass sie den Vortrag des Antragstellers zu einer möglichen Verletzung des Antragspatents nicht mehr plausibel erscheinen lassen.

3. Sind in einer von Antragsgegnerseite eingereichten Schutzschrift keine Nichtverletzungsargumente enthalten, kann dies den Verdacht einer möglichen Verletzung des Antragspatents erhärten.

SCHLAGWÖRTER:

Inspektion und Beweissicherung; Prüfungsverfahren; hinreichende Verletzungswahrscheinlichkeit

HEADNOTES:

1. To prevent a mere 'fishing expedition', an order for inspection and/or preservation of evidence must be based on plausible grounds that the patent in question is subject to infringement (in line with UPC_CoA_239/2025, Order of 26 May 2025, para. 12 – Centripetal v Palo Alto).

2. Where possible alternative solutions exist, it is precisely one – if not the primary – purpose of the proceedings for the preservation of evidence to investigate further, on the basis of the suspicion of a possible patent infringement grounded in specific connecting facts, and to secure evidence as to whether, and if so to what extent, the embodiment under investigation makes use of the technical teaching protected by the patent in question, and not, in fact, of a possible alternative solution. Possible non-infringing alternative solutions therefore preclude an order for inspection and/or preservation of evidence only if they render the Applicant's submission regarding a possible infringement of the patent in question no longer plausible.

3. If a protective letter filed by the respondent does not contain any arguments demonstrating non-infringement, this may reinforce the suspicion of a possible infringement of the patent in question.

KEYWORDS:

preservation of evidence and inspection; request for review; sufficient likelihood of infringement

ANTRAGSTELLERIN:

fiskaly GmbH, vertreten durch ihre Geschäftsführer Johannes Ferner, Simon Tragatschnig und Patrick Gaubatz, Mariahilfer Straße 36/5, 1070 Wien, Österreich

vertreten durch:	Rechtsanwalt Sebastian Dworschak, Nordemann Czychowski & Partner Rechtsanwältinnen und Rechtsanwälte mbB, Kurfürstendamm 178, 10707 Berlin, Deutschland
elektronische Zustelladresse:	sebastian.dworschak@nordemann.de
mitwirkender Patentanwalt:	Patentanwalt Ralf Emig, Maikowski & Ninnemann Patentanwälte Partnerschaft mbB, Kurfürstendamm 54-55, 10707 Berlin, Deutschland

ANTRAGSGEGNERINNEN:

1. **SwissBit AG**, vertreten durch ihren Verwaltungsratspräsidenten Bernd Stefan Hofschen, ihr Verwaltungsratsmitglied und Mitglied der Geschäftsleitung Benjamin Schüler und ihr Verwaltungsratsmitglied Thomas Harald Luft, Industriestrasse 4, 9552 Bronschhofen, Schweiz

2. **Swissbit Germany AG,** vertreten durch ihren Vorstand Lars Lust und Chris Schwarze, Bitterfelder Straße 22, 12681 Berlin, Deutschland

vertreten durch:	Rechtsanwalt Dr. Thomas Lynker, TALIENS Partnerschaft von Rechtsanwälten mbB, Amalienstraße 15 f, 80333 München, Deutschland
elektronische Zustelladresse:	thomas.lynker@taliens.com
mitwirkender Patentanwalt:	Patentanwalt Michael Platzöder, Platzöder Patentanwaltsgesellschaft mbH, Inselkammerstraße 10, 82008 Unterhaching, Deutschland
elektronische Zustelladresse:	m.platzoeder@platzoeder.eu

ANTRAGSPATENT:

EUROPÄISCHES PATENT NR. EP 4 285 308 B8

SPRUCHKÖRPER/KAMMER:

Spruchkörper 1 der Lokalkammer Düsseldorf

MITWIRKENDE RICHTER:

Diese Anordnung wurde durch den Vorsitzenden Richter Thomas, den rechtlich qualifizierten Richter Adocker als Berichterstatter und die rechtlich qualifizierte Richterin Dr. Schumacher erlassen.

VERFAHRENSSPRACHE: Deutsch

GEGENSTAND: R. 197.3 VerfO – Prüfung einer Anordnung zur Inspektion und Beweissicherung

MÜNDLICHE VERHANDLUNG: 25. August 2026

KURZE DARSTELLUNG DES SACHVERHALTS:

1. Die Antragstellerin ist Inhaberin des Europäischen Patents EP 4 285 308 B8 (Anlage NM AST 4; nachfolgend „Antragspatent"), das am 28. Januar 2022 unter Inanspruchnahme der Priorität der EP-Anmeldung 21154250 vom 29. Januar 2021 in englischer Verfahrenssprache angemeldet wurde. Die Veröffentlichung der Erteilung des Antragspatents erfolgte am 26. Juni 2024, die korrigierte Patentschrift B8 wurde am 17. Juli 2024 veröffentlicht. Es handelt sich um ein Europäisches Patent mit einheitlicher Wirkung. Die einheitliche Wirkung wurde am 2. September 2024 eingetragen.

2. Gegen die Erteilung des Antragspatents wurde kein Einspruch eingelegt.

3. Das Antragspatent trägt die Bezeichnung „SECURELY REGISTERING A SEQUENCE OF TRANSACTIONS" (Sichere Registrierung einer Sequenz von Transaktionen). Der Antrag der Antragstellerin bezieht sich primär auf dessen Anspruch 6 und auf die auf diesen rückbezogenen Unteransprüche 7 - 9 sowie daneben auf die unabhängigen Ansprüche 1, 10 und 12. In der englischen Verfahrenssprache sind diese Ansprüche wie folgt formuliert:

   Anspruch 1:

   „A method for securely registering a sequence of transactions with a distributed system (1), wherein the distributed system (1) comprises a registration device (6) and a signature device (8), wherein the registration device (6) comprises a transaction storage (16) for storing signed transaction records (15) signed by the signature device (8), wherein the signature device (8) comprises a key usage counter that is incremented with each signature generated by the signature device (8), wherein each signed transaction record (15) comprises an associated value of the key usage counter at the time of the signature, wherein the method comprises: comparing a present value of the key usage counter with a last recorded value, which last recorded value is the associated value of a last signed transaction record in the transaction storage (16), loading at least one previously signed trans action record (23) from a record buffer (24) of the signature device (8) responsive to detecting a gap between the present value and the last recorded value, and transmitting the loaded at least one previously signed transaction record (23) to the registration device (6)."

   Anspruch 6:

   „A distributed system (1) for securely registering a sequence of transactions, wherein the distributed system (1) comprises a registration device (6) and a signature device (8), wherein the registration device (6) comprises a transaction storage (16) for storing signed transaction records (15) signed by the signature device (8), wherein the signature device (8) comprises a

key usage counter and a record buffer (24) for buffering signed transaction records (15), wherein each signed transaction record (15) comprises an associated value of the key usage counter at the time of the signature, wherein the signature device (8) is configured to load at least one previously signed transaction record (23) from the record buffer (24) responsive to a detection of a gap between a present value of the key usage counter and the associated value of a last signed transaction record in the transaction storage (16), and for transmitting the loaded at least one previously signed trans action record (23) to the registration device (6)."

Anspruch 7:

„The distributed system (1) of claim 6, **characterised in that** the registration device (6) is configured to send an indication (18) of the associated value of a last signed transaction record to the signature device (8)."

Anspruch 8:

„The distributed system of claim 7, **characterised in that** the signature device (8) is configured to reject providing a signature of a new unsigned transaction record (10) responsive to detecting a gap between the present value and the associated value of the last signed transaction record."

Anspruch 9:

„The distributed system of claim 6, **characterised in that** the registration device (6) is configured to, upon receipt of a new signed transaction record (15) from the signature device (8), compare the associated value of the new signed transaction record (15) with the associated value of the last signed transaction record and to request a retransmission of at least one previously signed transaction record (23) from the signature device (8) responsive to a detection of a gap between the compared values."

Anspruch 10:

„A computer program comprising instructions to cause a registration device (6) comprising a transaction storage (16) for storing signed transaction records (15), wherein each signed transaction record (15) comprises an associated value of a key usage counter at the time of the signature, to execute the steps of: accessing the transaction storage (16) and determining the associated value of the last signed transaction record in the transaction storage (16) as the last recorded value of the key usage counter, sending an indication (18) of said last recorded value to a signature device (8), receiving from the signature device (8) at least one previously signed transaction record (23), wherein the at least one previously signed transaction record (23) is loaded by the signature de vice (8) from a record buffer responsive to detecting a gap between a present value of the key usage counter and the received last recorded value; and storing the received at least one previously signed transaction record (23) in the transaction storage (16)."

Anspruch 12:

„A computer program comprising instructions to cause a signature device (8) comprising a key usage counter, which key usage counter is incremented with each signature generated by the signature device (8), and a record buffer (24) for buffering at least one previously signed transaction record (23), wherein each signed transaction record (15) comprises an associated value of a key usage counter at the time of the signature, to execute the steps of: receiving an indication (18) of a last recorded value of the key usage counter from a registration device (6),

loading at least one previously signed transaction record (23) from the record buffer (24) responsive to detecting a gap between a present value of the key usage counter and the received last recorded value, and transmitting the loaded at least one previously signed transaction record (23) to the registration device (6)."

4. In der eingetragenen deutschen Übersetzung lauten die Ansprüche wie folgt:

Anspruch 1:

„Verfahren zur sicheren Registrierung einer Folge von Transaktionen mit einem verteilten System (1), wobei das verteilte System (1) eine Registrierungsvorrichtung (6) und eine Signaturvorrichtung (8) aufweist, wobei die Registrierungsvorrichtung (6) einen Transaktionsspeicher (16) zum Speichern von signierten Transaktionsdatensätzen (15) auf weist, die von der Signaturvorrichtung (8) signiert wurden, wobei die Signaturvorrichtung (8) einen Schlüsselnutzungszähler aufweist, der mit jeder von der Signaturvorrichtung (8) erzeugten Signatur inkrementiert wird, wobei jeder signierte Transaktionsdatensatz (15) einen zugehörigen Wert des Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist, wobei das Verfahren aufweist: Vergleichen eines aktuellen Wertes des Schlüsselnutzungszählers mit einem zuletzt aufgezeichneten Wert, wobei der zuletzt aufgezeichnete Wert der zu gehörige Wert eines zuletzt signierten Transaktionsdatensatzes in dem Transaktionsspeicher (16) ist, Laden mindestens eines zuvor signierten Transaktionsdatensatzes (23) aus einem Datensatzpuffer (24) der Signaturvorrichtung (8) in Reaktion auf das Erfassen einer Lücke zwischen dem aktuellen Wert und dem zuletzt aufgezeichneten Wert, und Übertragen des geladenen, mindestens einen zuvor signierten Transaktionsdatensatzes (23) an die Registrierungsvorrichtung (6)."

Anspruch 6:

„Ein verteiltes System (1) zur sicheren Registrierung einer Folge von Transaktionen, wobei das verteilte System (1) eine Registrierungsvorrichtung (6) und eine Signaturvorrichtung (8) aufweist, wobei die Registrierungsvorrichtung (6) einen Transaktionsspeicher (16) zum Speichern von signierten Transaktionsdatensätzen (15) auf weist, die von der Signaturvorrichtung (8) signiert wurden, wobei die Signaturvorrichtung (8) einen Schlüsselnutzungszähler und einen Datensatzpuffer (24) zum Puffern von signierten Transaktionsdatensätzen (15) aufweist, wobei jeder signierte Transaktionsdatensatz (15) einen zugehörigen Wert des Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist, wobei die Signaturvorrichtung (8) so konfiguriert ist, dass sie mindestens einen zuvor signierten Transaktionsdatensatz (23) aus dem Datensatzpuffer (24) lädt, wenn eine Lücke zwischen einem aktuellen Wert des Schlüsselnutzungszählers und dem zugehörigen Wert eines letzten signierten Transaktionsdatensatzes im Transaktionsspeicher (16) erkannt wird, und dass sie den geladenen mindestens einen zuvor signierten Transaktionsdatensatz (23) an die Registrierungsvorrichtung (6) überträgt."

Anspruch 7:

„Verteiltes System (1) nach Anspruch 6, **dadurch gekennzeichnet, dass** die Registrierungsvorrichtung (6) so konfiguriert ist, dass sie eine Angabe (18) des zugehörigen Werts eines zuletzt signierten Transaktionsdatensatzes an die Signaturvorrichtung (8) sendet."

Anspruch 8:

„Verteiltes System nach Anspruch 7, **dadurch gekennzeichnet, dass** die Signaturvorrichtung (8) so konfiguriert ist, dass sie die Bereitstellung einer Signatur eines neuen, nicht signierten

Transaktionsdatensatzes (10) in Reaktion auf die Erkennung einer Lücke zwischen dem aktuellen Wert und dem zugehörigen Wert des letzten signierten Transaktionsdatensatzes ablehnt."

Anspruch 9:

„Verteiltes System nach Anspruch 6, **dadurch gekennzeichnet, dass** die Registrierungsvorrichtung (6) so konfiguriert ist, dass sie bei Empfang eines neuen signierten Transaktionsdatensatzes (15) von der Signaturvorrichtung (8) den zugehörigen Wert des neuen signierten Transaktionsdatensatzes (15) mit dem zugehörigen Wert des letzten signierten Transaktionsdatensatzes vergleicht und als Reaktion auf die Erkennung einer Lücke zwischen den verglichenen Werten eine erneute Übertragung von mindestens einem zuvor signierten Transaktionsdatensatz (23) von der Signaturvorrichtung (8) anfordert."

Anspruch 10:

„Computerprogramm mit Anweisungen, um eine Registrierungsvorrichtung (6), die einen Transaktionsspeicher (16) zum Speichern signierter Transaktionsdatensätze (15) aufweist, wobei jeder signierte Transaktionsdatensatz (15) einen zugehörigen Wert eines Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist, zu veranlassen, die folgenden Schritte auszuführen: Zugreifen auf den Transaktionsspeicher (16) und Bestimmen des zugehörigen Wertes des letzten signierten Transaktionsdatensatzes in dem Transaktionsspeicher (16) als den zuletzt aufgezeichneten Wert des Schlüsselnutzungszählers, Senden einer Angabe (18) des zuletzt aufgezeichneten Wertes an eine Signaturvorrichtung (8), Empfangen mindestens eines zuvor signierten Transaktionsdatensatzes (23) von der Signaturvorrichtung (8), wobei der mindestens eine zuvor signierte Transaktionsdatensatz (23) von der Signaturvorrichtung (8) aus einem Datensatzpuffer geladen wird, der auf das Erfassen einer Lücke zwischen einem aktuellen Wert des Schlüsselnutzungszählers und dem empfangenen zuletzt aufgezeichneten Wert reagiert; und Speichern des empfangenen mindestens einen zuvor signierten Transaktionsdatensatzes (23) in dem Transaktionsspeicher (16)."

Anspruch 12:

„Computerprogramm, das Anweisungen aufweist, um eine Signaturvorrichtung (8), die einen Schlüsselnutzungszähler aufweist, wobei der Schlüsselnutzungszähler mit jeder von der Signaturvorrichtung (8) erzeugten Signatur inkrementiert wird, und einen Datensatzpuffer (24) zum Puffern mindestens eines zuvor signierten Transaktionsdatensatzes (23) zu veranlassen, wobei jeder signierte Transaktionsdatensatz (15) einen zugehörigen Wert eines Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist, die folgenden Schritte auszuführen: Empfangen einer Angabe (18) eines zuletzt aufgezeichneten Wertes des Schlüsselnutzungszählers von einer Registrierungsvorrichtung (6), Laden mindestens eines zuvor signierten Transaktionsdatensatzes (23) aus dem Datensatzpuffer (24) in Reaktion auf das Erfassen einer Lücke zwischen einem aktuellen Wert des Schlüsselnutzungszählers und dem empfangenen zuletzt aufgezeichneten Wert, und Übertragen des geladenen, mindestens einen zuvor signierten Transaktionsdatensatzes (23) an die Registrierungsvorrichtung (6)."

5. Am 20. April 2026 hat die Antragstellerin einen Antrag auf Anordnung einer Inspektion und Beweissicherung an den deutschen Standorten der Antragsgegnerinnen gestellt.

6. Die Lokalkammer Düsseldorf hat daraufhin mit Anordnung vom 27. April 2026 Folgendes angeordnet:

„Es wird ohne vorherige Anhörung der Antragsgegnerinnen folgende Inspektions- und Beweissicherungsanordnung erlassen:

1. Der Antragstellerin wird gestattet, in Bezug auf eine Verwirklichung der Merkmale der Ansprüche 6 - 9, 1, 10 und 12 des Europäischen Patents EP 4 285 308 durch das Produkt Swissbit Cloud-TSE 2, die lauten:

> *Ein verteiltes System (1) zur sicheren Registrierung einer Folge von Transaktionen, wobei das verteilte System (1) eine Registrierungsvorrichtung (6) und eine Signaturvorrichtung (8) aufweist, wobei die Registrierungsvorrichtung (6) einen Transaktionsspeicher (16) zum Speichern von signierten Transaktionsdatensätzen (15) aufweist, die von der Signaturvorrichtung (8) signiert wurden, wobei die Signaturvorrichtung (8) einen Schlüsselnutzungszähler und einen Datensatzpuffer (24) zum Puffern von signierten Transaktionsdatensätzen (15) aufweist, wobei jeder signierte Transaktionsdatensatz (15) einen zugehörigen Wert des Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist, wobei die Signaturvorrichtung (8) so konfiguriert ist, dass sie mindestens einen zuvor signierten Transaktionsdatensatz (23) aus dem Datensatzpuffer (24) lädt, wenn eine Lücke zwischen einem aktuellen Wert des Schlüsselnutzungszählers und dem zugehörigen Wert eines letzten signierten Transaktionsdatensatzes im Transaktionsspeicher (16) erkannt wird, und dass sie den geladenen mindestens einen zuvor signierten Transaktionsdatensatz (23) an die Registrierungsvorrichtung(6) überträgt.*
>
> *(Anspruch 6)*
>
> *Verteiltes System (1) nach Anspruch 6, dadurch gekennzeichnet, dass die Registrierungsvorrichtung (6) so konfiguriert ist, dass sie eine Angabe (18) des zugehörigen Werts eines zuletzt signierten Transaktionsdatensatzes an die Signaturvorrichtung (8) sendet.*
>
> *(Anspruch 7)*
>
> *Verteiltes System nach Anspruch 7, dadurch gekennzeichnet, dass die Signaturvorrichtung (8) so konfiguriert ist, dass sie die Bereitstellung einer Signatur eines neuen, nicht signierten Transaktionsdatensatzes (10) in Reaktion auf die Erkennung einer Lücke zwischen dem aktuellen Wert und dem zugehörigen Wert des letzten signierten Transaktionsdatensatzes ablehnt.*
>
> *(Anspruch 8)*
>
> *Verteiltes System nach Anspruch 6, dadurch gekennzeichnet, dass die Registrierungsvorrichtung (6) so konfiguriert ist, dass sie bei Empfang eines neuen signierten Transaktionsdatensatzes (15) von der Signaturvorrichtung (8) den zugehörigen Wert des neuen signierten Transaktionsdatensatzes (15) mit dem zugehörigen Wert des letzten signierten Transaktionsdatensatzes vergleicht und als Reaktion auf die Erkennung einer Lücke zwischen den verglichenen Werten eine erneute Übertragung von mindestens einem zuvor signierten Transaktionsdatensatz (23) von der Signaturvorrichtung (8) anfordert.*
>
> *(Anspruch 9)*

Verfahren zur sicheren Registrierung einer Folge von Transaktionen mit einem verteilten System (1), wobei das verteilte System (1) eine Registrierungsvorrichtung (6) und eine Signaturvorrichtung (8) aufweist, wobei die Registrierungsvorrichtung (6) einen Transaktionsspeicher (16) zum Speichern von signierten Transaktionsdatensätzen (15) aufweist, die von der Signaturvorrichtung (8) signiert wurden, wobei die Signaturvorrichtung (8) einen Schlüsselnutzungszähler aufweist, der mit jeder von der Signaturvorrichtung (8) erzeugten Signatur inkrementiert wird, wobei jeder signierte Transaktionsdatensatz (15) einen zugehörigen Wert des Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist, wobei das Verfahren aufweist: Vergleichen eines aktuellen Wertes des Schlüsselnutzungszählers mit einem zuletzt aufgezeichneten Wert, wobei der zuletzt aufgezeichnete Wert der zugehörige Wert eines zuletzt signierten Transaktionsdatensatzes in dem Transaktionsspeicher (16) ist, Laden mindestens eines zuvor signierten Transaktionsdatensatzes (23) aus einem Datensatzpuffer (24) der Signaturvorrichtung (8) in Reaktion auf das Erfassen einer Lücke zwischen dem aktuellen Wert und dem zuletzt aufgezeichneten Wert, und Übertragen des geladenen, mindestens einen zuvor signierten Transaktionsdatensatzes (23) an die Registrierungsvorrichtung (6).

(Anspruch 1)

Computerprogramm mit Anweisungen, um eine Registrierungsvorrichtung (6), die einen Transaktionsspeicher (16) zum Speichern signierter Transaktionsdatensätze (15) aufweist, wobei jeder signierte Transaktionsdatensatz (15) einen zugehörigen Wert eines Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist, zu veranlassen, die folgenden Schritte auszuführen: Zugreifen auf den Transaktionsspeicher (16) und Bestimmen des zugehörigen Wertes des letzten signierten Transaktionsdatensatzes in dem Transaktionsspeicher (16) als den zuletzt aufgezeichneten Wert des Schlüsselnutzungszählers, Senden einer Angabe (18) des zuletzt aufgezeichneten Wertes an eine Signaturvorrichtung (8), Empfangen mindestens eines zuvor signierten Transaktionsdatensatzes (23) von der Signaturvorrichtung (8), wobei der mindestens eine zuvor signierte Transaktionsdatensatz (23) von der Signaturvorrichtung (8) aus einem Datensatzpuffer geladen wird, der auf das Erfassen einer Lücke zwischen einem aktuellen Wert des Schlüsselnutzungszählers und dem empfangenen zuletzt aufgezeichneten Wert reagiert; und Speichern des empfangenen mindestens einen zuvor signierten Transaktionsdatensatzes (23) in dem Transaktionsspeicher (16).

(Anspruch 10)

Computerprogramm, das

Anweisungen aufweist, um eine Signaturvorrichtung (8), die einen Schlüsselnutzungszähler aufweist, wobei der Schlüsselnutzungszähler mit jeder von der Signaturvorrichtung (8) erzeugten Signatur inkrementiert wird, und einen Datensatzpuffer (24) zum Puffern mindestens eines zuvor signierten Transaktionsdatensatzes (23) zu veranlassen, wobei jeder signierte Transaktionsdatensatz (15) einen zu gehörigen Wert eines Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist, die folgenden Schritte auszuführen: Empfangen einer Angabe (18) eines zuletzt auf- gezeichneten Wertes des Schlüsselnutzungszählers von einer Registrierungsvorrichtung (6), Laden mindestens eines zuvor signierten Transaktionsdatensatzes (23) aus dem Datensatzpuffer (24) in Reaktion auf das Erfassen einer Lücke

zwischen einem aktuellen Wert des Schlüsselnutzungszählers und dem empfangenen zuletzt aufgezeichneten Wert, und Übertragen des geladenen, mindestens einen zuvor signierten Transaktionsdatensatzes (23) an die Registrierungsvorrichtung (6).

(Anspruch 12)

a) die folgenden Dokumente und Unterlagen durch einen Sachverständigen zu inspizieren, die sich an den Standorten der Antragsgegnerinnen

- Bitterfelder Straße 22, 12681 Berlin und
- Leuchtenbergring 3, 81677 München

befinden, umfassend

aa) die Zertifizierungsunterlagen einschließlich des Prüfberichts für das Verfahren BSI K-TR-0612-2024 und davon insbesondere die im Kapitel 7.3/7.4 des Konformitätsreports erwähnten Dokumente einschließlich des Umgebungsschutzkonzepts (Secure Platform Concept) in der Version 1.0.2, und des Swissbit Cloud SMAERS – Guidance Documentation in der Version 1.0.3;

bb) Quellcodes sowie Softwaredokumentation einschließlich Ablaufdiagramme;

cc) Betriebs- und Installationshandbücher sowie Entwicklungsdokumentation einschließlich Lasten- und Pflichtenhefte;

dd) Konfigurationsdateien, Logs und Betriebsdaten einschließlich der Dokumentation über die spezifisch ablaufenden Softwareversionen in der Betriebsumgebung einschließlich der Aushändigung oder Anfertigung von Kopien und Offenlegung aller dafür erforderlichen Passwörter

und zu diesem Zweck die an den vorgenannten Standorten befindlichen Räume der Antragsgegnerinnen zu betreten;

b) Beweise zu sichern durch

aa) die Erstellung und Vorlage einer ausführlichen Beschreibung durch einen Sachverständigen über die Ergebnisse der Maßnahmen gemäß Ziffer 1. a) im Hinblick auf die Verwirklichung der Merkmale der Ansprüche 6 sowie 7 - 9, 1, 10 und 12 des Europäischen Patents EP 4 285 308, einschließlich einer detaillierten Beschreibung der Funktionsweise der Swissbit Cloud-TSE 2 der Antragsgegnerinnen und der Feststellung der konkret betriebenen Hard- und Softwareversionen (Hash-Werte) sowie eine Stellungnahme dazu, ob das Produkt die Merkmale der Ansprüche 6 sowie 7 - 9, 1, 10 und 12 des Europäischen Patents EP 4 285 308 verwirklicht,

bb) die Fertigung von Kopien oder Lichtbildern der vorgenannten Dokumente und Unterlagen in Bezug auf Design, Konfiguration, Zertifizierung und Ein-

satz der Swissbit Cloud-TSE 2 der Antragsgegnerinnen auf Kosten der Antragstellerin, soweit dies für die Erstellung der ausführlichen Beschreibung erforderlich ist,

cc) im Falle der Weigerung der Antragsgegnerinnen, Kopien gemäß Ziffer 1. b) bb) zu fertigen, die Beschlagnahme von Kopien oder Lichtbildern technischer Dokumentationen, interner Entwicklungsunterlagen und Handbüchern und Unterlagen in Bezug auf Design, Konfiguration, Zertifizierung und Einsatz der Swissbit Cloud-TSE 2 der Antragsgegnerinnen.

2. Der Sachverständige soll die gemäß Ziffer 1. b) aa) zu fertigende schriftliche Beschreibung innerhalb eines Monats nach Durchführung der Inspektion nach Ziffer I. 1. a) vorlegen.

Die von dem Sachverständigen zu fertigende ausführliche Beschreibung und alle anderen Ergebnisse der Inspektion und Beweissicherung dürfen nur in einem Hauptsacheverfahren gegen die Antragsgegnerin zu 1 und/oder die Antragsgegnerin zu 2 verwendet werden.

3. Als gerichtlicher Sachverständiger für die Durchführung der Maßnahmen gemäß Ziffer 1. wird bestellt:

Patentanwalt Lars Grannemann, Cohausz & Florack, Bleichstr. 14, 40211 Düsseldorf, hilfsweise ein anderer Patentanwalt der Kanzlei Cohausz & Florack, Bleichstr. 14, 40211 Düsseldorf.

Zur Unterstützung des Sachverständigen kann der Sachverständige nach eigenem Ermessen den IT-Forensiker

Dipl. Inf. Fabian Unucka, FAST-DETECT GmbH, Inselkammerstr. 12, 82008 Unterhaching, hilfsweise einen anderen IT-Fachmann der FAST-DETECT GmbH

als Hilfsperson zur Unterstützung hinziehen.

4. Zur Unterstützung des Sachverständigen und seiner Hilfspersonen werden die für die in Ziffer 1.a) der Anordnung genannten Standorte für die Inspektion örtlich zuständigen Gerichtsvollzieher als weitere Hilfspersonen bestimmt.

5. Neben dem gerichtlichen Sachverständigen und seinen Hilfspersonen gemäß Ziffer 3. darf an jedem der in Ziffer 1.a) genannten Standorte für die Inspektion jeweils ein rechtsanwaltlicher und ein patentanwaltlicher Vertreter der nachfolgend angeführten UPC-Vertreter der Antragstellerin bei der Durchführung der Maßnahmen gemäß Ziffer 1. a) anwesend sein:

Sebastian Dworschak
Dr. Lorenz Müller-Tamm
Ralf Emig
Dr. Gunnar Baumgärtel.

Vertretungsorgane, Angestellte oder sonstige Mitarbeiter der Antragstellerin dürfen bei der Durchführung der unter Ziffer 1. genannten Maßnahmen nicht anwesend sein.

6. Den Antragsgegnerinnen wird aufgegeben,

   a) dem gerichtlichen Sachverständigen, seinen Hilfspersonen und den unter Ziffer 5. aufgeführten UPC-Vertretern der Antragstellerin den Zutritt zu den unter Ziffer 1. a) genannten Räumlichkeiten zu gestatten;

   b) dem gerichtlichen Sachverständigen und seinen Hilfspersonen Zugang zur Betriebsumgebung der Swissbit Cloud-TSE 2 zu gewähren und insbesondere die Feststellung zu ermöglichen, welche konkreten Software- und Hardwareversionen der TSE-Komponenten tatsächlich betrieben werden sowie auf Anforderung des Sachverständigen eine Instanz der Swissbit Cloud-TSE 2 Komponenten in Betrieb zu setzen;

   c) dem gerichtlichen Sachverständigen sowie seinen Hilfspersonen zu gestatten, zu Dokumentationszwecken zu fotografieren oder zu filmen, schriftliche Notizen anzufertigen und/oder für seine Notizen ein Diktiergerät zu verwenden und auf Kosten der Antragstellerin Kopien und Ausdrucke anzufertigen;

   d) digitale Beweise, d.h. die Zertifizierungsunterlagen (einschließlich des Prüfberichts für das Verfahren BSI-K-TR-0612-2024 und davon insbesondere die im Kapitel 7.3/7.4 des Konformitätsreports erwähnten Dokumente einschließlich des Umgebungsschutzkonzepts (Secure Platform Concept) in der Version 1.0.2, und des Swissbit Cloud SMA ERS – Guidance Documentation in der Version 1.0.3); Quellcodes sowie Softwaredokumentation einschließlich Ablaufdiagramme, Betriebs- und Installationshandbücher sowie Entwicklungsdokumentation einschließlich Lasten- und Pflichtenhefte; Konfigurationsdateien, Logs und Betriebsdaten einschließlich der Dokumentation über die spezifisch ablaufende Software- und Hardwareversion aller TSE-Komponenten in der Betriebsumgebung in Bezug auf die Swissbit Cloud-TSE 2 der Antragsgegnerinnen bereitzustellen sowie alle Passwörter und Daten offenzulegen, die zum Zugang zu den digitalen Beweisen erforderlich sind;

   e) dem gerichtlichen Sachverständigen sowie seinen Hilfspersonen zu gestatten, Kopien der digitalen Beweise anzufertigen;

   f) dem gerichtlichen Sachverständigen und seinen Hilfspersonen technische Dokumentationen, interne Entwicklungsunterlagen und Handbücher und Unterlagen in Bezug auf Design, Konfiguration, Zertifizierung und Einsatz der Swissbit Cloud-TSE 2 der Antragsgegnerinnen auszuhändigen oder, hilfsweise, dem gerichtlichen Sachverständigen und seinen Hilfspersonen zu gestatten, Kopien dieser Unterlagen anzufertigen;

   g) dem Sachverständigen und seinen Hilfspersonen den genauen Aufbewahrungsort der unter Ziffer 1 genannten Beweismittel zu benennen und Zugangshindernisse, wie z.B. einen Passwortschutz für den Zugriff auf elektronische Dokumente zu beseitigen oder etwaig verschlossene Räume oder Schränke zu öffnen.

7. Die an der Durchführung der Inspektion und der Beweissicherung beteiligten Perso-nen und insbesondere der Gerichtsvollzieher, der Sachverständige einschließlich seiner Hilfsperson und die Parteivertreter der Antragstellerin sind verpflichtet, Tatsachen, die ihnen im Rahmen der Ausführung der gesamten Anordnung zur Kenntnis gelangen, sowohl gegenüber Dritten als auch gegenüber der Antragstellerin geheim zu halten.

Zudem dürfen die vorgenannten Personen bis zu einer Freigabeanordnung des Einheitlichen Patentgerichts keine Gelegenheit bieten, der Antragstellerin oder Dritten Einblick in die als „Swissbit Cloud-TSE 2“ bezeichnete, cloudbasierte und zertifizierte technische Sicherheitseinrichtung der Antragsgegnerinnen, in die ggf. beschlagnahmten Unterlagen sowie in die durch den Sachverständigen zu fertigende ausführliche Beschreibung zu gewähren.

8. Die Antragsgegnerinnen sollen aufgefordert werden, nach Vorlage der ausführlichen Beschreibung des Sachverständigen zu etwaigen Geheimhaltungsinteressen Stellung zu nehmen. Den unter Ziffer 5. genannten UPC-Vertretern der Antragstellerin wird Gelegenheit gegeben werden, sich zur Stellungnahme der Antragsgegnerinnen zu äußern. Danach entscheidet das Gericht, ob und inwieweit die ausführliche Beschreibung des Sachverständigen und die gesicherten Beweise der Antragstellerin persönlich zur Kenntnis gebracht werden sollen und ob die Verschwiegenheitspflicht für die unter Ziffer 5. genannten UPC-Vertreter der Antragstellerin aufzuheben ist.

9. Die Antragstellerin ist verpflichtet, die Kosten der Inspektion und Beweissicherung einschließlich der Erstellung der ausführlichen Beschreibung durch den Sachverständigen zu tragen. Der Antragstellerin wird aufgetragen, vor Beginn der Inspektion dem Sachverständigen einen angemessenen, von diesem zu bestimmenden Kostenvorschuss zu zahlen, soweit dieser nicht auf einen solchen Kostenvorschuss verzichtet.

10. Die Anordnung ist den Antragsgegnerinnen persönlich in den unter Ziffer 1. a) genannten Räumlichkeiten durch einen der unter Ziffer 5. genannten UPC-Vertreter der Antragstellerin zuzustellen, zusammen mit einer Kopie des Antrags einschließlich seiner Anlagen sowie der Mitteilung über vorläufige Maßnahmen und den Anweisungen für den Zugang zum Verfahren (bereitgestellt durch das CMS), unverzüglich im Zeitpunkt der Durchführung der Maßnahmen gemäß Ziffer 1. Die Zustellung dieser Unterlagen soll im Zusammenwirken mit dem jeweils anwesenden, gem. Ziff. 4 der Anordnung bestellten Gerichtsvollzieher erfolgen. Sollte eine Zustellung an die Antragsgegnerin zu 1 in den unter Ziffer 1. a) genannten Räumlichkeiten nicht möglich sein, ist die Anordnung gemäß den allgemeinen Regeln zuzustellen.

11. Bei schuldhafter Zuwiderhandlung gegen diese Anordnung kann das Gericht für jeden Verstoß ein Zwangsgeld festsetzen, dessen Höhe das Gericht unter Berücksichtigung der Umstände des Einzelfalls bestimmen kann.

12. Die Maßnahmen zur Inspektion und zur Beweissicherung werden auf Antrag der Antragsgegnerinnen aufgehoben oder treten anderweitig außer Kraft, wenn die Antragstellerin nicht innerhalb einer Frist von höchstens 31 Kalendertagen oder 20 Arbeitstagen, je nachdem, welcher Zeitraum länger ist, nachdem die nach Ziffer 1. b) aa) durch den Sachverständigen zu erstellende ausführliche Beschreibung der Antragstellerin offengelegt wurde oder das Gericht durch eine endgültige Entscheidung entschieden hat, keinen Zugang zu dieser ausführlichen Beschreibung zu gewähren, eine Klage gegen die Antragsgegnerinnen erhoben hat.

13. Die Anordnung wird erst wirksam, wenn die Antragstellerin zugunsten der Antragsgegnerinnen eine Sicherheit in Form der Hinterlegung in Höhe von 10.000,00 EUR geleistet hat.

14. Im Übrigen wird der Antrag auf Inspektion und Beweissicherung zurückgewiesen.“

7. Die Inspektion und Beweissicherung fand am 19. Mai 2026 statt.

8. Der Sachverständige Grannemann führte die Inspektion und Beweissicherung am Münchner Standort der Antragsgegnerinnen durch, unterstützt durch die Obergerichtsvollzieherin Seisenberger und die IT-Forensiker Dipl. Inf. Unucka und Aßmus (siehe ausführlicher Bericht des Sachverständigen vom 15. Juni 2026 sowie Vollstreckungsprotokoll vom 19. Mai 2026). Vor Ort zeitlich durchgehend anwesend waren weiterhin der Vertreter der Antragstellerin, Rechtsanwalt Sebastian Dworschak, der Vertreter der Antragstellerin, Patentanwalt Ralf Emig, sowie zeitweise der Vertreter der Antragsgegnerin zu 2), Patentanwalt Michael Platzöder, der Vertreter der Antragsgegnerin zu 2) Rechtsanwalt Dr. Thomas Lynker, weiters Zeljko Angeloski, Director Marketing bei der Antragsgegnerin zu 2), sowie Hubertus Grobbel, Vice President Security Solutions, laut eigener Aussage angestellt bei der Antragsgegnerin zu 2. Ferner waren zwischenzeitlich per Video Chris Schwarze, Geschäftsführer der Antragsgegnerin zu 2), sowie Nicolas Schneider, Technischer Leiter der Antragsgegnerin zu 2), zugeschaltet.

9. Bei der Inspektion und Beweissicherung wurden die nachfolgend genannten Dokumente betreffend die festgestellten Softwareversionen inspiziert und gesichert:

   a) Swissbit Cloud CSP-L - Guidance Documentation, Version 1.1.5 (d2dac dec38e278adc011f1af19660d13b12c4a22), 2024-11-06 (Anlage SV1)

   b) Swissbit Cloud-TSE 2 - Secure Platform Concept (Umgebungsschutzkonzept, USK), Version 1.0.2 (7180367829459d9466d54daee97a431f04ad1d39), 2024-07-09 (Anlage SV2)

   c) Swissbit Cloud-TSE 2 - Trust Provisioning Concept, Version 1.0.3 (2e3d02f82937bc525387dd867faef2321211a281), 2024-08-30 (Anlage SV3)

   d) Betriebshandbuch CSPL (Cryptographic Service Provider Light), Doc ID 7622, Rev. 00, Temp. ID T4653, T_Rev. 00, L_review 12.06.2025, Verantwortlicher Hubertus Grobbel (hier die Seiten 1-13 auszugsweise als Anlage SV4)

   e) Swissbit Cloud SMAERS – Guidance Documentation, Version 1.0.3 (2e3d02f82937bc525387dd867faef2321211a281), 2024-08-30 (Anlage SV5)

   f) Swissbit Cloud-TSE 2 - Update Concept, Version 1.0.2 (7053f1e02a2b7328810bad83cc35681a81da34ae), 2024-08-09

   g) Swissbit Cloud-TSE 2 - CSP Configuration and Operation Concept (CSP Konfigurationskonzept), Version 1.1.3 (6fc1986579d71978b5892d1e143b2ef4e10cf7e4), 2024-07-22

   h) Swissbit Cloud CSP-L - Security Architecture (ARC), Version 1.1.2 (0fcba72f0dfa9bf44b86fa50867176eb8f4fff6c), 2024-07-08

   i) Swissbit Cloud CSP-L - TOE Design (TDS), Version 1.3.1 (0fcba72f0dfa9bf44b86fa50867176eb8f4fff6c), 2024-07-08 (Anlage SV6)

j) Quellcodepaket fiscal3-smaers-smaers-v1.0.5, umfassend u.a. die Dateien Csp.java (Anlage SV7a)

- CspImpl.java (Anlage SV7b)
- SmaersUnitImpl.java (Anlage SV7c)
- CspImplIntegrationTest.java (Anlage SV7d)
- SmaersUnitImplTest.java (Anlage SV7e)
- FuryInstance.java (Anlage SV7f)

k) Quellcodepaket fiscal3-cspl-v1.0.7, umfassend u.a. die Dateien

- ConfirmUsageCounterRequest.java (Anlage SV8a)
- ConfirmUsageCounterResponse.java (Anlage SV8b)
- ConfirmUsageCounterHandler.java (Anlage SV8c)
- UnconfirmedSignaturesErrorResponse.java (Anlage SV8d)
- UnconfirmedItem.java (Anlage SV8e)
- UnconfirmedItemType.java (Anlage SV8f)
- SignatureObject.java (Anlage SV8g)
- AuditRecordList.java (Anlage SV8h)
- UnconfirmedItemIntern.java (Anlage SV8i)
- AuditRecordStorageImpl.java (Anlage SV8j)
- TimestampDataRequest.java (Anlage SV8k)
- TimestampDataResponse.java (Anlage SV8l)
- TimestampDataHandler.java (Anlage SV8m)

l) Quellcodepaket fiscal3-smaers-tss-v1.0.5

10. Der Sachverständige hat am 15. Juni 2026 seine ausführliche Beschreibung erstellt.

11. Mit Schriftsatz vom 18. Juni 2026 haben die Antragsgegnerinnen einen Antrag auf Prüfung der Anordnung auf Inspektion und Beweissicherung nach R. 197.3 VerfO gestellt, über den die Lokalkammer Düsseldorf am 25. August 2026 online mündlich verhandelt hat.

ANTRÄGE:

12. Die Antragsgegnerinnen beantragen,

    I. die Anordnung der Lokalkammer Düsseldorf vom 27. April 2026, Az. UPC_CFI_1332/2026, in der mündlichen Verhandlung zu überprüfen;

    II. die Anordnung der Lokalkammer Düsseldorf vom 27. April 2026, Az. UPC_CFI_1332/2026, aufzuheben;

    hilfsweise,

    III. die Anordnung der Lokalkammer Düsseldorf vom 27. April 2026, Az. UPC_CFI_1332/2026, abzuändern und zusätzlich dem Sachverständigen in der zu prüfenden Anordnung aufzugeben, im Falle der Erhebung einer Hauptsacheklage die Produkte, Dokumente, Unterlagen und/oder Medien nach beendeter Erstellung der ausführlichen Beschreibung zum Gericht zu verbringen.

13. Die Antragstellerin beantragt,

    die Anordnung der Lokalkammer Düsseldorf vom 27. April 2026 zu bestätigen.

TATSÄCHLICHE UND RECHTLICHE STREITPUNKTE:

14. Die Antragsgegnerinnen tragen vor:

15. Von der Antragstellerin sei eine hinreichende Verletzungswahrscheinlichkeit für die streitentscheidenden Merkmale 6.4b und 6.6 des Anspruchs 6 des Antragspatents, die den sog. Lückenfüll-Mechanismus betreffen, nicht dargelegt worden. Die genannten Merkmale lauten wie folgt:

    6.4b [wobei die Signaturvorrichtung (8)] einen Datensatzpuffer (24) zum Puffern von signierten Transaktionsdatensätzen (15) aufweist

    6.6a wobei die Signaturvorrichtung (8) so konfiguriert ist, dass sie mindestens einen zuvor signierten Transaktionsdatensatz (23) aus dem Datensatzpuffer (24) lädt, wenn eine Lücke zwischen einem aktuellen Wert des Schlüsselnutzungszählers und dem zugehörigen Wert eines letzten signierten Transaktionsdatensatzes im Transaktionsspeicher (16) erkannt wird

    6.6b und [wobei die Signaturvorrichtung (8) so konfiguriert ist,] dass sie den geladenen mindestens einen zuvor signierten Transaktionsdatensatz (23) an die Registrierungsvorrichtung (6) überträgt

16. Ob und inwieweit die streitgegenständliche Ausführungsform diesen Mechanismus tatsächlich umsetze, sei der Antragstellerin nach eigenem Bekunden nicht bekannt. Dementsprechend stütze sie sich zur Begründung ihres Antrags ausschließlich auf ein Parteigutachten

von Prof. Dr. Eidenberger, der eine Verwirklichung zwar als „hoch wahrscheinlich“ einschätze, dies allerdings auf die fernliegende Erwägung stütze, dass die regulatorischen Rahmenbedingungen den technischen Spielraum derart einschränkten, dass nur die patentgemäße Lösung in Betracht komme. Letzteres sei offensichtlich unzutreffend.

17. Die BSI-Richtlinie TR-03153 verlange, dass bei der Übertragung keine Nachrichten verloren gehen und keine Lücken in den Sequenzen entstehen (vgl. auch Antragsschrift, Rdn. 100). Die Richtlinie schreibe aber gerade keine konkrete interne Algorithmik und insbesondere auch keine Pufferspeicherung signierter Datensätze in der Signaturvorrichtung vor. Dies würden auch die Antragstellerin und ihr Gutachter anerkennen.

18. Es sei nicht tragfähig, dass die Lokalkammer „*im Hinblick auf das Gutachten […]*“ eine Verwirklichung dieser Merkmale gleichwohl für wahrscheinlich gehalten habe. Die Antragstellerin und ihr Gutachter hätten eine gleichwertige, nicht patentverletzende Alternative vielmehr bereits selbst aktenkundig gemacht, in welcher das Problem von Verbindungsabbrüchen ebenfalls gelöst werden müsse, hierzu aber jedenfalls kein Speichermedium in der Signaturvorrichtung erforderlich sei.

19. Im Übrigen kämen zahlreiche technische Alternativen in Betracht, um das vermeintliche, von der Antragstellerin ausgemachte „Lückenproblem“ von vornherein vollständig zu vermeiden. Bei diesen technischen Alternativen seien die Merkmale 6.4b, 6.6a und 6.6b des Anspruchs 6 des Antragspatents ebenfalls nicht verwirklicht, die Richtlinienkonformität aber gleichwohl gewährleistet. Unter Berücksichtigung dieser patentfreien Alternativen hätte die Lokalkammer eine hinreichende Verletzungswahrscheinlichkeit zu verneinen gehabt.

20. Selbst wenn man von einer hinreichenden Verletzungswahrscheinlichkeit ausginge, hätte die Antragstellerin jedenfalls aber alle sonstigen, ihr zur Verfügung stehenden Beweismöglichkeiten ausschöpfen müssen, was sie nicht getan habe. Die Antragstellerin hätte ihre vergeblichen Bemühungen konkret darzulegen gehabt, etwa Internetrecherchen, Werbematerialanalysen, ein Testkauf und eine technische Überprüfung der angegriffenen Ausführungsform sowie Ermittlungen bei Abnehmern. Aus den Ausführungen der Antragstellerin sei dies jedenfalls nicht ersichtlich. Es fehle jede Konkretisierung, welche Erwerbsversuche wann und bei welchem Distributor unternommen wurden, sodass die Interessenabwägung zu Lasten der Antragstellerin ausfalle.

21. Im Übrigen habe die Lokalkammer auch zu Unrecht angenommen, dass der Antrag der Antragstellerin dringlich und der Erlass der Anordnung *ex-parte* erforderlich gewesen sei. Es habe weder die Gefahr einer Vernichtung von Beweismitteln noch die Gefahr bestanden, dass diese aus anderen Gründen nicht mehr verfügbar sein könnten. Der Umstand, dass die angegriffene Ausführungsform BSI-zertifiziert (BSI-K-TR-0612-2024) sei, spreche bereits unmittelbar gegen eine Gefahr der Manipulation oder Unterlagenvernichtung, denn dies hätte den Zertifizierungsverlust zur Folge.

22. Die Annahme, dass die Antragsgegnerinnen den Source Code oder andere Unterlagen hätten verstecken oder unzugänglich machen können, sei ebenfalls angesichts ihrer BSI- und ISO-27001-Zertifizierungen unrealistisch. Aufgrund der zertifizierten Geschäftsprozesse müssten Mitarbeitende unabhängig vom Speicherort jederzeit Zugriff auf die Systeme haben. Daher hätte sich die Antragsgegnerin auch nicht mit dem Hinweis auf eine Speicherung in der

Schweiz der Herausgabe des Source Codes entziehen können, was der Antragstellerin bekannt gewesen sei. Überdies sei eine Vollstreckung in der Schweiz aufgrund deren Mitgliedschaft zum Lugano-Abkommen gewährleistet.

23. Des Weiteren hätte die Lokalkammer angesichts zahlreicher Alternativen zur patentgemäßen Lösung zumindest im inter partes Verfahren mit den Parteien zu diskutieren gehabt, ob die patentgemäße Lösung verwirklicht ist.

24. Ferner würde der Zeitablauf zwischen Kenntniserlangung von der zu untersuchenden Ausführungsform im April 2025 und der Antragstellung am 20. April 2026 gegen die für eine Ex-parte-Anordnung erforderliche Dringlichkeit sprechen.

25. Die Beweissicherungs- und Inspektionsanordnung sei zudem auch unverhältnismäßig. Wie sich aus Rn. 147 der Antragsschrift ergebe, beziehe sich die BSI-Zertifizierung auf konkret geprüfte Software-Versionen, deren Komponenten über spezifische Hash-Werte identifizierbar seien. Die Nutzung einer veränderten Software würde außerhalb der – verpflichtend vorgeschriebenen – Zertifizierung erfolgen.

26. Daraus ergebe sich unmittelbar, dass jede Veränderung der zertifizierten Software der Antragsgegnerinnen stets zu 100 % nachweisbar sei. Denn ergebe sich in Bezug auf einen bestimmten Source Code ein anderer Hash-Wert als der für die zertifizierte Software hinterlegte Hash-Wert, sei dies ein unmittelbarer Beweis dafür, dass es sich nicht um den Source Code der zertifizierten Software handle. Dieser Umstand hätte für die Lokalkammer Anlass genug sein müssen, mildere Mittel als das mit der Anordnung gewährte unangekündigte und zwangsweise Eindringen in die Geschäftsräume der Antragsgegnerinnen nebst Beschlagnahme des Source Codes in Betracht zu ziehen. Eine Vorlageanordnung hinsichtlich des Source Codes hätte jedenfalls dem Anliegen der Antragstellerin in gleicher Weise Rechnung tragen können. Mit dem Source Code hätte die Antragstellerin alles erlangt, was notwendig ist, um zu prüfen, ob eine Verwirklichung der Merkmale 6.4b und 6.6 vorliegt oder nicht. Eine weitere Dokumentation, Logfiles oder dergleichen sowie die Betrachtung der Nutzung der Software in der Betriebsumgebung sei hierfür nicht erforderlich.

27. Im Übrigen sei die Anordnung auch angesichts der zwischen den Parteien laufenden Lizenzverhandlungen nicht angemessen. Die Antragstellerin habe in der Antragsschrift zu den Lizenzverhandlungen nur unvollständig vorgetragen und so ein unzutreffendes Bild erzeugt. Zum Zeitpunkt der Antragstellung am 20. April 2026 hätten die Lizenzverhandlungen zwischen den Parteien nämlich noch angedauert und seien aus Sicht der Antragsgegnerinnen auch durchaus (noch) erfolgversprechend gewesen.

28. Die Antragstellerin trägt vor:

29. Die Merkmale 6.1-6.4a und 6.5 hätten bereits auf Grundlage der Zertifizierungen und maßgeblichen BSI-Richtlinien sicher festgestellt werden können. Nur bezüglich der Merkmale 6.4b und 6.6 hätten Restzweifel bestanden, wobei sich hinsichtlich dieser Merkmale die hinreichende Verletzungswahrscheinlichkeit aus den regulatorischen Rahmenbedingungen und dem Gutachten von Prof. Eidenberger ergebe.

30. Die von den Antragsgegnerinnen vorgetragenen denkbaren Alternativen – deren Gleichwertigkeit mit der patentgemäßen Lösung bestritten werde – stünden dem Erlass einer Beweissicherungs- und Inspektionsanordnung nicht entgegen.

31. Die Antragsgegnerinnen hätten auch nicht dargestellt, dass die zu untersuchende Ausführungsform mit höherer Wahrscheinlichkeit einen anderen als den patentgemäßen Mechanismus zur Herstellung der Lückenlosigkeit der Transaktionsdatensätze nutzen würde.

32. Bereits der Umstand, dass die patentgemäße Lösung seit Veröffentlichung der Patentanmeldung des Antragspatents öffentlich zugänglich sei, lege bei einer Ex-ante-Betrachtung nahe, dass die Antragsgegnerinnen die patentgemäße Lösung verwenden würden. Der weitere Umstand, dass in der von den Antragsgegnerinnen eingereichten Schutzschrift keine Nichtverletzungsargumentation enthalten sei, habe zusätzlich ex ante die Verletzungswahrscheinlichkeit erhärtet. Auf diese Ex-ante-Sicht komme es an.

33. Gleichermaßen habe der Umstand, dass sich die Antragsgegnerinnen außergerichtlich, etwa im Wege der geführten Lizenzverhandlungen, geweigert hätten, die von ihnen gewählte Lösung zur Herstellung der Lückenlosigkeit der Transaktionsdatensätze offenzulegen, ex ante die Verletzungswahrscheinlichkeit zusätzlich erhärtet.

34. Außerdem sei die Besichtigung für die Antragstellerin auch erforderlich gewesen, um die Patentverletzung sicher nachweisen zu können. Alle sonstigen zumutbaren Erkenntnisquellen habe die Antragstellerin zuvor bereits ausgeschöpft. Sie habe insbesondere auch umfassende Recherchen in öffentlich zugänglichen Quellen vorgenommen, wie die Quellennachweise im Besichtigungsantrag zeigen würden.

35. Die für den Nachweis der Anspruchsverwirklichung relevanten Abläufe der angegriffenen Ausführungsform – gerade im Hinblick auf den Lückenfüll-Mechanismus in der Signaturvorrichtung – liefen auf einer speziellen, gesicherten Infrastruktur in der Cloud ab. Der testweise Erwerb hätte zwar die Nutzung der angegriffenen Ausführungsform ermöglicht, jedoch wäre es kaum denkbar gewesen, hieraus Rückschlüsse auf die konkrete Ausgestaltung des Lückenfüll-Mechanismus zu ziehen. Ein Erwerb der angegriffenen Ausführungsform sei versucht worden, jedoch gescheitert. Abgesehen davon hätte dieser ohnehin nicht zur Aufklärung beitragen können und wäre nicht nur kein „gleich wirksames“ Mittel, sondern vollständig ungeeignet zur weiteren Aufklärung der Patentverletzung gewesen.

36. Es erscheine schon ausgeschlossen, dass Nutzer der Software überhaupt technisch Zugang zu dem Software-Code hätten und diesen dekompilieren könnten. Damit sei schon aus technischer Sicht ausgeschlossen, dass ein testweiser Erwerb geeignet gewesen wäre, die Patentverletzung weiter aufzuklären. Zum anderen sei die Dekompilierung aus urheberrechtlicher Sicht grundsätzlich dem Rechtsinhaber vorbehalten und damit auch der Antragstellerin nicht gestattet, auch nicht zur Beschaffung von Verletzungsnachweisen.

37. Darüber hinaus sei es zum Nachweis, ob die patentgemäße Lösung benutzt werde, erforderlich, neben dem Source Code auch weitere Informationen, wie insbesondere Entwicklungsinformationen, zu erlangen, und darüber hinaus auch die Betriebsumgebung und die Systemarchitektur der angegriffenen Ausführungsform in laufendem Betrieb zu betrachten.

38. Zur Anordnung ex-parte bringt die Antragstellerin vor, die Antragsgegnerinnen hätten in ihrem Überprüfungsantrag keine neuen Tatsachen oder Beweismittel vorgetragen, sodass dem Gericht keine andere Tatsachengrundlage vorliege, als wenn es kurzfristig eine Anhörung vor Erlass der Anordnung durchgeführt hätte.

39. Die länderübergreifende Gesellschaftsstruktur der Antragsgegnerinnen – mit Sitz der zertifizierten Antragsgegnerin zu 1) im Ausland in der Schweiz – begründe ferner eine konkrete Gefahr für die mögliche Beweisvereitelung bei Ankündigung einer Beweissicherungs- und Inspektionsmaßnahme – insbesondere sei dies aus Ex-ante-Sicht so.

40. So sei es gerade bei Cloud-Lösungen wie der streitgegenständlichen Ausführungsform möglich, den faktischen Zugriff auf die Cloud bzw. die dahinterstehende Systemarchitektur und den Quellcode zu erschweren und zu vereiteln.

41. Auch die Zertifizierung der streitgegenständlichen Ausführungsform schließe Vereitelungshandlungen nicht aus. Zwar sei eine Veränderung der Software aufgrund der spezifischen Hash-Werte tatsächlich grundsätzlich feststellbar. Die Zertifizierung hätte die Antragsgegnerinnen allerdings nicht daran gehindert, den Zugriff auf Dokumente, Log-Files und Quellcode bei entsprechender Vorwarnung durch eine Anhörung zu erschweren oder zu verweigern. Entscheidend sei nicht nur die Frage der Manipulierbarkeit, sondern insbesondere auch die der Auffindbarkeit.

42. Im Übrigen stehe auch die seit 2025 bestehende Kenntnis der Antragstellerin vom Angebot der angegriffenen Ausführungsform nicht dem Erlass der Besichtigungsanordnung entgegen, da eine Besichtigungsanordnung keine zeitliche Dringlichkeit erfordere.

43. Die Anordnung sei auch verhältnismäßig. Insbesondere stelle die Besichtigungsanordnung das mildeste geeignete Mittel zur Beweissicherung dar. Alternativen habe die Antragstellerin entweder ausgeschöpft oder sie seien nicht gleichwertig gewesen.

44. Auch wäre eine Anordnung auf Beweisvorlage gemäß Art. 59 EPGÜ nicht gleichwertig gewesen. Eine solche Anordnung dürfe nach Art. 59 Abs. 1 S. 2 EPGÜ nicht zu einer Pflicht zur (strafrechtlichen) Selbstbelastung führen, d.h., die Antragsgegnerinnen hätten auf dieser Grundlage selbst die Beweismittel selektieren und die für die Patentverletzung entscheidenden Informationen zurückhalten können. Auch hätte es die bloße Dokumentenvorlage nicht ermöglicht, die Betriebsumgebung und die Systemarchitektur der zu untersuchenden Ausführungsform in laufendem Betrieb zu betrachten. Im Übrigen sei eine Beweissicherungs- und Inspektionsanordnung gemäß Art. 60 EPGÜ auch nicht subsidiär zu einer Beweisvorlage nach Art. 59 EPGÜ.

45. Das Verfahren nach Art. 60 EPGÜ beinhalte ferner schon seiner Struktur nach einen Ausgleich der Interessen von Besichtigungsschuldner und -gläubiger.

46. Die Anordnung vom 27. April 2026 enthalte im Übrigen in den Ziff. 5, 7, 8 und 13 umfangreiche Schutzvorkehrungen zugunsten der Antragsgegnerinnen: Der Sachverständige sei gegenüber Dritten zur Verschwiegenheit verpflichtet, die Antragstellerin persönlich von der Teilnahme ausgeschlossen, der gerichtliche Sachverständige als Kontrollinstanz dazwischen-

geschaltet, ein Entscheidungsvorbehalt des Gerichts über die Offenlegung des Sachverständigenberichts festgelegt und die Hinterlegung einer Sicherheit angeordnet worden.

47. Auch angesichts der Lizenzverhandlungen zwischen den Parteien bleibe die Anordnung verhältnismäßig. Nicht nachvollziehbar sei die Ausführung der Antragsgegnerinnen, dass der Besichtigungsantrag für sie „völlig überraschend“ gekommen sei, obwohl sie im November 2025 eine Schutzschrift hinterlegt hatten. Die Antragstellerin sei an einer gemeinsamen Lösung der Auseinandersetzung interessiert gewesen und habe dazu die Begutachtung durch eine neutrale Stelle vorgeschlagen. Dies hätten die Antragsgegnerinnen jedoch abgelehnt.

48. Ergänzend wird auf das schriftsätzliche Vorbringen der Parteien Bezug genommen.

GRÜNDE DER ANORDNUNG:

49. Der Prüfungsantrag der Antragsgegnerinnen ist zulässig. Er ist jedoch in weiten Teilen unbegründet und hat nur im Umfang des Hilfsantrages Erfolg.

I. Zulässigkeit des Prüfungsantrags

50. Gegen die Zulässigkeit des Prüfungsantrags bestehen keine Bedenken.

51. Gemäß R. 197.3 VerfO ist der Antrag auf Prüfung der Anordnung zur Beweissicherung 30 Tage nach Vollziehung der Maßnahme zu stellen. Die Beweissicherung und Inspektion erfolgte am 19. Mai 2026. Die Antragsgegnerinnen haben den Überprüfungsantrag am 18. Juni 2026 und somit fristgerecht bei Gericht eingereicht.

II. (Un-)Begründetheit des Prüfungsantrags

52. Der Prüfungsantrag der Antragsgegnerinnen hat in der Sache nur hinsichtlich des Hilfsantrags Erfolg.

1. Grundsätze

53. Die Lokalkammer Düsseldorf hat sich bereits in der Vergangenheit den von der Lokalkammer Brüssel in der Anordnung vom 12. November 2025 (UPC_CFI_407/2025 – Organon Heist v. Genentech) aufgestellten Grundsätzen angeschlossen (siehe bereits UPC_CFI_834/2025 (LK Düsseldorf), Anordnung vom 19. Dezember 2025, Rn. 34 ff. – Ecovacs Robotics v. Roborock) und hält daran fest. Danach hat das Gericht im Rahmen der Prüfung nach R. 197.3 VerfO eine doppelte Prüfung vorzunehmen:

54. Zunächst hat das Gericht zu prüfen, ob es zu Recht entschieden hat, eine Ex-parte-Anordnung zur Inspektion und Beweissicherung zu erlassen (R. 194.1 (d) i.V.m. R. 194.2 VerfO). Bei dieser Beurteilung muss das Gericht die Tatsachen und Beweismittel berücksichtigen, (i) die im Antrag auf Erlass einer Anordnung zur Inspektion und Beweissicherung vorgebracht wurden, und (ii) die, sofern sie dem Gericht nicht offengelegt wurden, entweder öffentlich bekannt sind oder als dem Antragsteller vernünftigerweise bekannt gelten. Sofern Tatsachen und Beweismittel nicht offengelegt wurden, hat das Gericht zu prüfen, ob dieses Versäumnis als Verletzung der Pflicht des Antragstellers nach R. 192.3 VerfO anzusehen ist. Danach hat der Antragsteller alle ihm bekannten Tatsachen

offenzulegen, welche die Entscheidung des Gerichts darüber, ob eine Anordnung ohne Anhörung des Antragsgegners zu erlassen ist, beeinflussen könnten.

55. Anschließend hat das Gericht zu prüfen, ob die Anordnung zur Inspektion und Beweissicherung abzuändern, aufzuheben oder zu bestätigen ist, R. 197.4 VerfO. Bei dieser Beurteilung beschränken sich die zu berücksichtigenden Beweismittel nicht auf solche, die entweder öffentlich oder dem Antragsteller vernünftigerweise bekannt sind. Vielmehr umfasst diese Prüfung alle von den Parteien vorgebrachten Tatsachen und Beweismittel, R. 197.3 (b) VerfO. Die Beurteilung bezieht sich auf die materielle Prüfung der Voraussetzungen für den Erlass (Art. 60 (1) und (3) EPGÜ) sowie den Umfang und die Bedingungen, die in der Anordnung zur Inspektion und Beweissicherung festgelegt sind.

56. Die vorgenannten Beurteilungsschritte sind bezogen auf den Zeitpunkt des Erlasses der zu überprüfenden Anordnung vorzunehmen.

57. Die Prüfung erstreckt sich somit nicht auf die Vollziehung der Anordnung zur Inspektion und Beweissicherung, das Ergebnis dieser Vollziehung oder etwaige während der Vollziehung erhobene Informationen (Beweismittel).

58. Die Anordnung einer Beweissicherung und Inspektion setzt voraus, dass eine Patentverletzung plausibel erscheint; überhöhte Beweisanforderungen sind nicht zu stellen. Nach der Rechtsprechung des Berufungsgerichts darf der Beweismaßstab im Besichtigungs- und Inspektionsverfahren nicht zu hoch angesetzt werden (UPC_CoA_239/2025, Anordnung vom 28. Mai 2025, Rn. 9 ff. – Centripetal v. Palo Alto). Ausreichend ist die glaubhafte Darlegung einer möglichen Patentverletzung (UPC_CFI_834/2025 (LK Düsseldorf), Anordnung vom 4. September 2025, S. 15 – Ecovacs Robotics v. Roborock). Das Erfordernis des Art. 60 Abs. 1 EPGÜ, „vernünftigerweise verfügbare Beweise" vorzulegen, stellt daher eine geringere Anforderung dar als die Beweislast im Verletzungsverfahren, insbesondere für solche Merkmale, zu denen für den Antragsteller kein Zugang zu Beweismitteln besteht (UPC CoA, a.a.O., Rn. 12).

2. Anwendung auf den vorliegenden Fall

a) Zur hinreichenden Verletzungswahrscheinlichkeit

59. Die Antragstellerin hat eine hinreichende Verletzungswahrscheinlichkeit dargelegt (Art. 60 (1) EPGÜ.

60. Auch wenn im Beweissicherungsverfahren, wie bereits ausgeführt, keine überhöhten Anforderungen an die Darlegung einer Verletzungswahrscheinlichkeit zu stellen sind, reicht die bloße Spekulation, das Patent könnte verletzt sein, nicht aus, um eine Beweissicherungsanordnung zu erlassen. Um einen reinen Ausforschungsbeweis (sog. „fishing expedition“) auszuschließen, der keine Grundlage in Art. 60 EPGÜ findet, setzt die Anordnung einer Beweissicherung daher voraus, dass es plausibel erscheint, dass das Patent verletzt wird. Dies gilt insbesondere dann, wenn die Beweissicherungsanordnung, wie im vorliegenden Fall, ohne Anhörung der Antragsgegnerseite erlassen wurde (UPC_CoA_239/2025, Anordnung v. 26. Mai 2025, Rn. 12 – Centripetal v. Palo Alto).

61. Ausgehend von diesen Grundsätzen hat die Antragstellerin in ihrem Antrag auf Beweissicherung und Inspektion eine hinreichende Verletzungswahrscheinlichkeit dargelegt. Das Ergebnis des im Rahmen des vorliegenden Verfahrens eingeholten Sachverständigengutachtens ist an dieser Stelle vor dem Hintergrund der gebotenen Ex-ante-Betrachtung unbeachtlich.

62. Das Vorbringen der Antragstellerin hat sich nicht auf den Hinweis beschränkt, ihr Patent werde möglicherweise verletzt. Vielmehr hat sie zugleich ein Privatgutachten von Prof. Eidenberger vorgelegt, aus welchem sie, in Kombination mit den regulatorischen Rahmenbedingungen, nachvollziehbar und damit plausibel dargelegt hat, weshalb sie auch von einer (möglichen) Verletzung der den Kern der Auseinandersetzung bildenden Merkmale 6.4.b. und 6.6. von Patentanspruch 1 des Antragspatents ausgeht. Ob, wovon Prof. Eidenberger in seinem Gutachten ausgegangen ist, die regulatorischen Rahmenbedingungen den technischen Spielraum tatsächlich derart einschränken, dass nur die patentgemäße Lösung in Betracht kommt, bedarf an dieser Stelle keiner abschließenden Bewertung. Jedenfalls lassen die gutachterlichen Ausführungen von Prof. Eidenberger in Verbindung mit den regulatorischen Bestimmungen jedenfalls den Schluss zu, dass eine Verwirklichung der durch das Antragspatent unter Schutz gestellten technischen Lehre ernsthaft in Betracht kommt. Für die plausible Darlegung einer Verletzungswahrscheinlichkeit ist dies ausreichend.

63. Hinzu kommt, dass sich die Parteien bereits im Vorfeld des Antrages auf Anordnung einer Inspektion und Beweissicherung längere Zeit in Lizenzverhandlungen befanden. Den innerhalb dieser Verhandlungen geäußerten Vorschlag der Antragstellerin, die in Rede stehende Ausführungsform durch eine neutrale Stelle begutachten zu lassen, haben die Antragsgegnerinnen unstreitig abgelehnt. Dies hat auf Seiten der Antragstellerin naturgemäß und zu Recht den Verdacht genährt, dass die Antragsgegnerinnen von der technischen Lehre des Streitpatents Gebrauch machen.

64. Darüber hinaus haben die Antragsgegnerinnen bereits im Vorfeld des Besichtigungsverfahrens eine Schutzschrift eingereicht. Dass in dieser Schutzschrift keine Nichtverletzungsargumentation enthalten war, hat bei der gebotenen Ex-ante-Betrachtung das Vorliegen einer hinreichenden Verletzungswahrscheinlichkeit erhärtet.

65. Entgegen der Auffassung der Antragsgegnerinnen ist eine hinreichende Verletzungswahrscheinlichkeit nicht bereits deshalb zu verneinen, weil, was vorliegend keiner abschließenden Bewertung bedarf, möglicherweise patentfreie Alternativlösungen existieren.

66. Wie bereits im Einzelnen dargelegt hat die Antragstellerin mittels eines Privatgutachtens unter Berücksichtigung der regulatorischen Rahmenbedingungen, des vorgerichtlichen Verhaltens der Antragsgegnerinnen sowie der durch diese eingereichten Schutzschrift die Möglichkeit einer Verletzung des Streitpatents durch die zu untersuchende Ausführungsform plausibel dargelegt. Existieren mögliche Alternativlösungen, ist es gerade eine, wenn nicht die wesentliche Aufgabe des Beweissicherungsverfahrens, ausgehend von dem auf konkrete Anknüpfungstatsachen begründeten Verdacht einer möglichen Patentverletzung weiter aufzuklären und Beweise dafür zu sichern, ob und gegebenenfalls in welchem Umfang die zu untersuchende Ausführungsform von der durch das Antragspatent geschützten technischen Lehre, und eben nicht von einer möglichen Alternativlösung, Gebrauch macht.

67. Der Anordnung von Beweissicherungsmaßnahmen stehen mögliche Alternativlösungen erst dann entgegen, wenn sie dazu führen, dass sie den Vortrag des Antragstellers zu einer möglichen Verletzung des Antragspatents nicht mehr plausibel erscheinen lassen. Das ist vorliegend jedoch nicht der Fall.

b) Ausschöpfung aller sonstigen außergerichtlichen Beweismöglichkeiten

68. Dass die Antragstellerin vor Antragstellung nicht alle ihr sonst zur Verfügung stehenden, zumutbaren, erfolgversprechenden und mit einer niedrigeren Eingriffsintensität verbundenen Erkenntnisquellen ausgeschöpft hätte, vermag die Kammer nicht festzustellen.

69. Es kann dahinstehen, ob das lediglich pauschal gehaltene Vorbringen der Antragstellerin ausreicht, um den ernsthaften Versuch eines Testkaufs hinreichend darzulegen. Selbst wenn ein solcher Testkauf möglich gewesen wäre, ist nicht erkennbar, dass ein solcher die Antragstellerin in die Lage versetzt hätte, die Funktionsweise der streitgegenständlichen Ausführungsform und insbesondere die den Kern des Beweissicherungsverfahrens bildende Verwirklichung der Merkmale 6.4.b und 6.6 hinreichend aufzuklären. Die Antragstellerin hat dies mit der Begründung in Abrede gestellt, es erscheine schon ausgeschlossen, dass Nutzer der Software überhaupt technisch Zugang zu dem Software-Code hätten und diesen dekompilieren könnten. Bei der zu untersuchenden Ausführungsform handele es sich um ein verteiltes System, bei dem sich die für die Merkmale 6.4.b und 6.6 besonders relevante Signaturvorrichtung nicht im Kassensystem, sondern in einer gesonderten Umgebung in der Cloud befinde. Dem haben die Antragsgegnerinnen nichts entgegenzusetzen vermocht. Sie haben insbesondere nicht dargelegt, ob und ggf. wie allein ein Testkauf die Antragstellerin in die Lage versetzt hätte, die streitgegenständliche Ausführungsform so zu analysieren, dass ihrem Aufklärungs- und Beweissicherungsinteresse hinreichend Rechnung getragen wird (anders: UPC_CFI_834/2024, (LK Düsseldorf), Anordnung vom 4. September 2025 – Ecovacs Robotics v. Roborock).

70. Ergänzend zu den fehlenden Erkenntnismöglichkeiten aus einem Testkauf hat die Antragstellerin nachvollziehbar dargelegt, dass auch die durch sie vorgenommenen umfassenden Recherchen in öffentlich zugänglichen Quellen nicht geeignet waren, Restzweifel im Hinblick auf eine mögliche Verwirklichung der Merkmale 6.4.b und 6.6. zu beseitigen.

c) Ex-parte-Anordnung

71. Der Erlass der Anordnung ex-parte war gerechtfertigt.

72. Gemäß R. 197.1 VerfO kann das Gericht Maßnahmen zur Beweissicherung ohne vorherige Anhörung des Antragsgegners insbesondere dann anordnen, wenn dem Antragsteller durch eine Verzögerung wahrscheinlich ein nicht wiedergutzumachender Schaden entstünde oder wenn nachweislich die Gefahr besteht, dass Beweismittel vernichtet werden oder aus anderen Gründen nicht mehr verfügbar sein könnten.

73. Jedenfalls die Voraussetzungen der zweiten Variante sind vorliegend erfüllt.

74. Selbst wenn, was zu Gunsten der Antragsgegnerinnen unterstellt werden kann, eine nachträgliche Manipulation oder Abänderung des zertifizierten Quellcodes nicht möglich und

eine Veränderung der Software aufgrund der spezifischen Hash-Werte grundsätzlich feststellbar ist, hätte dies die Antragsgegnerinnen nicht daran gehindert, den Zugriff auf Dokumente, Log-Files und Quellcodes bei entsprechender Vorwarnung durch eine Anhörung zumindest zu erschweren. Mit der bloßen Nachverfolgbarkeit möglicher Manipulationen wäre der Antragstellerin demgegenüber nicht geholfen. Sie würde der Antragstellerin lediglich zu der Erkenntnis verhelfen, sie müsse die Besichtigung gegebenenfalls wiederholen.

75. Dieser Umstand allein rechtfertigt bereits eine Ex-parte-Anordnung. Im vorliegenden Fall kommt jedoch die länderübergreifende Gesellschaftsstruktur der Antragsgegnerinnen hinzu. Selbst wenn die Antragsgegnerinnen, was zu ihren Gunsten unterstellt werden kann, diese bisher weder für eine Beweisvereitelung benutzt haben noch eine entsprechende konkrete Absicht dafür hatten, verstärkt diese Struktur aus der maßgeblichen Ex-ante-Sicht der Antragstellerin die Gefahr, dass bestimmte Beweismittel bei einer vorherigen Anhörung der Antragsgegnerinnen ihrem Zugriff entzogen werden oder zumindest ein solcher Zugriff erschwert wird.

76. Durch eine Ex-parte-Anordnung wurden die Antragsgegnerinnen auch nicht unangemessen in ihren Rechten beeinträchtigt.

77. Zwar haben die Antragsgegnerinnen zu Recht darauf hingewiesen, dass eine Besichtigung in ihren Geschäftsräumen mit einer hohen Eingriffsintensität verbunden ist. Dass die Besichtigung darüber hinausgehend auch zu einer konkreten Beeinträchtigung des Geschäftsbetriebes der Antragsgegnerinnen geführt hat, ist demgegenüber weder vorgetragen noch ersichtlich. Dem Geheimhaltungsinteresse der Antragsgegnerinnen haben demgegenüber insbesondere die in der Anordnung vom 27. April 2026 in den Ziff. 5, 7, 8 und 13 enthaltenen umfangreichen Schutzmaßnahmen Rechnung getragen.

d) Zeitliche Dringlichkeit

78. R.194.2 (a) VerfO besagt, dass das Gericht bei der Ausübung seines Ermessens zu berücksichtigen hat, wie dringlich *die Klage* ist. Ein Kriterium der zeitlichen Dringlichkeit der Beweissicherung und/oder Inspektion, wie es sich bei den Regelungen über die Anordnung vorläufiger Maßnahmen findet, sehen weder das EPGÜ noch die VerfO bei der Beurteilung vor, ob einem Antrag auf Beweissicherung und/oder Inspektion stattgegeben werden soll (UPC_CoA_2/2025, Anordnung v. 15. Juli 2025, Rn. 35 – Valinea v. Tiru).

79. Dies vorausgeschickt sind die Dringlichkeit der Klage und damit die Notwendigkeit der Anordnung einer Inspektion und Beweissicherung vorliegend gegeben. Der Umstand, dass sich die Antragsgegnerinnen außergerichtlich im Zuge der geführten Lizenzverhandlungen geweigert haben, die von ihnen gewählte Lösung zur Herstellung der Lückenlosigkeit der Transaktionsdatensätze offenzulegen, indiziert bereits die Dringlichkeit der Klage.

e) Verhältnismäßigkeit

80. Die Besichtigungs- und Beweissicherungsanordnung ist auch verhältnismäßig.

81. Soweit die Antragsgegnerinnen die Verhältnismäßigkeit unter Verweis auf die Möglichkeit der Anordnung einer Vorlage des Source-Codes in Frage stellen wollen, handelt es sich bei

einer solchen Anordnung bereits um kein gleichwertiges Mittel.

82. Zum einen wäre eine solche Vorlageanordnung bereits mit dem Risiko verbunden gewesen, dass sich die Antragsgegnerinnen auf Art. 59 (1) (2) EPGÜ berufen. Danach darf die Beweisvorlage nicht zu einer Pflicht zur (strafrechtlichen) Selbstbelastung führen. Hätte sich die Antragstellerin auf einen Antrag auf Anordnung einer solchen Vorlage beschränkt, hätte daher das Risiko bestanden, dass die Antragsgegnerinnen auf dieser Grundlage selbst die Beweismittel selektiert und die für die Patentverletzung entscheidenden Informationen zurückgehalten hätten. Hinzu kommt, dass die bloße Dokumentenvorlage es dem Sachverständigen auch nicht ermöglicht hätte, die Betriebsumgebung und die Systemarchitektur der zu untersuchenden Ausführungsform im laufenden Betrieb zu betrachten, was aus Sicht der Kammer notwendig war, um beurteilen zu können, ob die Antragsgegnerinnen den patentgemäßen Mechanismus zur Herstellung der Lückenlosigkeit der Transaktionsdatensätze verwenden.

83. Dass der Antrag auf Beweissicherung und Inspektion trotz laufender Lizenzverhandlungen gestellt wurde, ist nicht relevant, da die Parteien keine Vereinbarung getroffen haben, die rechtliche Schritte während laufender Lizenzverhandlungen ausschließt.

3. Hilfsantrag

84. Da keine Einwände seitens der Antragstellerin gegen den hilfsweisen Antrag der Antragsgegnerinnen erhoben wurden, die Anordnung der Lokalkammer Düsseldorf vom 27. April 2026 um eine Herausgabeanordnung gegenüber dem Sachverständigen zu ergänzen, konnte eine solche Anordnung wie aus dem Tenor ersichtlich ergehen.

III. Freigabe und Schutz vertraulicher Informationen

85. Geheimhaltungsinteressen können unabhängig von einem Prüfungsantrag nach R. 197.3 VerfO geltend gemacht werden und bedürfen einer eigenständigen Beurteilung (vgl. UPC_CoA_177/2024, Anordnung vom 23. Juli 2024, Rn. 12 – Progress Maschinen & Automation v. AWM). Es wird daher im Anschluss an das Prüfungsverfahren gesondert über den Umfang der Freigabe der ausführlichen Beschreibung unter Berücksichtigung der von den Antragsgegnerinnen geltend gemachten Geheimhaltungsinteressen zu entscheiden sein.

ANORDNUNG:

I. Auf den Hilfsantrag der Antragsgegnerinnen hin wird die Anordnung der Lokalkammer Düsseldorf vom 27. April 2026 dahingehend ergänzt, dass dem Sachverständigen zusätzlich aufgegeben wird, im Fall der Erhebung einer Hauptsacheklage gegen die Antragsgegnerin zu 1. und/oder die Antragsgegnerin zu 2. die Produkte, Dokumente, Unterlagen und/oder Medien und nach beendeter Erstellung der ausführlichen Beschreibung zur Kanzlei der Lokalkammer Düsseldorf zu verbringen.

II. Im Übrigen wird der Prüfungsantrag der Antragsgegnerinnen zurückgewiesen.

Erlassen am 7. September 2026
NAMEN UND UNTERSCHRIFTEN

Vorsitzender Richter Thomas	Digitally signed Thomas Ronny 2026-09-03 13:55:57 +0200 Unified Patent Court Einheitliches Patentgericht Juridiction unifiée du brevet
Rechtlich qualifizierter Richter Adocker	Thomas Adocker Digital unterschrieben von Thomas Adocker Datum: 2026.09.03 15:07:56 +02'00'
Rechtlich qualifizierte Richterin Dr. Schumacher	Digitally signed Schumacher Jule Kathrin 2026-09-03 14:11:47 +0200 Unified Patent Court Einheitliches Patentgericht Juridiction unifiée du brevet
Für den Hilfskanzler	LAURA CHANTAL DANIEL Digital unterschrieben von LAURA CHANTAL DANIEL Datum: 2026.09.03 15:30:17 +02'00'

INFORMATIONEN ÜBER DIE BERUFUNG

Die Parteien können gegen diese Anordnung innerhalb von 15 Tagen nach ihrer Zustellung Berufung einlegen (Art. 73(2)(a), 60 EPGÜ, R. 220.1(c), 224.1(b) VerfO).