# Anordnung

**des Gerichts erster Instanz des Einheitlichen Patentgerichts**
**erlassen am 27. April 2026**
**betreffend EP 4 285 308 B8**

ANTRAGSTELLERIN:

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

| | |
|---|---|
| vertreten durch: | Sebastian Dworschak, Nordemann Czychowski & Partner Rechtsanwältinnen und Rechtsanwälte mbB, Kurfürstendamm 178, 10707 Berlin, Deutschland |
| elektronische Zustelladresse: | sebastian.dworschak@nordemann.de |
| mitwirkender 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

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: Art. 60 EPGÜ, R. 194 (d), 196, 197, 199 VerfO – Antrag auf Inspektion und Beweissicherung

ZUSAMMENFASSUNG DES SACHVERHALTS UND DES VORBRINGENS DER ANTRAGSTELLERIN:

1. Am 20. April 2026 hat die Antragstellerin einen Antrag auf Anordnung einer Inspektion und Beweissicherung an den deutschen Standorten der Antragsgegnerinnen gestellt. Eine Hauptsacheklage wurde bislang nicht erhoben, doch hat die Antragstellerin angegeben, zu beabsichtigen, eine solche nach der beantragten Besichtigung bei der Lokalkammer Düsseldorf zu erheben.

2. Die Antragstellerin ist Inhaberin des Europäischen Patents EP 4 285 308 B8 (die korrigierte Patentschrift B8 entspricht inhaltlich der Fassung des EP 4 285 308 B1, 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.

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

4. 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 die 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)."

5. 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)."

6. Die Antragstellerin führt in ihrem Antrag aus, die Antragsgegnerinnen seien Teil der Swissbit Unternehmensgruppe. Die Antragsgegnerin zu 1 mit Sitz in Bronschhofen, Schweiz, sei im Jahr 2001 gegründet worden und sei ein Technologieunternehmen, das auf Lösungen für Datenspeicherung und den Schutz von Daten und digitalen Identitäten spezialisiert ist. Sie entwickle und produziere u.a. Hardware-Sicherheitslösungen wie Produkte mit Technischen Sicherheitseinrichtungen (TSEs) für den Einsatz in Kassensystemen (Anlagen NM AST 6 und NM AST 7). Sie habe begonnen, auch cloudbasierte TSE-Lösungen zu entwickeln und zu vertreiben. Unter der Bezeichnung „Swissbit Cloud-TSE 2" (nachfolgend: angegriffene Ausführungsform) vertreibe sie ihre cloudbasierte, zertifizierte technische Sicherheitseinrichtung für die manipulationssichere Aufzeichnung von Kassendaten. Diese

biete sie in verschiedenen „Abonnement“-Modellen an (Anlage NM AST 8).

7. Die Antragstellerin führt in ihrem Antrag ferner aus, die Antragsgegnerin zu 2 mit Sitz in Berlin sei die deutsche Landesgesellschaft der Swissbit Unternehmensgruppe (Anlage NM AST 9). Gegenstand ihres Unternehmens sei unter anderem die Entwicklung, der Vertrieb und, nach Vorliegen von erforderlichen Genehmigungen, die Produktion von elektronischen Komponenten und Systemen wie der angegriffenen Ausführungsform. Sie ermögliche mit ihren technischen Systemen den Betrieb der angegriffenen Ausführungsform in Deutschland (Anlage NM AST 10).

8. Die Antragstellerin habe im Jahr 2025 Kenntnis davon erlangt, dass die Antragsgegnerin zu 1 seit dem 1. April 2025 ihr Produkt „Swissbit Cloud-TSE 2“ in Deutschland anbiete. Sie hätte sich daraufhin mit einer Berechtigungsanfrage vom 12. September 2025 (Anlage NM AST 11) an die Antragsgegnerin zu 1 gewandt.

9. Zur weiteren Klärung des Sachverhalts habe die Antragstellerin eine Überprüfung durch eine neutrale Stelle vorgeschlagen, die im Rahmen der Zertifizierung bereits sowohl mit der Antragstellerin als auch der Antragsgegnerin zu 1 zusammengearbeitet hätte, nämlich die SRC Security Research & Consulting („SRC“). Eine vorschlagsgemäße unabhängige Klärung durch die SRC habe die Antragsgegnerin zu 1 jedoch abgelehnt. Eine unabhängige Überprüfung habe nicht stattgefunden.

10. In der Folge sei es zu Einigungsgesprächen zwischen den Parteien gekommen. Die Antragsgegnerin zu 1 habe eine Patentverletzung in Abrede gestellt, jedoch Verhandlungen aufgenommen, deren Gegenstand die Lizenzierung des Antragspatents für die Nutzung in Softwareprodukten und insbesondere Cloud-Diensten der Antragsgegnerin zu 1 gewesen sei. Diese Gespräche seien bisher ergebnislos geblieben.

11. Laut Antragstellerin würden die Antragsgegnerinnen mit hoher Wahrscheinlichkeit das Antragspatent verletzen, indem sie die angegriffene Ausführungsform betreiben und anbieten.

12. Laut Antragstellerin handle es sich bei der angegriffenen Ausführungsform um eine softwarebasierte Technische Sicherheitseinrichtung (TSE) für den Bereich elektronischer Kassensysteme. Sie diene der korrekten und manipulationssicheren Aufzeichnung von steuerrelevanten Daten im Rahmen von elektronischen Bezahlvorgängen (sog. „Fiskalisierung von Online-Kassensystemen“). Die Nutzung von zertifizierten Sicherheitslösungen sei seit 2020 gesetzlich verpflichtend und deren Technologie und Ausgestaltung streng geregelt.

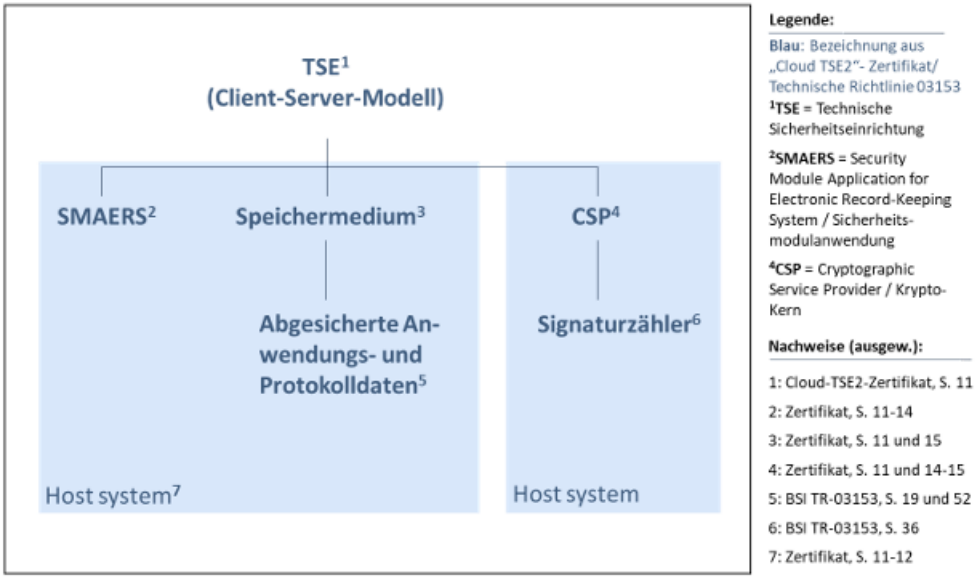
13. Die Technische Sicherheitseinrichtung TSE sei für ein Kassensystem vorgesehen, wie es z.B. im Einzelhandel verwendet werde. Kaufe ein Kunde ein Produkt und zahle, werde über das Kassensystem des Verkäufers eine Transaktion erstellt, deren Schritte auf Grundlage der TSE mit einer Transaktionsnummer versehen, in der Reihenfolge protokolliert, signiert und dauerhaft abgespeichert würden. Über eine Schnittstelle könnten insbesondere Steuerbehörden die signierten Belegdaten erhalten und nachprüfen, ob das betroffene Unternehmen seine steuerrelevanten Transaktionen richtig und vollständig aufgezeichnet habe. Die Technische Sicherheitseinrichtung TSE fungiere damit als sicherer Hafen zwischen dem steuerpflichtigen Verkäufer und den Steuerbehörden und stelle die Integrität der im Kassensystem aufgezeichneten steuerrelevanten Daten sicher.

14. Die angegriffene Ausführungsform teile die TSE dazu konkret in zwei Systemumgebungen auf, nämlich in

    - eine erste Umgebung mit der Sicherheitsanwendung, die sog. „SMAERS“-Einheit („SMAERS“ für „Security Module Application for Electronic Record-keeping Systems“), und mit einem Speichermedium und

    - in eine zweite Umgebung, die die sog. „CSP“-Einheit („CSP“ für „Cryptographic Service Provider“) mit einem Signaturzähler enthalte.

15. Die TSE der Antragstellerinnen stelle sich schematisch wie folgt dar:




16. Die TSE der Antragsgegnerinnen verfüge über drei (vorliegend relevante) Komponenten, nämlich die SMAERS-Einheit, das Speichermedium und die CSP-Einheit. Die SMAERS-Einheit liege zusammen mit dem Speichermedium in einem gemeinsamen Host-System bzw. Docker-Container.

17. Die SMAERS-Einheit diene dazu, alle steuerrelevanten Daten eines Kassenvorgangs aufzubereiten. Die Daten würden von der SMAERS-Einheit erfasst, für die Signierung durch die CSP-Einheit vorbereitet und dann an die CSP-Einheit übersandt.

18. Die CSP-Einheit diene dazu, die von der SMAERS-Einheit übermittelten Daten kryptographisch, d.h. verschlüsselt und mittels digitaler Signatur, zu signieren. Sie liege in einer von der SMAERS-Einheit und dem Speichermedium getrennten Cloud-Umgebung, um eine unabhängige Signierung der einzelnen Transaktionen sicherzustellen. Die Signatur schütze so Transaktionen und Rechnungen vor nachträglichen Manipulationen. Im Kontext von Cloud-Lösungen werde die CSP auch regelmäßig als „CSP-L“ („L“ steht für „Light“) bezeichnet.

19. Im Anschluss würden die signierten, abgesicherten Daten zurück an das Host-System bzw. den Docker-Container der SMAERS-Einheit übersandt und dort auf dem Speichermedium abgespeichert. Das Speichermedium ermögliche die dauerhafte Sicherung der Transaktionsdaten.

20. Der Einsatz von TSEs in elektronischen Kassensystemen sei gesetzlich vorgeschrieben und geregelt. Wegen ihrer steuerrechtlichen Bedeutung müssten TSE-Softwarelösungen wie die angegriffene Ausführungsform von einer zertifizierten Prüfstelle überprüft und vom (deutschen) Bundesamt für Sicherheit in der Informationstechnik (im Folgenden „BSI“) zertifiziert werden, bevor sie vertrieben werden dürfen. Die entsprechenden regulatorischen Anforderungen ergäben sich vor allem aus § 146a Abgabenordnung (AO), der Kassensicherungsverordnung und den darauf aufbauenden Technischen Richtlinien und Schutzprofilen des BSI. Die angegriffene Ausführungsform müsse daher sicherstellen, dass sämtliche Geschäftsvorfälle in elektronischen Systemen – wie etwa Bezahlvorgänge von Kunden – „einzeln, vollständig, richtig, zeitgerecht und geordnet“ aufgezeichnet werden (§ 146a Abs. 1 AO).

21. Die angegriffene Ausführungsform habe die für den Vertrieb notwendigen Zertifikate – auf Grundlage der Technischen Richtlinien und der Schutzprofile – vom BSI erhalten.

22. Dazu zähle insbesondere die Zertifizierung auf Grundlage der zentralen Technischen Richtlinie BSI TR-03153, Version 1.1.1, die im Rahmen des Zertifizierungsprozesses von TSE-Softwarelösungen von der Prüfstelle bzw. dem BSI geprüft werde. Sie enthalte verbindliche technische Vorgaben für den Aufbau, die Funktionsweise und die Sicherheitsanforderungen von TSEs wie der angegriffenen Ausführungsform.

23. Mit Ausstellung des Zertifikats für die Cloud-TSE-2-Software der Antragsgegnerin zu 1 hätten die Prüfstelle und das BSI bestätigt, dass die angegriffene Ausführungsform mit sämtlichen zwingenden Vorgaben aus der Richtlinie BSI TR-03153 konform sei. Das Erfüllen dieser Richtlinien-Vorgaben und die Feststellungen in dem Zertifizierungsdokument ließen daher eindeutige Rückschlüsse auf die Systemarchitektur der angegriffenen Ausführungsform und somit auf die Wahrscheinlichkeit einer Verletzung des Antragspatents zu.

24. Aus der Zertifizierung der angegriffenen Ausführungsform durch das BSI ergebe sich eindeutig die Verwirklichung der Merkmale 6.1-6.4a und 6.5 des Antragspatents gemäß Merkmalsgliederung Anlage NM AST 13, dies sind die nachfolgenden Merkmale:

    6.1 Ein verteiltes System (1) zur sicheren Registrierung einer Folge von Transaktionen

    6.2 wobei das verteilte System (1) eine Registrierungsvorrichtung (6) und eine Signaturvorrichtung (8) aufweist

    6.3 wobei die Registrierungsvorrichtung (6) einen Transaktionsspeicher (16) zum Speichern von signierten Transaktionsdatensätzen (15) aufweist, die von der Signaturvorrichtung (8) signiert wurden

    6.4a wobei die Signaturvorrichtung (8) einen Schlüsselnutzungszähler [aufweist]

    6.5 wobei jeder signierte Transaktionsdatensatz (15) einen zugehörigen Wert des Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist

25. Im Hinblick auf die Verwirklichung der Merkmale 6.4b und 6.6a sowie 6.6b des Antragspatents gemäß Merkmalsgliederung Anlage NM AST 13, nämlich

    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

bestünden zwar Restzweifel, jedoch würden die Feststellungen des (von ihr beauftragten) Gutachters [redacted] (Anlage NM AST 20) ergeben, dass auch eine Verwirklichung dieser Merkmale hoch wahrscheinlich sei. Schließlich deute auch das außergerichtliche Verhalten der Antragsgegnerin zu 1 auf die Verletzung hin, die zwar den Vorwurf der Patentverletzung pauschal zurückweise, gleichwohl aber über eine Lizenzierung des Antragspatents verhandle, und eine unabhängige Begutachtung durch eine neutrale Stelle ablehne.

26. Zusammenfassend würden zwar naturgemäß nur beschränkte Erkenntnismöglichkeiten über die konkrete Ausgestaltung der angegriffenen Ausführungsform vorliegen. Allerdings erscheine es vor dem Hintergrund der regulatorischen Rahmenbedingungen und der technischen Alternativen hoch wahrscheinlich, dass die angegriffene Ausführungsform einen patentgemäßen Lückenfüll-Mechanismus implementiere, soweit sie die rechtlichen Rahmenbedingungen erfüllt.

27. Davon ausgehend sei Anspruch 6 des Antragspatents durch die angegriffene Ausführungsform hoch wahrscheinlich verwirklicht. Aus denselben Gründen gelte dies auch für die nebengeordneten Ansprüche 1, 10 und 12. Anspruch 1 schütze spiegelbildlich ein Verfahren zur Umsetzung des verteilten Systems gemäß Anspruch 6. Anspruch 10 stelle ein Computerprogramm für die Umsetzung der Registrierungsvorrichtung unter Schutz. Anspruch 12 schütze schließlich das die Signaturvorrichtung umsetzende Computerprogramm. Ebenso erscheine eine Verwirklichung der Unteransprüche 7 – 9 wahrscheinlich, da diese weitere Details der konkreten Umsetzung des Lückenfüllmechanismus betreffen, zu deren tatsächlichen Verletzung allerdings erst eine Begutachtung auf Basis der zu sichernden Beweismittel Aufschluss geben könne.

28. Die Antragsgegnerinnen würden das Antragspatent benutzen, indem sie die angegriffene Ausführungsform arbeitsteilig betreiben und vermarkten. Während die Antragsgegnerin zu 1 die angegriffene Ausführungsform in Deutschland anbiete, ermögliche und fördere die Antragsgegnerin zu 2 dies in erheblichem Maße, indem sie jedenfalls Teile der Systeme innerhalb Deutschlands betreibe.

29. Die Antragsgegnerin zu 1 biete die angegriffene Ausführungsform in Deutschland an. Bereits in ihrer Pressemitteilung anlässlich der Zertifizierung der angegriffenen Ausführungsform im April 2025 führe die Antragsgegnerin zu 1 aus, dass die „Swissbit Cloud-TSE 2“ über ihre Vertriebspartner „ab sofort […] erhältlich“ sei (Anlage NM AST 8).

30. Bestätigt werde der bereits begonnene Vertrieb durch den Internetauftritt der Antragsgegnerin zu 1. Dort präsentiere die Antragsgegnerin zu 1 die „Swissbit Cloud-TSE 2“ mit ihren technischen Eigenschaften und Einsatzgebieten und verweise auf ein „flexibles Abonnement-Modell“ für die Nutzung der angegriffenen Ausführungsform (Anlage NM AST

21).

31. Die angegriffene Ausführungsform sei auch bei einer Vertriebspartnerin der Antragsgegnerin zu 1, der Jarltech Europe GmbH (im Folgenden „Jarltech“), direkt abonnierbar. Die Angebote reichten dabei von einem Nutzungszeitraum von 3 bis 5 Jahren. Die Antragsgegnerin zu 1 sei in dieses Angebot gleich mehrfach eingebunden. So werde in den jeweiligen Angeboten auf der Internetseite von Jarltech auf die AGB der Antragsgegnerin zu 1 verwiesen (Anlage NM AST 22). Am Ende der Angebotsseite von Jarltech finde sich außerdem eine Swissbit-Produktbroschüre zur angegriffenen Ausführungsform, die ausweislich des Copyright-Vermerks von der Antragsgegnerin zu 1 stamme. In dieser Broschüre bewerbe die Antragsgegnerin zu 1 die „Swissbit Cloud-TSE 2“ umfassend und führe selbst aus, dass sie die Software-Lösung „anbietet“ (Anlage NM AST 23, dort S. 2 unten).

32. Überdies sei die Antragsgegnerin zu 1 auch Inhaberin des maßgeblichen BSI-Zertifikats (Anlage NM AST 14), so dass insgesamt von einem Anbieten der angegriffenen Ausführungsform durch die Antragsgegnerin zu 1 auszugehen sei.

33. Die Antragsgegnerin zu 2 fungiere als deutsche Landesgesellschaft und ermögliche und fördere den Vertrieb der angegriffenen Ausführungsform, indem sie die erforderlichen Systeme in Deutschland mitentwickle und betreibe.

34. Zahlreiche Indizien ließen darauf schließen, dass die Infrastruktur der angegriffenen Ausführungsform in Deutschland betrieben werde. So werde die angegriffene Ausführungsform in einem You Tube-Video des Swissbit-YouTube-Kanals, das die angegriffene Ausführungsform präsentiere, als „Entwickelt, zertifiziert und betrieben in Deutschland“ beschrieben (Anlage NM AST 24).

35. Ebenso werde die angegriffene Ausführungsform in der Produktbroschüre der Antragsgegnerin zu 1, die dem Angebot bei Jarltech beigefügt sei, mit den Eigenschaften „Made in Germany“ und „in Deutschland gehostet“ beworben (Anlage NM AST 23).

36. Dafür, dass für den Betrieb der angegriffenen Ausführungsform in Deutschland nur die Antragsgegnerin zu 2 in Betracht komme, spreche, dass nur sie eindeutig zuzuordnende Standorte in Deutschland für einen solchen Betrieb besitze, dies ihrem Geschäftszweck entspreche und sich dies aus einem entsprechenden TÜV-Zertifikat der Antragsgegnerin zu 2 ergebe.

37. Aus dem Handelsregister ergebe sich, dass allein der Antragsgegnerin zu 2 – und nicht der Antragsgegnerin zu 1 – deutsche Standorte eindeutig zuzuordnen seien (Anlage NM AST 9).

38. Spezifisch gehe ferner der Betrieb von zumindest Teilsystemen der angegriffenen Ausführungsform durch die Antragsgegnerin zu 2 aus einer deutschen TÜV-Zertifizierung hervor. Dieses Zertifikat gelte ausdrücklich für den „Betrieb eines Cryptographic Service Provider Light“ (CSP-L) (Anlage NM AST 25).

39. Es sei davon auszugehen, dass diese CSP-Ls für den Betrieb der angegriffenen Ausführungsform verwendet werden. Schon die Richtlinie BSI TR-03153 beschreibe CSP-Ls als Komponente nur von cloudbasierten TSEs (S. 38 der Richtlinie, Anlage NM AST 17).

40. Die CSP-Ls seien darüber hinaus im Produktportfolio der Swissbit Unternehmensgruppe, soweit ersichtlich, nur für die angegriffene Ausführungsform relevant, sodass sich von dem

zertifizierten Betrieb der CSP-Ls durch die Antragsgegnerin zu 2 eine direkte Verbindung zur Nutzung der angegriffenen Ausführungsform ergebe (Anlagen NM AST 18 und 19).

41. Die beiden Antragsgegnerinnen würden im Hinblick auf die Vermarktung, den Vertrieb und den Betrieb der angegriffenen Ausführungsform arbeitsteilig vorgehen. Während die Antragsgegnerin zu 1 vorrangig die Vermarktung und den Vertrieb der angegriffenen Ausführungsform übernehme, stelle die Antragsgegnerin zu 2 die technische Infrastruktur für zumindest Teile des Betriebs der angegriffenen Ausführungsform bereit. Die insoweit ineinandergreifende und verzahnte Zusammenarbeit der Antragsgegnerinnen ohne klare Trennung zwischen den Antragsgegnerinnen zeige sich an gleich mehreren Indizien.

42. So werde auf der „Swissbit"-Unternehmenswebseite einerseits die Antragsgegnerin zu 1 im Impressum als Herausgeberin an erster Stelle genannt. Direkt im Anschluss werde dort andererseits aber auch die Antragsgegnerin zu 2 unter dem Hinweis „Information zur Landesgesellschaft in Deutschland" aufgeführt (Anlage NM AST 26).

43. Die Verbindung der Antragsgegnerinnen werde außerdem an den deutschen Standorten deutlich. So existiere neben Berlin offenbar ein weiterer deutscher Standort am Leuchtenbergring 3 in 81677 München. Dieser Standort sei in das TÜV-Zertifikat für die CSP-Ls ebenfalls aufgenommen (Anlage NM AST 25) und werde auch auf der „Swissbit"-Webseite der Antragsgegnerin zu 2 zugeordnet (Anlage NM AST 27).

44. Jedoch werde im Eintrag auf der BSI-Webseite der oben genannte Münchener Standort wiederum der Antragsgegnerin zu 1 zugewiesen (Anlage NM AST 28), sodass offenbar keine strikte Abgrenzung des Geschäftsbetriebs vorliege, sondern vielmehr von einem gemeinschaftlichen Handeln und Produktangebot der verbundenen Gesellschaften auszugehen sei.

45. Auch am Berliner Standort zeige sich das Zusammenwirken der Antragsgegnerinnen. Am Eingangstor des Berliner Standorts der Antragsgegnerinnen sei nur die Bezeichnung „Swissbit" ohne Differenzierung nach Antragsgegnerin zu 1 oder 2 angebracht und auch auf dem Klingelschild/Briefkasten ergebe sich keine Differenzierung:


(Foto Anlage NM AST 29)

46. Im Übrigen sei die – neben dem Klingelschild angebrachte – Swissbit-Marke für die Antragsgegnerin zu 1 (und nicht etwa für die Antragsgegnerin zu 2) registriert, sodass auch hier eine entsprechende Vermischung vorliege.

47. Für die enge, arbeitsteilige Verbindung spreche auch, dass die Pressemitteilung zur Cloud-TSE 2 vom 28. Mai 2024 auf der Swissbit-Webseite ausweislich der dortigen Ortsangabe aus Berlin stamme (Anlage NM AST 14).

48. Das Wirken der Antragsgegnerinnen stelle sich als eng verflochtene, arbeitsteilige Zusammenarbeit dar, bei der beide Gesellschaften jeweils eigenständige und unverzichtbare Beiträge in der Vertriebs- und Betriebskette der „Swissbit Cloud-TSE 2“ erbringen würden.

49. Die beantragte Besichtigung sei erforderlich, da die Antragstellerin die Patentverletzung ohne eine Besichtigung mangels Alternativen nicht vollständig nachweisen könne. Alle bisherigen Ermittlungsmaßnahmen hätten die seitens der Antragstellerin nicht zweifelsfrei nachweisbaren Merkmale 6.4b und 6.6 nicht aufklären können. Dies liege auch an der Natur der angegriffenen Ausführungsform, bei der die besichtigungsrelevanten Abläufe innerhalb der Software und – jedenfalls zu Teilen – in einer speziellen, gesicherten Infrastruktur bei den Antragsgegnerinnen ablaufen würden.

50. Es sei auch nicht damit zu rechnen, dass ein testweiser Erwerb der angegriffenen Ausführungsform zur Aufklärung beitragen könnte. Denn der Erwerb ermögliche zwar die Nutzung der angegriffenen Ausführungsform, jedoch sei es kaum denkbar, daraus Rückschlüsse auf die konkrete Ausgestaltung des Lückenfüllmechanismus ziehen zu können. Abgesehen davon, ob man die Software in einem erworbenen Produkt überhaupt technisch erfolgreich dekompilieren könnte und dürfte, sei nicht damit zu rechnen, dass die hier maßgeblichen Softwarebestandteile überhaupt bereitgestellt würden. Es sei vielmehr damit zu rechnen, dass diese auf den Servern der Antragsgegnerinnen ablaufen, was insbesondere deshalb gelte, weil die noch festzustellenden Merkmale 6.4b und 6.6 sich auf den Krypto-Kern (CSP) beziehen würden, der jedenfalls bei den Antragsgegnerinnen ablaufen werde. Aus Erwerbersicht stelle sich die Nutzung der angegriffenen Ausführungsform daher als „Blackbox“ dar, d.h. als ein Produkt, das zwar bestimmungsgemäß genutzt, dessen interne Funktionsweise jedoch – insbesondere die Implementierung des Lückenfüll-Mechanismus – von außen weder beobachtet noch nachvollzogen werden könne.

51. Gleichwohl habe sich die Antragstellerin um den Erwerb einer angegriffenen Ausführungsform über einen Distributor bemüht, um jedenfalls weitere Anhaltspunkte, z.B. aus der mitgelieferten Dokumentation, zu erlangen. Allerdings sei selbst dieser Versuch gescheitert und die Antragstellerin habe bisher keinerlei Zugriffsmöglichkeit, um die angegriffene Ausführungsform zu analysieren.

52. Auch Recherchen in öffentlich zugänglichen Quellen, wie z.B. Fachpublikationen, Produktdokumentationen oder sonstigen Internetveröffentlichungen, zu der angegriffenen Ausführungsform hätten keine weitere Aufklärung für die Merkmale 6.4b und 6.6 herbeiführen können.

53. Der Antragstellerin stünden damit keine Möglichkeiten zur Verfügung, um weitere Nachweise für eine Patentverletzung zu erlangen. Die notwendigen beweismäßigen Feststellungen könnten laut Vorbringen der Antragstellerin jedoch von einem Sachverständigen bei Zugang zu den Räumlichkeiten der Antragsgegnerinnen in Berlin und München unschwer getroffen werden. Der Sachverständige könne so die entsprechenden Vorrichtungen und Unterlagen in Augenschein nehmen und seine Erkenntnisse dokumentieren.

54. Die Antragstellerin argumentiert, dass die Anordnung auch ohne vorherige Anhörung der Antragsgegnerinnen zu erlassen sei. Es bestehe die Gefahr, dass relevante Unterlagen und Daten beiseitegeschafft oder jedenfalls deren Auffindbarkeit deutlich erschwert werden. Dies gelte insbesondere vor dem Hintergrund, dass die Antragsgegnerinnen als eng verbundene Schwesterunternehmen neben den deutschen Standorten in Berlin und München über einen Schweizer Standort in Bronschhofen (gemäß Handelsregisterauszug Anlage NM AST 6) – als Sitz der Antragsgegnerin zu 1 – verfügten, an den Unterlagen und Daten verlagert bzw. durch den die Unterlagen/Zugriffe aus Berlin unterdrückt werden könnten.

55. Eine Vollziehung der Besichtigung in der Schweiz wäre – wenn überhaupt – nur mit erheblich höherem Aufwand, Kosten und Rechtsunsicherheit bei gegebenenfalls verschlechterter Beweislage möglich, da die Schweiz weder EPG-Mitgliedstaat noch EU-Mitglied ist.

56. Am 14. November 2025 haben die Antragsgegnerinnen eine Schutzschrift gegen die Antragstellerin sowie die fiskaly Germany GmbH (PL_58/2025) beim Einheitlichen Patentgericht für den Fall eingereicht, dass die Antragstellerin die Anordnung einstweiliger Maßnahmen beantragt. Für diesen Fall beantragen die Antragsgegnerinnen, einen solchen Antrag vollumfänglich zurückzuweisen. Hilfsweise beantragen die Antragsgegnerinnen, vor der Anordnung einstweiliger Maßnahmen gehört zu werden, den Spruchkörper um einen technisch qualifizierten Richter zu ergänzen und die Vollstreckung einer solchen Anordnung von der Anordnung einer Sicherheitsleistung abhängig zu machen. Zur Begründung haben die Antragsgegnerinnen in ihrer Schutzschrift ausgeführt, die Antragstellerin bzw. die fiskaly Germany GmbH hätten bisher keine Tatsachen präsentiert, welche die Grundlage für einen Verletzungsvorwurf in Bezug auf die angegriffene Ausführungsform bilden könnten. Darüber hinaus hätten die Antragsgegnerinnen den Rechtsbestand des Streitpatents summarisch geprüft. Bereits auf der Grundlage dieser Prüfung erweise sich das Streitpatent als nicht rechtsbeständig. Überdies habe es die Antragstellerin versäumt, rechtzeitig einstweilige Maßnahmen zu beantragen. Schließlich sei die Anordnung einstweiliger Maßnahmen auch unverhältnismäßig.

ANTRÄGE DER ANTRAGSTELLERIN:

57. Die Antragstellerin beantragt,

I. folgende Anordnung ohne vorherige Anhörung der Antragsgegnerinnen zu erlassen:

1. Die Beweissicherung und Inspektion im Hinblick auf die 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).

durch

a) Inspektion der deutschen Standorte der Antragsgegnerinnen

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

b) Sicherung und Offenlegung digitaler Beweise bezüglich des Produkts Swissbit Cloud TSE 2, umfassend insbesondere

- 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;

- Quellcodes sowie Softwaredokumentation einschließlich Ablaufdiagramme;

- Betriebs- und Installationshandbücher sowie Entwicklungsdokumentation ein schließlich Lasten- und Pflichtenhefte;

- 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;

c) Beschlagnahme von Kopien oder, hilfsweise, Sicherung durch Anfertigen 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;

d) Erstellung und Vorlage eines schriftlichen Berichts an das Gericht (Sachverständigenbericht) über die Ergebnisse der Maßnahmen gemäß Ziffer 1. a) bis c) 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 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,

innerhalb einer Frist von einem Monat nach Durchführung der

Maßnahmen gemäß Ziffer 1. a) bis c).

2. als gerichtlichen Sachverständigen für die Durchführung der Maßnahmen gemäß Ziffer 1. zu bestellen:

   Patentanwalt Lars Grannemann, Cohausz & Florack, Bleichstr. 14, 40211 Düsseldorf, hilfsweise einen anderen Patentanwalt der Kanzlei Cohausz & Florack, Bleichstr. 14, 40211 Düsseldorf;

   zur Unterstützung des Sachverständigen kann der Sachverständige nach eigenem Ermessen den IT-Forensiker [redacted] FAST-DETECT GmbH, Inselkammerstr. 12, 82008 Unterhaching, hilfsweise einen anderen IT-Fachmann der FAST-DETECT GmbH als Hilfsperson zur Unterstützung hinzuziehen.

3. Neben dem gerichtlichen Sachverständigen und seiner Hilfsperson gemäß Ziffer 2. dürfen folgende UPC-Vertreter der Antragstellerin bei der Durchführung der Maßnahmen gemäß Ziffer 1. a) bis c) anwesend sein:

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

   Diese UPC-Vertreter sind verpflichtet, gegenüber der Antragstellerin und ihren Mitarbeitern alle Tatsachen, die ihnen bei der Durchführung der gesamten Anordnung in Bezug auf die Geschäftstätigkeit der Antragsgegnerinnen zur Kenntnis gelangen, geheim zu halten. Vertretungsorgane, Angestellte oder sonstige Mitarbeiter der Antragstellerin dürfen bei der Durchführung der unter Ziffer 1. genannten Maßnahmen nicht anwesend sein.

4. den Antragsgegnerinnen aufzugeben,

   a) dem gerichtlichen Sachverständigen, seiner Hilfsperson und den unter Ziffer 3. aufgeführten UPC-Vertretern der Antragstellerin den Zutritt zu den unter Ziffer 1. a) genannten Räumlichkeiten zu gestatten;

   b) dem gerichtlichen Sachverständigen und seiner Hilfsperson 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; dem gerichtlichen Sachverständigen sowie seiner Hilfsperson ist gestattet, 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;

   c) 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; dem gerichtlichen Sachverständigen sowie seiner Hilfsperson ist gestattet, Kopien der digitalen Beweise anzufertigen.

d) dem gerichtlichen Sachverständigen 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 zu gestatten, Kopien dieser Unterlagen anzufertigen.

e) dem Sachverständigen den genauen Aufbewahrungsort der unter Ziffer 1 b) und c) 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.

5. Der gerichtliche Sachverständige und seine Hilfsperson sind verpflichtet, gegenüber Dritten Verschwiegenheit zu wahren. Die Antragsgegnerinnen werden aufgefordert, nach Vorlage des Sachverständigenberichts zu etwaigen Geheimhaltungsinteressen Stellung zu nehmen. Den unter Ziffer 3. genannten UPC-Vertretern der Antragstellerin wird Gelegenheit gegeben, zur Stellungnahme der Antragsgegnerinnen Stellung zu nehmen. Danach entscheidet das Gericht, ob und inwieweit der Sachverständigenbericht und die gesicherten Beweise der Antragstellerin persönlich zur Kenntnis gebracht werden sollen und ob die Verschwiegenheitspflicht für die unter Ziffer 3. genannten UPC-Vertreter der Antragstellerin aufzuheben ist.

6. Die Antragstellerin ist verpflichtet, die Kosten der Inspektion und Beweissicherung ein schließlich der Fertigung der ausführlichen Beschreibung zu tragen. Der Antragstellerin wird aufgegeben, vor Beginn der Inspektion dem Sachverständigen einen angemessenen, von diesem zu bestimmenden Kostenvorschuss zu zahlen, soweit dieser nicht auf einen solchen Kostenvorschuss verzichtet.

7. Die Anordnung ist den Antragsgegnerinnen persönlich in den unter Ziffer 1. a) genannten Räumlichkeiten durch einen der unter Ziffer 3. 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. Sollte eine Zustellung an die Antragsgegnerin zu I in den unter Ziffer 1. a) genannten Räumlichkeiten nicht möglich sein, ist die Anordnung gemäß der [sic!] allgemeinen Regeln zuzustellen.

8. Hilfsweise, sofern das Gericht die Leistung einer Sicherheit für die Verfahrenskosten und sonstigen Auslagen sowie für etwaige Schäden, für die die Antragstellerin gegenüber den Antragsgegnerinnen haftbar sein könnte, für erforderlich hält, die Antragstellerin zu verpflichten, eine Sicherheit in Höhe von 10.000,00 EUR oder, höchst hilfsweise, in einer vom Gericht für angemessen erachteten anderen Höhe zu leisten.

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

10. 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 der nach Ziffer 1. d) zu fertigende Sachverständigenbericht der Antragstellerin offengelegt wurde oder das Gericht durch eine endgültige Entscheidung entschieden hat, keinen Zugang zu diesem Sachverständigenbericht zu gewähren, eine Klage gegen die Antragsgegnerinnen erhoben hat.

II. Hilfsweise – für den Fall, dass das Gericht Maßnahmen ohne vorherige Anhörung der Antragsgegnerinnen für nicht angemessen erachten sollte – wird beantragt, den Antragsgegnerinnen eine Erwiderungsfrist von nicht mehr als 10 Arbeitstagen einzuräumen und die unter Ziffer I. 1. beantragten Maßnahmen anschließend im beschleunigten Verfahren durchzuführen.

*GRÜNDE DER ANORDNUNG:*

58. Der zulässige Antrag auf Anordnung einer Inspektion und Beweissicherung (R. 192, 199 VerfO) hat im tenorierten Umfang Erfolg.

I.

59. Die Lokalkammer Düsseldorf ist gemäß Art. 32 (1) c), 33 (1) b), 60 EPGÜ zuständig. Der Antrag ist gemäß R. 192 VerfO in zulässiger Art und Weise gestellt worden. Insbesondere hat die Antragstellerin auch vorgetragen, dass sie beabsichtigt, gegen die Antragsgegnerinnen bei der Lokalkammer Düsseldorf Hauptsacheklage zu erheben.

II.

60. Ferner hat die Antragstellerin glaubhaft dargelegt, dass das Antragspatent durch die Antragsgegnerinnen wahrscheinlich verletzt wird (Art. 60 (1) EPGÜ), wobei sie für eine abschließende Bewertung auf die Inspektion und Beweissicherung angewiesen ist. Angesichts der geschilderten Umstände des Falles ist es möglich, dass das Produkt „Swissbit Cloud-TSE 2“ von der technischen Lehre des Antragspatents Gebrauch macht.

61. Die als Inhaberin des Antragspatents aktivlegitimierte Antragstellerin hat nachvollziehbar erläutert, dass mit Ausstellung des Zertifikats für die Cloud-TSE-2-Software der Antragsgegnerin zu 1 die Prüfstelle und das BSI bestätigt haben, dass die angegriffene Ausführungsform mit sämtlichen zwingenden Vorgaben aus der Richtlinie BSI TR-03153 konform ist. Das Gericht schließt sich der Schlussfolgerung der Antragstellerin an, dass das Erfüllen dieser Richtlinien-Vorgaben und die Feststellungen in dem Zertifizierungsdokument eindeutige Rückschlüsse auf die Systemarchitektur der angegriffenen Ausführungsform und somit auf die Wahrscheinlichkeit einer Verletzung des Antragspatents zulassen.

62. Des Weiteren hat die Antragstellerin nachvollziehbar erläutert, dass sich aus der Zertifizierung der angegriffenen Ausführungsform durch das BSI die Verwirklichung der Merkmale 6.1-6.4a und 6.5 des Antragspatents gemäß Merkmalsgliederung Anlage NM AST 13 ergibt, dies sind die nachfolgenden Merkmale:

    6.1 Ein verteiltes System (1) zur sicheren Registrierung einer Folge von Transaktionen

    6.2 wobei das verteilte System (1) eine Registrierungsvorrichtung (6) und eine Signaturvorrichtung (8) aufweist

    6.3 wobei die Registrierungsvorrichtung (6) einen Transaktionsspeicher (16) zum Speichern von signierten Transaktionsdatensätzen (15) aufweist, die von der Signaturvorrichtung (8) signiert wurden

    6.4a wobei die Signaturvorrichtung (8) einen Schlüsselnutzungszähler [aufweist]

    6.5 wobei jeder signierte Transaktionsdatensatz (15) einen zugehörigen Wert des Schlüsselnutzungszählers zum Zeitpunkt der Signatur aufweist

63. Im Hinblick auf die Verwirklichung der Merkmale 6.4b und 6.6a sowie 6.6b des Antragspatents gemäß Merkmalsgliederung Anlage NM AST 13, nämlich

    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

    hält es das Gericht im Hinblick auf das Gutachten von [redacted] (Anlage NM AST 20) für nachvollziehbar, dass eine Verwirklichung dieser Merkmale wahrscheinlich ist, jedoch nur nachgewiesen werden kann, wenn eine Beweissicherung und Inspektion wie beantragt vorgenommen wird. Dies ergibt sich insbesondere aus der Natur der angegriffenen Ausführungsform, bei der die besichtigungsrelevanten Abläufe innerhalb der Software und – jedenfalls zu Teilen – in einer speziellen, gesicherten Infrastruktur bei den Antragsgegnerinnen ablaufen.

64. Ferner hält es das Gericht zumindest insoweit, als es für die Anordnung der beantragten Beweissicherung und Inspektion erforderlich ist, für wahrscheinlich, dass auch die

Unteransprüche 7 bis 9 sowie die nebengeordneten unabhängigen Ansprüche 1, 10 und 12 verletzt sind. Auch diesbezüglich geht das Gericht davon aus, dass ein Nachweis nur möglich ist, wenn eine Beweissicherung und Inspektion wie beantragt vorgenommen wird, da wie erwähnt die besichtigungsrelevanten Abläufe innerhalb der Software und – jedenfalls zu Teilen – in einer speziellen, gesicherten Infrastruktur bei den Antragsgegnerinnen ablaufen.

65. Die Stellung des Antrags gegen beide Antragsgegnerinnen begegnet vor dem Hintergrund des arbeitsteiligen Vorgehens der Antragsgegnerinnen bei der Vermarktung, dem Vertrieb und dem Betrieb der angegriffenen Ausführungsform keinen Bedenken. Während die Antragsgegnerin zu 1 vorrangig Vermarktung und Vertrieb der angegriffenen Ausführungsform übernimmt, stellt die Antragsgegnerin zu 2 die technische Infrastruktur für zumindest Teile des Betriebs der angegriffenen Ausführungsform bereit. Es liegt eine ineinandergreifende und verzahnte Zusammenarbeit der Antragsgegnerinnen ohne klare Trennung zwischen diesen vor. Es ist daher die Passivlegitimation hinsichtlich beider Antragsgegnerinnen gegeben und der Antrag hinsichtlich beider Antragsgegnerinnen berechtigt.

66. Soweit die Antragsgegnerinnen in ihrer sich in erster Linie gegen die Anordnung einstweiliger Maßnahmen richtenden Schutzschrift eine Verletzung des Antragspatents in Frage stellen, steht dies dem Erlass der beantragten Inspektions- und Beweissicherungsanordnung nicht entgegen. Die Antragsgegnerinnen stellen eine Verletzung des Antragspatents in ihrer Schutzschrift lediglich mit der Begründung in Frage, weder die Antragstellerin noch die fiskaly Germany GmbH hätten bisher konkrete Erläuterungen präsentiert, welche die Grundlage des erhobenen Verletzungsvorwurfs durch die angegriffene Ausführungsform bilden könnten. Im Gegenteil verlangten die Antragstellerin sowie die fiskaly Germany GmbH, dass die Antragsgegnerinnen Fragen zu technischen Details der angegriffenen Ausführungsform beantworteten. Dementsprechend fehle es bisher an einer stichhaltigen und fundierten Darlegung von Antragstellerseite, aus welchen Gründen diese der Auffassung sei, die angegriffene Ausführungsform falle in den Schutzbereich des Streitpatents. Gerade diese Wissenslücken auf Antragstellerseite soll jedoch das vorliegende, auf eine Inspektion und Beweissicherung gerichtete Verfahren schließen. Die Ausführungen in der Schutzschrift untermauern daher allenfalls das Beweissicherungsinteresse der Antragstellerin. Sie stellen keinen Grund dar, allein aufgrund des Vorliegens der Schutzschrift von einer ex-parte-Anordnung abzusehen.

67. Eine nähere Prüfung der Rechtsbeständigkeit des Antragspatents ist im Rahmen des vorliegenden Verfahrens nicht vorzunehmen. Etwas anderes kann nur dann gelten, wenn es klare Anhaltspunkte dafür gibt, den Rechtsbestand des Antragspatents in Zweifel zu ziehen, etwa in Folge einer negativen Rechtsbestandsentscheidung (vgl. UPC_CoA_327/2025, Anordnung vom 15. Juli 2025, Rn. 43 – Maguin v. Tiru). Solche Anhaltspunkte liegen jedoch nicht vor. Soweit sich die Antragsgegnerinnen in ihrer Schutzschrift vom 14. November 2025 darauf berufen, es seien derzeit weder ein Einspruch gegen die Erteilung des Antragspatents noch ein Nichtigkeitsverfahren anhängig, handelt es sich allenfalls um ein Indiz für die Rechtsbeständigkeit des Antragspatents, nicht jedoch dagegen.

68. Abgesehen davon unterscheidet sich der Zweck eines Antrags auf Inspektion und Beweissicherung von demjenigen einer Hauptsacheklage (vgl. UPC_CoA_239/2025, Anordnung vom 28. Mai 2025, Rn. 11 – Centripetal v. Palo Alto Networks). Zweck der Maßnahmen ist es, Beweismittel zu erlangen, die in einem Hauptsacheverfahren verwendet werden können (vgl. R. 196.2, 199.2 VerfO), wozu auch die Verwendung der Beweismittel

zur Entscheidung darüber gehört, ob ein Verfahren in der Hauptsache oder ein Verfahren auf Anordnung einstweiliger Maßnahmen überhaupt eingeleitet werden soll (vgl. UPC_CoA_177/2024, Anordnung vom 23. Juli 2024, Leitsatz 1 – Progress Maschinen & Automation v. AWM; UPC_CFI_407/2025 (LK Brüssel), Anordnung vom 12. November 2025, Leitsatz 4 – Organon Heist v. Genentech). Auf eine abschließende Klärung zwischen den Parteien streitiger Fragen ist das Verfahren auf Beweissicherung und Inspektion hingegen nicht gerichtet (siehe auch UPC_CFI_1325/2025 (LK Düsseldorf), Anordnung vom 23. Januar 2026, Rn. 17 – Van Loon Beheer v. Inverquark).

69. Im Lichte dessen sind die Ausführungen in der Schutzschrift zum Rechtsbestand des Antragspatents, in welcher mangelnde erfinderische Tätigkeit und mangelnde Offenbarung des Antragspatents argumentiert wird, allenfalls kursorisch zu prüfen. Die dortigen Ausführungen lassen nach Ansicht des Gerichts nach kursorischer Prüfung den Rechtsbestand jedenfalls nicht so zweifelhaft erscheinen, dass sie gegen die Erlassung der begehrten Anordnung auf Inspektion und Beweissicherung sprechen.

III.

70. Die Antragstellerin hat ferner dargelegt, dass der Antrag dringlich ist (R. 194.2 a) VerfO). Zudem hat sie Gründe für den Erlass einer Anordnung ex parte aufgezeigt (R. 194. 2 b), c), 197 VerfO).

1.

71. Die Inspektion bzw. Beweissicherungsmaßnahme ist dringlich.

72. Dass die angegriffene Ausführungsform möglicherweise von der technischen Lehre der Patentansprüche 6 und der auf diesen rückbezogenen Unteransprüche 7 - 9 sowie daneben der unabhängigen Ansprüche 1, 10 und 12 Gebrauch macht, hat die Antragstellerin nachvollziehbar dargelegt. Jedoch kann eine hinreichende Substantiierung nur über eine Untersuchung der in den Räumen der Antragsgegnerinnen befindlichen Unterlagen und Quellcodes erfolgen. Es ist der Antragstellerin nach ihrem Vortrag nicht möglich, anders als durch eine Inspektion Zugang zu den für eine Substantiierung des Verletzungsvorwurfs erforderlichen Unterlagen zu erhalten. Die Antragstellerin hat nicht nur nachvollziehbar dargelegt, weshalb nicht damit zu rechnen ist, dass ein testweiser Erwerb der angegriffenen Ausführungsform zur Aufklärung beitragen könnte, da ein solcher Erwerb zwar die Nutzung der angegriffenen Ausführungsform ermögliche, aber keine Rückschlüsse auf die konkrete Ausgestaltung des Lückenfüllmechanismus zulasse. Vielmehr hat sich die Antragstellerin sogar gleichwohl um den Erwerb einer angegriffenen Ausführungsform über einen Distributor bemüht, um jedenfalls weitere Anhaltspunkte, zum Beispiel aus der Dokumentation zu erlangen. Allerdings ist ein solcher Versuch gescheitert, weshalb die Antragstellerin außerhalb einer Inspektion keinerlei Zugriffsmöglichkeit hat, um die angegriffene Ausführungsform zu analysieren. Insbesondere hat die Antragstellerin nachvollziehbar erläutert, dass Recherchen in öffentlich zugänglichen Quellen, wie etwa Fachpublikationen, Produktdokumentationen oder sonstigen Internetveröffentlichungen, zu der angegriffenen Ausführungsform keine weitere Aufklärung in Bezug auf die Verwirklichung der Merkmale 6.4.b. und 6.6. hätten herbeiführen können. Eine Inspektion in den Räumen der Antragsgegnerinnen bietet der Antragstellerin daher Gelegenheit, über die auf dieser Grundlage zu fertigende ausführliche Beschreibung eines Sachverständigen weitere Erkenntnisse über die Ausgestaltung der angegriffenen Ausführungsform zu

erlangen und Beweismittel zu sammeln.

73. Auch wenn die Antragstellerin ausweislich ihres eigenen Vortrages bereits im Jahr 2025 Kenntnis davon erlangt hat, dass die Antragsgegnerin zu 1 die angegriffene Ausführungsform in Deutschland anbietet, und daraufhin schon im September 2025 eine Berechtigungsanfrage versandt hat, woraufhin die Parteien in einen Austausch über eine mögliche Verletzung des Streitpatents im Hinblick auf eine mögliche Verletzung des Streitpatents durch die angegriffene Ausführungsform getreten sind, steht dies der begehrten Anordnung einer Beweissicherung und Inspektion nicht entgegen. Wie bereits das Berufungsgericht bestätigt hat, ist zwischen der Beurteilung der Dringlichkeit im Zusammenhang mit einem Antrag auf Beweissicherung (R. 194.2(a) VerfO) und der Beurteilung der Dringlichkeit im Zusammenhang mit einem Antrag auf einstweilige Maßnahmen (R. 209.2(b) VerfO) zu unterscheiden. Bei der Ausübung seines Ermessens, ob einstweilige Maßnahmen anzuordnen sind, hat das Gericht auch eine unangemessene Verzögerung bei der Beantragung einstweiliger Maßnahmen zu berücksichtigen (R. 211.4 VerfO). Eine solche Anforderung wird weder durch das EPGÜ noch durch die Verfahrensordnung gestellt, wenn zu beurteilen ist, ob ein Antrag auf Beweissicherung zu gewähren ist (UPC_CoA_2/2025, Anordnung vom 15. Juli 2025, Leitsatz 3 – Valinea v. Tiru). Das Fehlen einer zeitlichen Dringlichkeit könnte daher allenfalls dann problematisch sein, wenn das Zuwarten zu einem Wegfall des Beweissicherungsinteresses geführt hätte. Dafür fehlt es vorliegend jedoch an Anhaltspunkten.

2.

74. Die Antragstellerin hat in zureichender und nachvollziehbarer Weise Gründe für den Erlass einer Anordnung ex-parte aufgezeigt (R. 194.2 b), c), 197 VerfO). Andernfalls bestünde die nachweisliche Gefahr, dass Beweismittel vernichtet oder aus anderen Gründen nicht mehr verfügbar sein werden (R. 197.1 Alt. 2 VerfO).

75. Es ist nachvollziehbar und entspricht der Lebenserfahrung, dass bei vorheriger Verständigung der Antragsgegnerinnen die Gefahr bestünde, dass relevante Unterlagen und Daten beiseitegeschafft oder jedenfalls deren Auffindbarkeit deutlich erschwert werden. Dies gilt insbesondere vor dem Hintergrund, dass die Antragsgegnerinnen als eng verbundene Schwesterunternehmen neben den deutschen Standorten in Berlin und München über einen Schweizer Standort in Bronschhofen (gemäß Handelsregisterauszug Anlage NM AST 6) – als Sitz der Antragsgegnerin zu 1 – verfügen, an den Unterlagen und Daten verlagert bzw. durch den die Unterlagen/Zugriffe aus Deutschland unterdrückt werden könnten.

IV.

76. Im Rahmen der Ermessensentscheidung überwiegen die Interessen der Antragstellerin.

77. Die Antragstellerin hat nachvollziehbar dargelegt, dass das Antragspatent durch die Antragsgegnerinnen wahrscheinlich verletzt wird und dass sie für eine abschließende Bewertung auf die Inspektion und Beweissicherung angewiesen ist. Demgegenüber ist nicht erkennbar, dass eine wesentliche Belastung der Antragsgegnerinnen durch die angeordneten Maßnahmen entsteht. Die Argumentation der Antragstellerin, wonach die beabsichtigte Besichtigung und Inspektion der technischen Systeme minimalinvasiv seien und den Betrieb der Systeme nicht grundsätzlich einschränken wird, erscheint dem Gericht

glaubwürdig und nachvollziehbar. Den Geheimhaltungsinteressen der Antragstellerinnen tragen die in die Anordnung aufgenommenen Geheimnisschutzanordnungen hinreichend Rechnung.

V.

78. Die Antragstellerin hat die Gerichtsgebühr für den Antrag auf Inspektion und Beweissicherung entrichtet, R. 192.5 VerfO.

VI.

79. Entsprechend Ziff. I.1.a des Antrags war die Inspektion und entsprechend Ziff. I.1.b-d des Antrags die Beweissicherung im Hinblick auf die Verletzung des Antragspatents durch die angegriffene Ausführungsform anzuordnen.

80. Die Inspektion und der damit verbundene Zutritt zu den beiden deutschen Standorten der Antragsgegnerinnen gem. Ziff. I.1.a des Antrags dient einerseits dazu, die Betriebsumgebung der angegriffenen Ausführungsform zu besichtigen, einschließlich der Feststellung zu konkret betriebenen Software- und Hardwareversionen, sowie andererseits dem Auffinden der zu sichernden analogen und digitalen Beweismittel. Beide Standorte sind gem. der TÜV-Zertifizierung (Anlage NM AST 25) dazu zertifiziert, CSP-Ls zu betreiben, die genaue interne Aufteilung zwischen den Standorten ist bisher jedoch unbekannt. Es ist daher der Antrag auf Inspektion an beiden Standorten berechtigt.

81. In Ziff. I.1.b des Antrags wird in Einklang mit R. 196.1(d) VerfO die Sicherung und Offenlegung digitaler Beweismittel beantragt, die den Nachweis der Verwirklichung der Merkmale der Ansprüche 6-9, 1, 10 und 12 des Antragspatents ermöglichen. Dies sind insbesondere spezifische Zertifizierungsunterlagen, aber auch der Quellcode und allgemeinere technische Dokumentationen sowie Daten, die Rückschlüsse über den Betrieb der Komponenten zulassen (Konfigurationsdateien, Logs und Betriebsdaten). Die beantragte Offenlegung der digitalen Beweise einschließlich sämtlicher Passwörter und Zugangsdaten basiert darauf, dass die patentverletzungsrelevante Funktionsweise der angegriffenen Ausführungsform praktisch nur auf Basis von internen Unterlagen festgestellt werden kann und sich einer äußerlichen Betrachtung entzieht. Die Behauptung der Antragstellerin, dass ohne Zugang zu diesen Daten die Maßnahme ins Leere liefe, ist glaubhaft. Dies gilt spiegelbildlich für die Beschlagnahme bzw. hilfsweise Sicherung von Kopien der analogen Beweismittel gem. Ziff. I.1.c des Antrags basierend auf R. 196.1(c) VerfO.

82. Mit der Erstellung und Vorlage des schriftlichen Berichts gem. Ziff. I.1.d des Antrags wird von der Antragstellerin in Einklang mit R. 196.1(a) VerfO die Beweissicherung der Erkenntnisse aus der Inspektion und Sichtung weiterer Beweismittel durch den gerichtlichen Sachverständigen beantragt. Der schriftliche Sachverständigenbericht dient der Sicherung der Ergebnisse der Inspektion und notwendigen Feststellungen im Hinblick auf den Besichtigungsgegenstand.

83. Der gem. Ziff. I.2 des Antrags vorgeschlagene Sachverständige ist als Patentanwalt und ausgebildeter Spezialist für Informations- und Kommunikationstechnik – mit technischen Schwerpunkten in den Bereichen Informations- und Kommunikationstechnik, insbesondere Funknetze und Datenverarbeitung, Steuerungs- und Regelungstechnik, Mikrosystemtechnik sowie Software – zur Begutachtung der streitgegenständlichen Frage geeignet. Er hat ein Studium der Elektrotechnik, Informationstechnik und Technischen Informatik absolviert

(Anlage NM AST 34). Es bestehen seitens des Gerichts keine Bedenken, den von der Antragstellerin vorgeschlagenen Sachverständigen zu beauftragen. Das Gericht hält ferner das Vorbringen der Antragstellerin für glaubhaft, wonach keine Umstände bekannt sind, die der Sachverständigenbestellung des vorgeschlagenen Sachverständigen entgegenstehen und insbesondere keine die Bestellung ausschließende Beziehung des vorgeschlagenen Sachverständigen zu den Parteien bekannt ist. Es erscheint dem Gericht ferner sinnvoll, dass sich der von der Antragstellerin vorgeschlagene Sachverständige wie beantragt zur praktischen Durchführung der Maßnahme nach eigenem Ermessen eines IT-Forensikers bedienen kann.

84. Die gem. Ziff. I.3 des Antrags beantragte Anwesenheit von gleich vier benannten UPC-Vertretern der Antragstellerin, wenn auch unter Verschwiegenheitsanordnung, ist unverhältnismäßig. Es ist nicht ersichtlich, warum nicht die Anwesenheit von jeweils einem rechts- und einem patentanwaltlichen UPC-Vertreter (an jedem der beiden Standorte der Inspektion und Beweissicherung) ausreichend sein soll. Der Kreis der Anwesenden war daher wie aus der Anordnung ersichtlich zu beschränken.

85. Die in Ziff. I.4 des Antrags beantragten Pflichten der Antragsgegnerinnen regeln notwendige Einzelheiten für die Durchführung der gem. Ziff. I.1 beantragten Inspektion und Beweissicherung. Es ist für das Gericht nachvollziehbar, dass es erforderlich ist, dass dem Sachverständigen, seiner Hilfsperson und den gem. Ziff. I.3 aufgeführten Vertretern der Zutritt (Ziff. I.4.a) und dem Sachverständigen und seiner Hilfsperson Zugang zur Betriebsumgebung der angegriffenen Ausführungsform (Ziff. I.4.b) gestattet wird. Gleiches gilt für die Inbetriebsetzungspflicht sowie Duldung der Anfertigung von Foto- oder Filmaufnahmen und Notizen.

86. Die gem. Ziff. I.4 c)-e) des Antrags beantragten Pflichten betreffen aus Sicht des Gerichts zur Beweissicherung erforderliche Detailaspekte, wie die Bereitstellung und Offenlegung von digitalen Dokumenten einschließlich der erforderlichen Passwörter, die Aushändigung und Gestattung von Vervielfältigungen von analogen Beweismitteln sowie die Mitteilung über die entsprechenden Aufbewahrungsorte.

87. Die Ziff. I.5 bis I.7 des Antrags der Antragstellerin stoßen auf keine Bedenken. In Ziff. I.5 ist eine übliche Geheimhaltungsanordnung und in Ziff. I.6 eine übliche Kostentragungs- und Vorschussverpflichtung beantragt. Ziff. I.7 sieht in angemessener Weise besichtigungsspezifische Zustellungsmodalitäten vor.

88. Zur Unterstützung des Sachverständigen und dessen Hilfsperson bei der Durchführung der Beweissicherung und Inspektionen hat das Gericht von der durch R. 196.5 S. 2 VerfO eingeräumten Möglichkeit Gebrauch gemacht, die Unterstützung durch Gerichtsvollzieher anzuordnen.

89. Die gegenüber den Verfahrensbevollmächtigten, dem Sachverständigen und dem Gerichtsvollzieher angeordneten Geheimnisschutzmaßnahmen tragen den Geheimhaltungsinteressen der Antragsgegnerinnen Rechnung. Gleiches gilt für das geschilderte Prozedere nach Erhalt des Sachverständigenberichts.

90. Ferner war anzuordnen, dass der durch den Sachverständigen zu erstellende Bericht sowie sämtliche sonstigen Ergebnisse der Maßnahmen zur Beweissicherung nur in einem Hauptsacheverfahren gegen die Antragsgegnerin zu 1 und/oder die Antragsgegnerin zu 2

verwendet werden dürfen (R. 196.2 VerfO).

91. Die Kosten der durch den Sachverständigen durchzuführenden Inspektion und Beweissicherung einschließlich der durch den Sachverständigen zu erstellenden ausführlichen Beschreibung hat die Antragstellerin jedenfalls bis auf Weiteres zu zahlen, da sie die Inspektion und Beweissicherung begehrt. Soweit der Sachverständige nicht auf die Zahlung eines Vorschusses für seine Kosten verzichtet, hat die Antragstellerin an die Sachverständigen vor Beginn der Inspektion einen durch diesen zu bestimmenden, angemessenen Vorschuss zu zahlen.

92. Die Anordnung ist zusammen mit den in der Anordnung genannten Schriftstücken durch den Gerichtsvollzieher im Zusammenwirken mit einem der bei der Inspektion und Beweissicherung anwesenden Vertreter der Antragstellerin gemäß R. 197.2 VerfO zuzustellen.

VII.

93. Die in die Anordnung aufgenommene allgemeine Androhung von Zwangsmitteln gibt dem Gericht die notwendige Flexibilität, um auf eventuelle Verstöße gegen diese Anordnung unter Berücksichtigung der Interessen beider Parteien sowie der Schwere des Verstoßes reagieren zu können.

94. Gemäß R. 196.6 VerfO ordnet das Gericht an, dass der Antragsteller für die Kosten des Rechtsstreits und die sonstigen dem Antragsgegner entstandenen oder entstehenden oder wahrscheinlich entstehenden Kosten, welche der Antragsteller möglicherweise tragen muss, sowie für die möglicherweise von dem Antragsteller zu leistende Entschädigung des dem Antragsgegner entstandenen oder wahrscheinlich entstandenen Schadens im Fall einer Anordnung ohne vorherige Anhörung des Gegners eine angemessene Sicherheit zu leisten hat, sofern keine besonderen Umstände dagegen sprechen. Auch wenn den Antragsgegnerinnen, anders bei einer Unterlassungsanordnung, durch die Inspektion und Beweissicherung allenfalls ein geringfügiger Schaden droht, weil die Antragsgegnerinnen auch weiterhin zur Vornahme sämtlicher Benutzungshandlungen hinsichtlich der angegriffenen Ausführungsform berechtigt sind und es daher gerechtfertigt sein kann, aufgrund der besonderen Dringlichkeit der Inspektion und Beweissicherung von der Anordnung einer Sicherheitsleistung Abstand zu nehmen (vgl. UPC_CFI_260/2025 (LK Düsseldorf), Anordnung v. 26.03.2025, S. 9 f. – OTEC Präzisionsfinish v. STEROS; Abgrenzung zu: UPC_CFI_177/2023 (LK Düsseldorf), Anordnung v. 22.06.2023 – myStromer v. Revolt), handelt es sich bei der Anordnung der Sicherheitsleistung im Fall einer ex-parte-Anordnung um den gesetzlichen Regelfall. Gründe, vorliegend von der Forderung nach einer solchen Sicherheitsleistung Abstand zu nehmen, sind weder vorgetragen noch ersichtlich. Insbesondere ist auf der Grundlage des Vorbringens der Antragstellerin nicht erkennbar, dass die mit der Sicherheitsleistung verbundene geringfügige zeitliche Verzögerung der Besichtigung zu einer Beeinträchtigung oder Gefährdung des Beweissicherungsinteresses der Antragstellerin führt.

95. Soweit die Antragstellerin unter Randziffer 190 ihrer Antragsschrift eine Kostenentscheidung nach R. 211.1 d) VerfO erwähnt, bezieht sich die angesprochene Norm auf die Anordnung einer vorläufigen Kostenerstattung, für die es als Grundvoraussetzung eines entsprechenden, bezifferten Antrages bedürfte, an dem es hier fehlt. Hinzu kommt, dass sich die betreffende Norm auf die Anordnung einstweiliger Maßnahmen im Sinne des Teils 3

(Regeln 205 ff.) der Verfahrensordnung bezieht. Die Regelungen zur Beweissicherung und Inspektion kennen eine solche vorläufige Kostenerstattung nicht. Für eine analoge Anwendung von R. 211.1 d) VerfO dürfte es demgegenüber sowohl an einer planwidrigen Regelungslücke als auch an einer gleichen Interessenlage fehlen, ohne dass dies vorliegend einer abschließenden Entscheidung bedarf.

*ANORDNUNG:*

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).*

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 Einsatz 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

   [redacted] 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 Personen 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.

Erlassen am 27. April 2026

NAMEN UND UNTERSCHRIFTEN

| | |
|---|---|
| Vorsitzender Richter Thomas | Ronny Thomas<br>Digital unterschrieben von Ronny Thomas<br>Datum: 2026.04.27 10:17:59 +02'00' |
| Rechtlich qualifizierter Richter Adocker | Thomas Adocker<br>Digital unterschrieben von Thomas Adocker<br>Datum: 2026.04.27 10:06:19 +02'00' |
| Rechtlich qualifizierte Richterin Dr. Schumacher | Jule Kathrin Schumacher<br>Digital unterschrieben von Jule Kathrin Schumacher<br>Datum: 2026.04.27 10:24:04 +02'00' |
| für den Hilfskanzler | LAURA CHANTAL DANIEL<br>Digital unterschrieben von LAURA CHANTAL DANIEL<br>Datum: 2026.04.27 10:29:37 +02'00' |

*INFORMATIONEN ZUR ÜBERPRÜFUNG UND BERUFUNG:*

Die Antragsgegnerinnen können innerhalb von 30 Tagen nach der Vollziehung der Maßnahmen eine Überprüfung der vorliegenden Anordnung beantragen (Art. 60 (6) EPGÜ, R. 197.3 VerfO).

Die nachteilig betroffene Partei kann gegen die vorliegende Anordnung innerhalb von 15 Tagen nach ihrer Zustellung Berufung einlegen (Art. 73 (2) a) EPGÜ, R. 220.1 c) VerfO).