Unified Patent Court
Einheitliches Patentgericht
Juridiction unifiée du brevet

Düsseldorf local division
UPC_CFI_1332/2026

Order
of the Court of First Instance of the Unified Patent Court
issued on 7 September 2026
concerning EP 4 285 308

HEADNOTES:

1. In order to prevent a mere 'fishing expedition', the order for an inspection and/or the preservation of evidence requires that it appears plausible that the patent in question is being infringed (in line with UPC_CoA_239/2025, order of 26 May 2025, para. 12 – Centripetal v. Palo Alto).

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

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

KEYWORDS:

Inspection and preservation of evidence; examination proceedings; sufficient likelihood of infringement

HEADNOTES:

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

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

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

KEYWORDS:

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

APPLICANT:

fiskaly GmbH, represented by its managing directors Johannes Ferner, Simon Tragatschnig and Patrick Gaubatz, Mariahilfer Straße 36/5, 1070 Vienna, Austria

represented by:	Sebastian Dworschak, Attorney-at-law, Nordemann Czychowski & Partner Attorneys-at-law mbB, Kurfürstendamm 178, 10707 Berlin, Germany
Electronic service address:	sebastian.dworschak@nordemann.de
Patent attorney involved:	Patent Attorney Ralf Emig, Maikowski & Ninnemann Patentan-wälte Partnerschaft mbB, Kurfürstendamm 54–55, 10707 Ber-lin, Germany

RESPONDENTS:

1. **SwissBit AG**, represented by its Chairman of the Board of Directors Bernd Stefan Hofschen, its Board member and member of the Executive Board Benjamin Schüler, and its Board member Thomas Harald Luft, Industriestrasse 4, 9552 Bronschhofen, Switzerland

2. **Swissbit Germany AG,** represented by its board members Lars Lust and Chris Schwarze, Bitterfelder Straße 22, 12681 Berlin, Germany

represented by:	Dr Thomas Lynker, Attorney-at-law, TALIENS Partnerschaft von Rechtsanwälten mbB, Amalienstraße 15 f, 80333 Munich, Germany
Electronic service address:	thomas.lynker@taliens.com
Patent attorney involved:	Patent Attorney Michael Platzöder, Platzöder Patentanwalts-gesellschaft mbH, Inselkammerstraße 10, 82008 Unterhaching, Germany
Email address for service:	m.platzoeder@platzoeder.eu

PATENT APPLICATION:

EUROPEAN PATENT NO. EP 4 285 308 B8

PANEL:

Panel 1 of the Düsseldorf local division

JUDGES INVOLVED:

This order was issued by Presiding Judge Thomas, legally qualified judge Adocker as judge-rapporteur, and legally qualified judge Dr Schumacher.

LANGUAGE OF THE PROCEEDINGS: German

SUBJECT: Rule 197.3 of the RoP – Review of an order for inspection and preservation of evidence

ORAL HEARING: 25 August 2026

BRIEF SUMMARY OF THE FACTS:

1. The applicant is the proprietor of European Patent EP 4 285 308 B8 (Annex NM AST 4; hereinafter 'the patent in question'), which was filed on 28 January 2022 in the language of the proceedings, claiming the priority of European patent application 21154250 dated 29 January 2021. The grant of the patent in question was published on 26 June 2024, and the corrected patent specification B8 was published on 17 July 2024. This is a European patent with unitary effect. Unitary effect took effect on
2. September 2024.

2. No preliminary objection was filed against the grant of the patent in question.

3. The patent in question is entitled 'SECURELY REGISTERING A SEQUENCE OF TRANSACTIONS'. The applicant's application relates primarily to claim 6 and to sub-claims 7–9, which are dependent on it, as well as to independent claims 1, 10 and 12. In the English language of the proceedings, these claims are worded as follows:

> Claim 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 current value of the key usage counter with a previously recorded value, which previously recorded value is the associated value of the most recent signed transaction record in the transaction storage (16), loading at least one previously signed transaction record (23) from a record buffer (24) of the signature device (8) in response to detecting a gap between the current value and the last recorded value, and transmitting the loaded at least one previously signed transaction record (23) to the registration device (6)."
>
> Claim 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) in response to detecting a gap between the current value of the key usage counter and the associated value of the last signed transaction record in the transaction storage (16), and to transmit the loaded at least one previously signed transaction record (23) to the registration device (6).”

Claim 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).”

Claim 8:

“The distributed system of claim 7, **characterised in that** the signature device (8) is configured to refuse to provide a signature for a new unsigned transaction record (10) in response to detecting a discrepancy between the current value and the associated value of the last signed transaction record.”

Claim 9:

“The distributed system of claim 6, **characterised in that** the registration device (6) is configured, 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) in response to detecting a gap between the compared values.”

Claim 10:

“A computer programme 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 device (8) from a record buffer in response to detecting a gap between a current 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).”

Claim 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) in response to detecting a gap between a current value of the key usage counter and the received last recorded value, and transmitting the loaded at least one previously signed transaction record (23) to the registration device (6).”

4. In the registered German translation, the claims read as follows:

Claim 1:
„Verfahren zur sicheren Registrierung einer Folge von Transaktionen mit einem verteilten Sys-tem (1), wobei das verteilte System (1) eine Registrierungsvorrichtung (6) und eine Signatur-vorrichtung (8) aufweist, wobei die Registrierungsvorrichtung (6) einen Transaktionsspeicher (16) zum Speichern von signierten Transaktionsdatensätzen (15) auf weist, die von der Signa-turvorrichtung (8) signiert wurden, wobei die Signaturvorrichtung (8) einen Schlüsselnutzungs-zähler aufweist, der mit jeder von der Signaturvorrichtung (8) erzeugten Signatur inkremen-tiert 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 aufge-zeichneten Wert, wobei der zuletzt aufgezeichnete Wert der zu gehörige Wert eines zuletzt signierten Transaktionsdatensatzes in dem Transaktionsspeicher (16) ist, Laden mindestens ei-nes zuvor signierten Transaktionsdatensatzes (23) aus einem Datensatzpuffer (24) der Signa-turvorrichtung (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).“

Claim 6:

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

Claim 7:

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

Claim 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 aktuel-len Wert und dem zugehörigen Wert des letzten signierten Transaktionsdatensatzes ablehnt."

Claim 9:

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

Claim 10:

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

Claim 12:

„Computerprogramm, das Anweisungen aufweist, um eine Signaturvorrichtung (8), die einen Schlüsselnutzungszähler aufweist, wobei der Schlüsselnutzungszähler mit jeder von der Signa-turvorrichtung (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 Schlüsselnutzungs-zählers zum Zeitpunkt der Signatur aufweist, die folgenden Schritte auszuführen: Empfangen einer Angabe (18) eines zuletzt aufgezeichneten Wertes des Schlüsselnutzungszählers von ei-ner Registrierungsvorrichtung (6), Laden mindestens eines zuvor signierten Transaktionsda-tensatzes (23) aus dem Datensatzpuffer (24) in Reaktion auf das Erfassen einer Lücke zwischen einem aktuellen Wert des Schlüsselnutzungszählers und dem empfangenen zuletzt aufgezeich-neten Wert, und Übertragen des geladenen, mindestens einen zuvor signierten Transaktions-datensatzes (23) an die Registrierungsvorrichtung (6)."

5. On 20 April 2026, the applicant filed an application for an order to carry out an inspection and to secure evidence at the respondents' German premises.

6. The Düsseldorf local division subsequently issued the following order on 27 April 2026:

"The following inspection and preservation of evidence order is issued without prior hearing of the respondents:

1. The applicant is authorised, with regard to the realisation of the features of claims 6–9, 1, 10 and 12 of European Patent EP 4 285 308 by the product Swissbit Cloud-TSE 2, which read:

> *A distributed system (1) for the secure registration of 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 memory (16) for storing signed transaction records (15) which have been 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) includes an associated value of the key usage counter at the time of signing, wherein the signing device (8) is configured to load at least one previously signed transaction record*
> *(23) from the record buffer (24) when a gap is detected between a current value of the key usage counter and the associated value of a most recent signed transaction record in the transaction memory (16), and to transmit the loaded at least one previously signed transaction record*
> *(23) to the registration device (6).*
>
> *(Claim 6)*
>
> *A distributed system (1) according to claim 6, characterised in that the registration device (6) is configured to send an indication (18) of the associated value of a most recently signed transaction record to the signature device (8).*
>
> *(Claim 7)*
>
> *A distributed system according to claim 7, characterised in that the signature device (8) is configured to refuse to provide a signature for a new, unsigned transaction data record (10) in response to the detection of a discrepancy between the current value and the associated value of the last signed transaction data record.*
>
> *(Claim 8)*
>
> *A distributed system according to claim 6, characterised in that the registration device (6) is configured such that, upon receipt of a new signed transaction record (15) from the signature device (8), compares the associated value of the new signed transaction record (15) with the associated value of the last signed transaction record and, in response to detecting a discrepancy between the compared values, requests the re-transmission of at least one previously signed transaction record (23) from the signing device (8).*
>
> *(Claim 9)*

A method for the secure registration of a sequence of transactions using 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 memory (16) for storing signed transaction records (15) that have been signed by the signature device (8), wherein the signing device (8) comprises a key usage counter which is incremented with each signature generated by the signing device (8), wherein each signed transaction record (15) comprises a corresponding value of the key usage counter at the time of signing, the method comprising: comparing a current value of the key usage counter with a most recently recorded value, wherein the most recently recorded value is the associated value of a most recently signed transaction record in the transaction memory (16), loading at least one previously signed transaction record (23) from a record buffer (24) of the signing device (8) in response to detecting a gap between the current value and the most recently recorded value, and transmitting the loaded at least one previously signed transaction record (23) to the registration device (6).

(Claim 1)

A computer programme comprising instructions for causing a registration device (6), which comprises a transaction memory (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 signing, to cause the registration device to perform the following steps: accessing the transaction memory (16) and determining the associated value of the most recent signed transaction record in the transaction memory (16) as the most recently recorded value of the key usage counter, sending an indication (18) of the most recently recorded value to a signature device (8), receiving at least one previously signed transaction record (23) from the signature device (8), wherein the at least one previously signed transaction data record (23) is loaded from the signature device (8) from a data record buffer that responds to the detection of a gap between a current value of the key usage counter and the received most recently recorded value; and storing the received at least one previously signed transaction record (23) in the transaction memory (16).

(Claim 10)

A computer programme comprising

comprises instructions for causing a signature device (8), which comprises a key usage counter—wherein the key usage counter is incremented with each signature generated by the signature device (8)— and a data record buffer (24) for buffering at least one previously signed transaction data record (23), wherein each signed transaction data record (15) comprises a corresponding value of a key usage counter at the time of signing, to perform the following steps: receiving an indication (18) of a most recently recorded value of the key usage counter from a registration device (6), loading at least one previously signed transaction data record (23) from the data record buffer (24) in response to the detection of a gap

between a current value of the key usage counter and the received most recently recorded value, and transmitting the loaded at least one previously signed transaction data record (23) to the registration device (6).

(Claim 12)

a) to have the following documents and records inspected by an expert at the premises of the respondents

- Bitterfelder Straße 22, 12681 Berlin and
- Leuchtenbergring 3, 81677 Munich,

comprising

aa) the certification documents, including the test report for procedure BSI K-TR-0612-2024 and, in particular, the documents mentioned in Chapter 7.3/7.4 of the Conformity Report, including the Secure Platform Concept (version 1.0.2) and the Swissbit Cloud SMAERS – Guidance Documentation (version 1.0.3);

bb) source codes and software documentation, including flowcharts;

cc) Operating and installation manuals, as well as development documentation, including requirements and specifications;

dd) Configuration files, logs and operational data, including documentation on the specific software versions running in the operational environment, including the handover or production of copies and the disclosure of all necessary passwords

and, for this purpose, to enter the respondents' premises located at the aforementioned sites;

b) to secure evidence by

aa) the preparation and submission by an expert of a detailed description of the results of the measures referred to in paragraph 1(a), with regard to the realisation of the features of claims 6 and 7
- 9, 1, 10 and 12 of European Patent EP 4 285 308, including a detailed description of the functioning of the respondents' Swissbit Cloud-TSE 2 and a determination of the specific hardware and software versions in use (hash values), as well as an opinion as to whether the product fulfils the features of claims 6 and 7 – 9, 1, 10 and 12 of the
European Patent EP 4 285 308,

bb) the production of copies or photographs of the aforementioned documents and records relating to the design, configuration, certification and

implementation of the respondents' Swissbit Cloud-TSE 2, at the claimant's expense, insofar as this is necessary for the preparation of the detailed description,

cc) in the event of the respondents' refusal to provide copies in accordance with paragraph 1(b)
bb), the seizure of copies or photographs of technical documentation, internal development documents, manuals and records relating to the design, configuration, certification and use of the respondents' Swissbit Cloud-TSE 2.

2. The expert shall submit the written description to be prepared in accordance with paragraph 1. b) aa) within one month of the inspection carried out in accordance with paragraph I. 1. a).

The detailed description to be prepared by the expert and all other findings from the inspection and preservation of evidence may only be used in proceedings on the merits against the first respondent and/or the second respondent.

3. The following is appointed as the court-appointed expert to carry out the measures in accordance with paragraph
1. is appointed:

Patent Attorney Lars Grannemann, Cohausz & Florack, Bleichstr. 14, 40211 Düsseldorf, or, in the alternative, another patent attorney from the firm Cohausz & Florack, Bleichstr. 14, 40211 Düsseldorf.

To assist the expert, the expert may, at his or her own discretion, call upon the IT forensic expert

Dipl. Inf. Fabian Unucka, FAST-DETECT GmbH, Inselkammerstr. 12, 82008 Unterhaching, or, in the alternative, another IT specialist from FAST-DETECT GmbH

as an assistant to provide support.

4. To assist the expert and his assistants, the bailiffs with local jurisdiction over the inspection sites specified in paragraph 1.a) of the order are designated as further assistants.

5. In addition to the court-appointed expert and his assistants as set out in paragraph 3, at each of the inspection sites specified in paragraph 1.a), one legal representative and one patent attorney representing the applicant's UPC representatives listed below may be present during the implementation of the measures set out in paragraph 1.a):

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

Representatives, employees or other staff of the applicant may not be present whilst the measures referred to in paragraph 1 are being carried out.

6. The respondents are ordered to

   a) to grant the court-appointed expert, his assistants and the applicant's UPC representatives listed under paragraph 5. access to the premises referred to in paragraph 1.
   a);

   b) to grant the court-appointed expert and his assistants access to the operating environment of the Swissbit Cloud-TSE 2 and, in particular, to enable them to ascertain which specific software and hardware versions of the TSE components are actually in operation, as well as to put an instance of the Swissbit Cloud-TSE 2 components into operation at the expert's request;

   c) to permit the court-appointed expert and his assistants to take photographs or film for documentation purposes, to take written notes and/or to use a dictaphone for his notes, and to make copies and printouts at the applicant's expense;

   d) digital evidence, i.e. the certification documents (including the test report for procedure BSI-K-TR-0612-2024 and, in particular, the documents mentioned in Chapter 7.3/7.4 of the Conformity Report, including the Secure Platform Concept (version 1.0.2) and the Swissbit Cloud SMA ERS – Guidance Documentation (version 1.0.3)); source codes and software documentation, including flowcharts, operating and installation manuals, and development documentation, including requirements and specifications; to provide configuration files, logs and operational data, including documentation detailing the specific software and hardware versions of all TSE components in the operating environment relating to the respondents' Swissbit Cloud-TSE 2, and to disclose all passwords and data necessary to access the digital evidence;

   e) to permit the court-appointed expert and his assistants to make copies of the digital evidence;

   f) to hand over to the court-appointed expert and his assistants technical documentation, internal development documents, manuals and records relating to the design, configuration, certification and deployment of the respondents' Swissbit Cloud-TSE 2 or, in the alternative, to permit the court-appointed expert and his assistants to make copies of these documents;

   g) to inform the expert and his assistants of the exact location of the evidence referred to in paragraph 1 and to remove any obstacles to access, such as password protection for access to electronic documents, or to open any locked rooms or cupboards.

7. The persons involved in carrying out the inspection and the preservation of evidence, and in particular the bailiff, the expert (including his assistant) and the applicant's legal representatives, are obliged to keep confidential, both from third parties and from the applicant, any facts that come to their knowledge in the course of executing the order in its entirety.

Furthermore, until an order for release is issued by the Unified Patent Court, the aforementioned persons must not provide any opportunity the applicant or third parties to inspect the respondents' cloud-based and certified technical security device designated 'Swissbit Cloud-TSE 2', any documents that may have been seized, or the detailed description to be prepared by the expert.

8. The respondents are to be requested to comment on any confidentiality interests following the submission of the expert's detailed description. The applicant's UPC representatives referred to in paragraph 5 will be given the opportunity to comment on the respondents' statement. The court shall then decide whether and to what extent the applicant is to be personally informed of the expert's detailed description and the preserved evidence, and whether the duty of confidentiality for the applicant's UPC representatives referred to in paragraph 5 is to be lifted.

9. The applicant is obliged to bear the costs of the inspection and the preservation of evidence, including the preparation of the detailed description by the expert. The applicant is ordered to pay the expert a reasonable advance on costs, to be determined by the expert, prior to the commencement of the inspection, unless the expert waives such an advance.

10. The order is to be served personally on the respondents at the premises referred to in paragraph 1. a), together with a copy of the application, including its annexes, as well as the notice of provisional measures and the instructions for accessing the proceedings (provided by the CMS), without delay at the time the measures set out in paragraph 1 are carried out. Service of these documents shall be effected in cooperation with the bailiff present at the time, appointed in accordance with paragraph 4 of the Order. Should it not be possible to effect service on the first respondent at the premises specified in paragraph 1. a), the Order shall be served in accordance with the general Rules.

11. In the event of a culpable breach of this order, the court may impose a penalty payment for each breach, the amount of which the court may determine having regard to the circumstances of the individual case.

12. The measures relating to inspection and the preservation of evidence shall be revoked on application by the respondents or shall otherwise cease to have effect if the applicant does not, within a period of no more than 31 calendar days or 20 working days, whichever is longer, after the detailed description to be drawn up by the expert in accordance with paragraph 1(b) aa) to be drawn up by the expert has been disclosed to the respondents, or the court has ruled by a final decision not to grant access to this detailed description, the applicant has brought an action against the respondents.

13. The order shall only take effect once the applicant has provided security in favour of the respondents in the form of a deposit of EUR 10,000.00.

14. In all other respects, the application for inspection and preservation of evidence is dismissed."

7. The inspection and preservation of evidence took place on 19 May 2026.

8. The expert witness Grannemann carried out the inspection and preservation of evidence at the respondents' premises in Munich, assisted by the senior bailiff Seisenberger and the IT forensic experts Dipl. Inf. Unucka and Aßmus (see the expert's detailed report of 15 June 2026 and the enforcement record of 19 May 2026). Also present on site throughout the proceedings were the applicant's representative, Attorney-at-law Sebastian Dworschak, the applicant's representative, patent attorney Ralf Emig, and, at times, the representative of the second respondent, patent attorney Michael Platz-öder, the representative of the second respondent, Dr Thomas Lynker, an Attorney-at-law, as well as Zeljko Angeloski, Director of Marketing at the second respondent, and Hubertus Grobbel, Vice President of Security Solutions, who, according to his own statement, is employed by the second respondent
2. Furthermore, Chris Schwarze, Managing Director of the second respondent, and Nicolas Schneider, Technical Director of the second respondent, were connected via video link at times.

9. During the inspection and preservation of evidence, the following documents relating to the identified software versions were inspected and secured:

   a) Swissbit Cloud CSP-L – Guidance Documentation, Version 1.1.5 (d2dac dec38e278adc011f1af19660d13b12c4a22), 6 November 2024 (Exhibit SV1)

   b) Swissbit Cloud-TSE 2 – Secure Platform Concept (Environmental Protection Concept, USK), Version 1.0.2 (7180367829459d9466d54daee97a431f04ad1d39), 9 July 2024 (An-
   nex SV2)

   c) Swissbit Cloud-TSE 2 – Trust Provisioning Concept, Version 1.0.3 (2e3d02f82937bc525387dd867faef2321211a281), 30 August 2024 (Appendix SV3)

   d) CSPL (Cryptographic Service Provider Light) Operating Manual, Doc ID 7622, Rev. 00, Temp. ID T4653, T_Rev. 00, L_review 12 June 2025, Responsible: Hubertus Grobbel (excerpts from pages 1–13 included here as Appendix SV4)

   e) Swissbit Cloud SMAERS – Guidance Documentation, Version 1.0.3 (2e3d02f82937bc525387dd867faef2321211a281), 30 August 2024 (Appendix SV5)

   f) Swissbit Cloud-TSE 2 – Update Concept, Version 1.0.2 (7053f1e02a2b7328810bad83cc35681a81da34ae), 9 August 2024

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

   h) Swissbit Cloud CSP-L – Security Architecture (ARC), Version 1.1.2 (0fcba72f0dfa9bf44b86fa50867176eb8f4fff6c), 8 July 2024

   i) Swissbit Cloud CSP-L – TOE Design (TDS), Version 1.3.1 (0fcba72f0dfa9bf44b86fa50867176eb8f4fff6c), 8 July 2024 (Appendix SV6)

j) Source code package fiscal3-smaers-smaers-v1.0.5, comprising, amongst other things, the files Csp.java (Annex SV7a)

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

k) Source code package fiscal3-cspl-v1.0.7, comprising, amongst other things, the files

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

l) Source code package fiscal3-smaers-tss-v1.0.5

10. The expert prepared his detailed report on 15 June 2026.

11. By document dated 18 June 2026, the respondents filed an application for a review of the order for inspection and preservation of evidence pursuant to Rule 197.3 of the RoP, which was heard orally online by the Düsseldorf local division on 25 August 2026.

APPLICATIONS:

12. The respondents request that

    I. that the order of the Düsseldorf local division of the Chamber of Commerce dated 27 April 2026, Ref. UPC_CFI_1332/2026, be reviewed at the oral hearing;

    II. that the order of the Düsseldorf local division of 27 April 2026, Ref. UPC_CFI_1332/2026, be set aside;

    in the alternative,

    III. to amend the order of the Düsseldorf local division dated 27 April 2026, Ref. UPC_CFI_1332/2026, and, in addition, to instruct the expert in the order under review to bring the products, documents, records and/or media before the court in the event of an action on the merits being brought, once the detailed description has been finalised.

13. The applicant requests that

    that the order of the Düsseldorf local division of 27 April 2026 be confirmed.

FACTUAL AND LEGAL ISSUES:

14. The respondents submit:

15. The applicant has failed to demonstrate a sufficient likelihood of infringement in respect of the decisive features 6.4b and 6.6 of claim 6 of the patent in suit, which relate to the so-called gap-filling mechanism. The features in question read as follows:

    6.4b *[wherein the signature device (8)] comprises a data record buffer (24) for buffering signed transaction data records (15)*

    6.6a *wherein the signature device (8) is configured to load at least one previously signed transaction record (23) from the record buffer (24) when a gap is detected between a current value of the key usage counter and the corresponding value of a last signed transaction record in the transaction memory (16)*

    6.6b *and [wherein the signature device (8) is configured] to transmit the loaded at least one previously signed transaction data record (23) to the registration device (6)*

16. Whether and to what extent the embodiment at issue actually implements this mechanism is, by the applicant's own admission, unknown to it. Accordingly, it relies exclusively on an expert opinion submitted by a party

by Prof. Dr Eidenberger, who, whilst assessing implementation as 'highly probable', bases this on the far-fetched consideration that the regulatory framework restricts the technical scope to such an extent that only the solution as claimed in the patent can be considered. The latter is manifestly incorrect.

17. The BSI guideline TR-03153 requires that no messages be lost during transmission and that no gaps arise in the sequences (see also the application, para. 100). However, the guideline does not prescribe any specific internal algorithm and, in particular, does not require the buffering of signed data records in the signing device. This is also acknowledged by the applicant and its expert.

18. It is untenable that the local division nevertheless considered it likely that these features would be realised *'in view of the expert opinion […]*'. On the contrary, the applicant and her expert had already put on record an equivalent, non-infringing alternative in which the problem of connection dropouts would also need to be resolved, but which in any case did not require a storage medium in the signature device.

19. Furthermore, numerous technical alternatives could be considered to completely avoid the alleged 'gap problem' identified by the applicant from the outset. In the case of these technical alternatives, features 6.4b, 6.6a and 6.6b of claim 6 of the patent in suit would likewise not be realised, whilst compliance with the guidelines would nevertheless be ensured. Taking these non-patented alternatives into account, the local division should have concluded that there was no sufficient likelihood of infringement.

20. Even if one were to assume a sufficient likelihood of infringement, the applicant would in any event have had to exhaust all other means of evidence available to it, which it failed to do. The applicant should have set out in concrete terms its unsuccessful efforts, such as internet searches, analyses of advertising material, a test purchase and a technical examination of the contested embodiment, as well as enquiries among customers. In any event, this is not apparent from the applicant's submissions. There is a complete lack of detail regarding which attempts to purchase were made, when they took place and with which distributor, meaning that the balancing of interests falls to the applicant's detriment.

21. Furthermore, the local division had also wrongly assumed that the applicant's application was urgent and that the *ex parte* order was necessary. There was neither a risk of evidence being destroyed nor a risk that it might no longer be available for other reasons. The fact that the contested product is BSI-certified (BSI-K-TR-0612-2024) already directly contradicts any risk of manipulation or destruction of documents, as this would result in the loss of certification.

22. The assumption that the respondents could have concealed the source code or other documents or rendered them inaccessible is also unrealistic in view of their BSI and ISO 27001 certifications. Due to the certified business processes, employees must have access to the systems at all times, regardless of the storage location. Therefore, the respondent could not have used the argument that the source code was stored in

Switzerland, which the claimant was aware of. Furthermore, enforcement in Switzerland is guaranteed by that country's membership of the Lugano Convention.

23. Furthermore, in view of the numerous alternatives to the solution claimed in the patent, the local division should at least have discussed with the parties, in the inter partes proceedings, whether the solution claimed in the patent had been implemented.

24. Furthermore, the time that elapsed between becoming aware of the embodiment under investigation in April 2025 and the filing of the application on 20 April 2026 would argue against the urgency required for an ex parte order.

25. The order for the preservation of evidence and inspection is also disproportionate. As is apparent from paragraph 147 of the application, the BSI certification relates to specifically tested software versions, the components of which can be identified by means of specific hash values. The use of modified software would take place outside the scope of the – mandatory – certification.

26. It follows directly from this that any modification to the respondents' certified software is always 100 per cent verifiable. For if, in relation to a particular source code, a hash value different from that on file for the certified software were to be found, this would constitute direct evidence that the source code in question was not that of the certified software. This circumstance should have been sufficient reason for the local division to consider less intrusive measures than the unannounced and forced entry into the respondents' business premises, together with the seizure of the source code, as granted by the order. An order requiring the production of the source code could, in any event, have served the applicant's purpose in the same way. With the source code, the applicant would have obtained everything necessary to verify whether or not the features 6.4b and 6.6 were present. No further documentation, log files or the like, nor an examination of the software's use in the operational environment, would be required for this purpose.

27. Furthermore, the order is also inappropriate in view of the ongoing licence negotiations between the parties. In the application regarding the licence negotiations, the applicant had presented an incomplete account and thus painted an inaccurate picture. At the time the application was filed on 20 April 2026, the licence negotiations between the parties were in fact still ongoing and, from the respondents' point of view, were certainly (still) promising.

28. The applicant submits:

29. Features 6.1–6.4a and 6.5 could already have been reliably established on the basis of the certifications and the relevant BSI guidelines. Only with regard to features
6.4b and 6.6, residual doubts had existed, although the sufficient likelihood of infringement in respect of these features was evident from the regulatory framework and the expert opinion of Prof. Eidenberger.

30. The conceivable alternatives put forward by the respondents – the equivalence of which to the solution claimed in the patent is disputed – do not preclude the issuance of an order for the preservation of evidence and an inspection order.

31. Nor had the respondents demonstrated that the embodiment under investigation was more likely to use a mechanism other than that described in the patent to ensure the completeness of the transaction data records.

32. The mere fact that the solution claimed by the patent has been publicly available since the publication of the patent application for the patent in question suggests, on an ex ante basis, that the respondents would use the solution claimed by the patent. The further fact that the protective letter submitted by the respondents did not contain any arguments regarding non-infringement further corroborated the likelihood of infringement ex ante. It is this ex ante assessment that is decisive.

33. Similarly, the fact that the respondents had refused, out of court – for example, during the licence negotiations – to disclose the solution they had chosen to ensure the completeness of the transaction data records further corroborated the likelihood of infringement ex ante.

34. Furthermore, the inspection was also necessary for the claimant in order to be able to prove the patent infringement beyond doubt. The claimant had already exhausted all other reasonable sources of information beforehand. In particular, it had also carried out extensive research in publicly accessible sources, as the references in the application for inspection would show.

35. The processes of the contested embodiment relevant to proving the fulfilment of the claims – particularly with regard to the gap-filling mechanism in the signature device – took place on a specialised, secure infrastructure in the cloud. Although a trial purchase would have enabled the use of the contested embodiment, it would have been hardly conceivable to draw conclusions from this regarding the specific design of the gap-filling mechanism. An attempt had been made to purchase the contested embodiment, but it had failed. Even setting that aside, such a purchase would not in any case have contributed to clarifying the matter and would not only have been an ‘equally effective’ means, but would have been entirely unsuitable for further clarification of the patent infringement.

36. It seems entirely out of the question that users of the software would have any technical access to the software code at all, let alone be able to decompile it. Thus, from a technical point of view alone, it is ruled out that a trial purchase would have been suitable for further clarifying the patent infringement. Furthermore, from a copyright perspective, decompilation is, in principle, reserved for the rights holder and is therefore not permitted even for the applicant, not even for the purpose of obtaining evidence of infringement.

37. Furthermore, in order to prove whether the solution covered by the patent is being used, it is necessary not only to obtain the source code but also further information, such as, in particular, development information, and, in addition, to examine the operating environment and the system architecture of the contested embodiment whilst it is in operation.

38. With regard to the ex parte order, the applicant argues that the respondents did not present any new facts or evidence in their application for review, meaning that the court has no different factual basis than it would have had if it had conducted a hearing at short notice prior to issuing the order.

39. The cross-border corporate structure of the respondents – with the registered office of the certified first respondent being located abroad in Switzerland – further gives rise to a concrete risk of potential obstruction of evidence should a preservation and inspection measure be announced; in particular, this is the case from an ex ante perspective.

40. In particular, with cloud solutions such as the version at issue, it is possible to make actual access to the cloud, or to the underlying system architecture and source code, more difficult and to frustrate such access.

41. Nor does the certification of the specific implementation at issue rule out acts of obstruction. It is true that, in principle, a modification to the software can indeed be detected on the basis of the specific hash values. However, the certification would not have prevented the defendants from making it more difficult or refusing access to documents, log files and source code, provided they were given adequate advance notice through a hearing. The decisive factor is not only the question of whether the software can be manipulated, but also, in particular, that of its traceability.

42. Furthermore, the applicant's knowledge, dating back to 2025, of the offer of the contested embodiment does not preclude the issuance of the inspection order, as an inspection order does not require any sense of urgency.

43. The order is also proportionate. In particular, the inspection order represents the least onerous suitable means of preserving evidence. The applicant had either exhausted all alternatives or they were not equivalent.

44. Nor would an order to produce evidence pursuant to Article 59 of the UPC Agreement have been equivalent. Under Article 59(1), second sentence, of the UPC Agreement, such an order must not lead to an obligation to incriminate oneself (under criminal law); in other words, the respondents could, on that basis, have selected the evidence themselves and withheld information decisive for the patent infringement. Furthermore, the mere production of documents would not have made it possible to examine the operating environment and system architecture of the embodiment under investigation whilst it was in operation. Moreover, an order for the preservation of evidence and inspection pursuant to Article 60 of the UPC Agreement is not subsidiary to an order for the production of evidence pursuant to Article 59 of the UPC Agreement.

45. Furthermore, the procedure under Article 60 of the UPC Agreement, by its very structure, already provides for a balancing of the interests of the party subject to inspection and the party requesting it.

46. Furthermore, the order of 27 April 2026 contains, in paragraphs 5, 7, 8 and 13, extensive safeguards in favour of the respondents: the expert is bound to confidentiality vis-à-vis third parties; the applicant is personally excluded from participation; the court-appointed expert has been brought in as a supervisory authority

, the court has reserved the right to decide on the disclosure of the expert's report, and the provision of security has been ordered.

47. Even in light of the licence negotiations between the parties, the order remains proportionate. The respondents' assertion that the application for an inspection came as a 'complete surprise' to them is incomprehensible, given that they had filed a protective letter in November 2025. The applicant had been interested in reaching an amicable resolution to the dispute and had proposed an assessment by a neutral body for this purpose. However, the respondents had rejected this.

48. Reference is also made to the documents submitted by the parties.

REASONS FOR THE ORDER:

49. The respondents' application for an examination is admissible. However, it is largely unfounded and is successful only to the extent of the alternative claim.

I. Admissibility of the application for review

50. There are no objections to the admissibility of the application for review.

51. Pursuant to Rule 197.3 of the RoP, the application for review of the order for the preservation of evidence must be lodged 30 days after the measure has been carried out. The preservation of evidence and inspection took place on 19 May 2026. The respondents lodged the application for review on
18 June 2026 and thus within the time limit.

II. (Un)merits of the application for review

52. The respondents' application for review is successful on the merits only in respect of the alternative claim.

1. Principles

53. The Düsseldorf local division has previously endorsed the principles established by the Brussels local division in the order of 12 November 2025 (UPC_CFI_407/2025 – Organon Heist v Genentech) (see also UPC_CFI_834/2025 (LD Düsseldorf), Order of 19 December 2025, para. 34 et seq. – Ecovacs Robotics v. Roborock) and continues to adhere to them. Accordingly, the Court must carry out a two-part assessment as part of the review under Rule 197.3 of the RoP:

54. Firstly, the court must examine whether it was correct to issue an ex parte order for inspection and preservation of evidence (Rule 194.1(d) in conjunction with Rule 194.2 of the RoP). In making this assessment, the court must take into account the facts and evidence (i) set out in the application for an order for inspection and preservation of evidence, and (ii) which, insofar as they have not been disclosed to the court, are either publicly known or are deemed to be reasonably known to the applicant. Where facts and evidence have not been disclosed, the court must examine whether this omission is to be regarded as a breach of the applicant's duty under Rule 192.3 of the RoP. Under that provision, the applicant must disclose all facts known to them

which might influence the court's decision as to whether an order should be issued without a hearing of the defendant.

55. The court must then assess whether the order for inspection and preservation of evidence is to be varied, set aside or confirmed, Rule 197.4 of the RoP. In making this assessment, the evidence to be taken into account is not limited to that which is either in the public domain or of which the applicant is reasonably aware. Rather, this assessment encompasses all facts and evidence put forward by the parties,
Rule 197.3(b) of the RoP. The assessment relates to the substantive examination of the conditions for issuance (Article 60(1) and (3) of the UPC Agreement) as well as the scope and conditions set out in the order for inspection and preservation of evidence.

56. The aforementioned assessment steps must be carried out with reference to the time at which the order under review was issued.

57. The review therefore does not extend to the enforcement of the order for inspection and preservation of evidence, the outcome of such enforcement, or any information (evidence) gathered during enforcement.

58. The granting of an order for the preservation of evidence and inspection presupposes that a patent infringement appears plausible; excessive standards of proof must not be imposed. According to the case law of the Court of Appeal, the standard of proof in inspection proceedings must not be set too high (UPC_CoA_239/2025, order of 28 May 2025, para. 9 et seq. – Centripetal v. Palo Alto). A credible allegation of a possible patent infringement is sufficient (UPC_CFI_834/2025 (LD Düsseldorf), Order of
4 September 2025, p. 15 – Ecovacs Robotics v Roborock). The requirement under Article 60(1) of the UPC Agreement to submit 'reasonably available evidence' therefore represents a lower standard than the burden of proof in infringement proceedings, particularly in respect of those features for which the applicant has no access to evidence (UPC CoA, loc. cit., para. 12).

2. Application to the present case

a) On a sufficient likelihood of infringement

59. The applicant has demonstrated a sufficient likelihood of infringement (Article 60
(1) UPC Agreement.

60. Even though, as already explained, no excessive requirements are to be imposed on the demonstration of a likelihood of infringement in proceedings for the preservation of evidence, mere speculation that the patent might be infringed is not sufficient to issue an order for the preservation of evidence. In order to rule out a purely exploratory search for evidence (a so-called 'fishing expedition'), which has no basis in Article 60 of the UPC Agreement, the granting of an order therefore requires that it appears plausible that the patent is being infringed. This applies in particular where, as in the present case, the order for the preservation of evidence was issued without hearing the respondent's side (UPC_CoA_239/2025, order of 26 May 2025, para. 12 – Centripetal v Palo Alto).

61. On the basis of these principles, the applicant has demonstrated a sufficient likelihood of infringement in its application for the preservation of evidence and inspection. The outcome of the expert opinion obtained in the context of the present proceedings is irrelevant at this stage in the light of the required ex ante assessment.

62. The applicant's submissions were not limited to the assertion that its patent might be infringed. Rather, she simultaneously submitted a private expert report by Prof. Eidenberger, from which she, in conjunction with the regulatory framework, has set out in a comprehensible and therefore plausible manner why she also assumes a (possible) infringement of features 6.4.b. and 6.6. of claim 1 of the patent in question, which form the core of the dispute. Whether, as Prof. Eidenberger assumed in his expert opinion, the regulatory framework actually restricts the technical scope to such an extent that only the solution disclosed in the patent can be considered does not require a definitive assessment at this stage. In any event, Prof. Eidenberger's expert findings, taken in conjunction with the regulatory provisions, at least allow the conclusion that the technical teaching protected by the patent in question is a serious possibility. This is sufficient to establish a plausible case for the likelihood of infringement.

63. Furthermore, the parties had already been engaged in licence negotiations for some time prior to the application for an order to carry out an inspection and preserve evidence. The respondents indisputably rejected the applicant's proposal, made during these negotiations, to have the embodiment in question assessed by a neutral body. This naturally and justifiably fuelled the applicant's suspicion that the respondents were making use of the technical teaching of the patent at issue.

64. Furthermore, the respondents had already filed a protective letter in the run-up to the inspection proceedings. The fact that this protective letter did not contain any arguments regarding non-infringement reinforced, in the required ex ante assessment, the existence of a sufficient likelihood of infringement.

65. Contrary to the respondents' view, a sufficient likelihood of infringement cannot be ruled out merely on the grounds that—which, in the present case, does not require a conclusive assessment—alternative solutions that do not infringe the patent may exist.

66. As already set out in detail, the applicant has plausibly demonstrated, by means of a private expert report and taking into account the regulatory framework, the respondents' pre-trial conduct and the protective letter submitted by them, the possibility of an infringement of the patent at issue by the embodiment under investigation. If possible alternative solutions exist, it is precisely one – if not the – essential purpose of the proceedings for the preservation of evidence to investigate further, on the basis of the suspicion of a possible patent infringement grounded in specific connecting facts, and to secure evidence as to whether, and if so to what extent, the embodiment under investigation makes use of the technical teaching protected by the patent in question, and not, in fact, from a possible alternative solution.

67. Possible alternative solutions preclude the order of measures to preserve evidence only if they render the applicant's submission regarding a possible infringement of the patent in question no longer plausible. However, this is not the case here.

b) Exhaustion of all other out-of-court means of obtaining evidence

68. The Chamber is unable to establish that, prior to filing the application, the applicant had failed to exhaust all other sources of information available to her which were reasonable, promising and involved a lower level of intrusion.

69. It need not be determined whether the applicant's arguments, which are merely general in nature, are sufficient to demonstrate a serious attempt to carry out a test purchase. Even if such a test purchase had been possible, it is not apparent that it would have enabled the applicant to sufficiently clarify the functioning of the embodiment at issue and, in particular, the implementation of features 6.4.b and 6.6, which form the core of the proceedings for the preservation of evidence. The applicant has disputed this on the grounds that it seems entirely out of the question that users of the software would have any technical access to the software code at all and would be able to decompile it. The embodiment under investigation is a distributed system in which the signature device—which is particularly relevant to features 6.4.b and 6.6—is not located in the till system but in a separate environment in the cloud. The respondents were unable to refute this. In particular, they did not explain whether, and if so how, a test purchase alone would have enabled the applicant to analyse the embodiment at issue in such a way as to take sufficient account of its interest in clarification and the preservation of evidence (see, however: UPC_CFI_834/2024, (LD Düsseldorf), Order of 4 September 2025 – Ecovacs Robotics
v. Roborock).

70. In addition to the lack of information that could be obtained from a test purchase, the applicant has plausibly demonstrated that even the comprehensive searches it carried out in publicly accessible sources were not sufficient to dispel any remaining doubts regarding the possible realisation of features 6.4.b and 6.6.

c) Ex parte order

71. The issuance of the ex parte order was justified.

72. Pursuant to Rule 197.1 of the RoP, the court may order measures to preserve evidence without prior hearing of the defendant, in particular where a delay would likely cause the applicant irreparable harm or where there is a demonstrable risk that evidence might be destroyed or might no longer be available for other reasons.

73. In any event, the conditions of the second scenario are met in the present case.

74. Even if – as may be assumed in favour of the respondents – subsequent manipulation or alteration of the certified source code is not possible and

a change to the software is, in principle, detectable on the basis of the specific hash values, this would not have prevented the respondents from at least making it more difficult to gain access to documents, log files and source codes by means of a hearing, provided they were given adequate advance notice. By contrast, the mere traceability of possible manipulations would be of no help to the applicant. It would merely lead the applicant to realise that it might have to repeat the inspection if necessary.

75. This circumstance alone already justifies an ex parte order. In the present case, however, the cross-border corporate structure of the respondents is an additional factor. Even if the respondents – which may be assumed in their favour – have not yet used this structure to obstruct the taking of evidence, nor had any specific intention to do so, this structure, from the applicant's relevant ex ante perspective, increases the risk that certain items of evidence would be withheld from the applicant or, at the very least, that access to them would be made more difficult were the respondents to be heard beforehand.

76. Nor were the respondents' rights unduly infringed by an ex parte order.

77. It is true that the respondents rightly pointed out that an inspection of their business premises involves a high degree of intrusion. However, it has neither been argued nor is it apparent that the inspection went beyond this to cause a specific disruption to the respondents' business operations. By contrast, the respondents' interest in confidentiality was taken into account, in particular, by the extensive protective measures set out in paragraphs 5, 7, 8 and 13 of the order of 27 April 2026.

d) Urgency

78. R.194.2(a) of the RoP states that, in exercising its discretion, the court must take into account the urgency of *the claim*. Neither the UPC Agreement nor the RoP provide for a criterion of urgency regarding the preservation of evidence and/or inspection, as is found in the rules on the order of provisional measures, when assessing whether an application for the preservation of evidence and/or inspection should be granted (UPC_CoA_2/2025, Order of 15 July 2025, para. 35 – Valinea v Tiru).

79. That being said, the urgency of the claim and, consequently, the necessity of ordering an inspection and preservation of evidence are established in the present case. The fact that the respondents refused, out of court during the licence negotiations, to disclose the solution they had chosen to ensure the completeness of the transaction records already indicates the urgency of the claim.

e) Proportionality

80. The order for inspection and preservation of evidence is also proportionate.

81. In so far as the respondents seek to challenge the proportionality by referring to the possibility of an order requiring the production of the source code,

such an order is not an equivalent measure.

82. Firstly, such an order to produce source code would have entailed the risk that the respondents might appeal to Article 59(1)(2) of the UPC Agreement. Under that provision, the production of evidence must not lead to an obligation to incriminate oneself (under criminal law). Had the applicant confined itself to an application for an order requiring such production, there would therefore have been a risk that the respondents would themselves have selected the evidence on that basis and withheld the information decisive for the patent infringement. Furthermore, the mere production of documents would not have enabled the expert to examine the operating environment and system architecture of the embodiment under investigation whilst it was in operation, which the Chamber considered necessary in order to assess whether the respondents were using the mechanism described in the patent to ensure the completeness of the transaction data records.

83. The fact that the application for the preservation of evidence and inspection was filed despite ongoing licence negotiations is irrelevant, as the parties have not entered into any agreement precluding legal action whilst licence negotiations are ongoing.

3. Alternative claim

84. As the applicant raised no objections to the respondents' alternative application to supplement the order of the Düsseldorf local division of 27 April 2026 with a production order directed at the expert, such an order could be made as set out in the operative part.

III. Disclosure and protection of confidential information

85. Confidentiality interests may be asserted independently of an application for examination under Rule 197.3 of the RoP and require a separate assessment (see UPC_CoA_177/2024, Order of 23 July 2024, para. 12 – Progress Maschinen & Automation v AWM). A separate decision will therefore have to be made following the examination proceedings regarding the scope of disclosure of the detailed description, taking into account the confidentiality interests asserted by the respondents.

ORDER:

I. In response to the respondents' alternative application, the order of the Düsseldorf local division of 27 April 2026 is supplemented to the effect that the expert is additionally instructed, in the event of a main action being brought against the first respondent and/or the second respondent, to transport the products, documents, records and/or media to the registry of the Düsseldorf local division once the detailed description has been finalised.

II. In all other respects, the respondents' application for an examination is dismissed.

Issued on 7 September 2026 NAMES
AND SIGNATURES

Presiding Judge Thomas	Digitally signed Thomas Ronny 3 September 2026 13:55:57 +0200 Unified Patent Court Einheitliches Patentgericht Juridiction unifiée du brevet
Legally qualified judge Adocker	Thomas Adocker Digitally signed by Thomas Adocker Date: 3 September 2026 15:07:56 +02'00'
Legally qualified judge Dr Schumacher	Digitally signed Schumacher Jule Kathrin 3 September 2026 14:11:47 +0200 Unified Patent Court Einheitliches Patentgericht Juridiction unifiée du brevet
On behalf of the Deputy-Registrar	LAURA CHANTAL DANIEL Digitally signed by LAURA CHANTAL DANIEL Date: 3 September 2026 15:30:17 +02'00'

INFORMATION REGARDING THE APPEAL

The parties may appeal against this order within 15 days of its service (Art. 73(2)(a), 60 UPC Agreement, R. 220.1(c), 224.1(b) RoP).