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 27 April 2026 concerning EP 4 285 308 B8

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, Nordemann Czychowski & Partner Solicitors and Attorneys-at-law mbB, Kurfürstendamm 178, 10707 Berlin, Germany
email address:	sebastian.dworschak@nordemann.de
Patent Attorney involved:	Ralf Emig, Maikowski & Ninnemann Patent Attorneys Partnership mbB, Kurfürstendamm 54-55, 10707 Berlin, 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 directors Lars Lust and Chris Schwarze, Bitterfelder Straße 22, 12681 Berlin, Germany

PATENT APPLICATION:

EUROPEAN PATENT NO. EP 4 285 308 B8

PANEL:

Panel 1 of the Düsseldorf local division JUDGES:

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 MATTER: Art. 60 UPC Agreement, R. 194(d), 196, 197, 199 of the RoP – Application for inspection and preservation of evidence

SUMMARY OF THE FACTS AND THE APPLICANT'S SUBMISSIONS:

1. On 20 April 2026, the applicant filed an application for an order for inspection and preservation of evidence at the respondents' German premises. No action on the merits has yet been brought, but the applicant has stated that it intends to bring such an action before the Düsseldorf local division following the requested inspection.

2. The applicant is the proprietor of European Patent EP 4 285 308 B8 (the corrected patent specification B8 corresponds in content to the version of EP 4 285 308 B1, 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 EP application 21154250 of 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. The unitary effect was registered on 2 September 2024.

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

4. The patent in question is entitled "SECURELY REGISTERING A SEQUENCE OF TRANSACTIONS". The applicant's application relates primarily to claim 6 and to dependent claims 7–9, which refer back to it, as well as to independent claims 1, 10 and 12. In the English language of the proceedings, the 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 a 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 reject providing a signature of a new unsigned transaction record (10) in response to detecting a gap between the present 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 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) in response to the detection of a gap between the compared values."

Claim 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 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)."

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

Claim 1:

"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 signature device (8) comprises a key usage counter which 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 signing, wherein the method comprises: comparing a current value of the key usage counter with a most recently recorded value, wherein the most recently recorded value is the corresponding 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 6:

"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) that 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 last 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 7:

"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 recent signed transaction record to the signature device (8)."

Claim 8:

"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 record (10) in response to the detection of a gap between the current value and the associated value of the last signed transaction record."

Claim 9:

"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 gap between the compared values, requests a retransmission of at least one previously signed transaction record (23) from the signing device (8)."

Claim 10:

"A computer program comprising instructions for causing a registration device (6), comprising a transaction memory (16) for storing signed transaction records (15), each signed transaction record (15) comprising an associated value of a key usage counter at the time of signing, to perform the following steps: accessing the transaction memory (16) and determining the associated value of the last 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 record (23) is loaded from the signature device (8) from a 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 12:

"A computer program comprising instructions for causing a signature device (8) having a key usage counter, wherein the 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 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 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 most recently recorded value, and transmitting the loaded at least one previously signed transaction record (23) to the registration device (6)."

6. In its application, the applicant states that the respondents are part of the Swissbit group of companies. The first respondent, based in Bronschhofen, Switzerland, was founded in 2001 and is a technology company specialising in solutions for data storage and the protection of data and digital identities. It develops and manufactures, among other things, hardware security solutions such as products with Technical Security Devices (TSEs) for use in point-of-sale systems (Exhibits NM AST 6 and NM AST 7). It has also begun to develop and market cloud-based TSE solutions. Under the name 'Swissbit Cloud-TSE 2' (hereinafter: the contested embodiment), it markets its cloud-based, certified technical security device for the tamper-proof recording of point-of-sale data. It

it offers this in various ‘subscription’ models (Annex NM AST 8).

7. The applicant further states in its application that the second respondent, based in Berlin, is the German subsidiary of the Swissbit Group (Annex NM AST 9). The scope of its business includes, among other things, the development, distribution and, subject to the necessary approvals, the production of electronic components and systems such as the contested embodiment. Through its technical systems, it enables the operation of the contested embodiment in Germany (Annex NM AST 10).

8. In 2025, the claimant became aware that the first respondent had been offering its product ‘Swissbit Cloud-TSE 2’ in Germany since 1 April 2025. It subsequently contacted the first respondent with a request for authorisation dated 12 September 2025 (Exhibit NM AST 11).

9. To further clarify the facts of the case, the applicant proposed a review by a neutral body which had already worked with both the applicant and the first respondent in the context of the certification process, namely SRC Security Research & Consulting (“SRC”). However, the first respondent rejected the proposed independent investigation by SRC. No independent review took place.

10. Subsequently, settlement talks took place between the parties. The first respondent denied any patent infringement but entered into negotiations concerning the licensing of the patent in suit for use in the first respondent’s software products and, in particular, cloud services. These talks have so far been inconclusive.

11. According to the claimant, the respondents are highly likely to be infringing the patent in suit by operating and offering the contested embodiment.

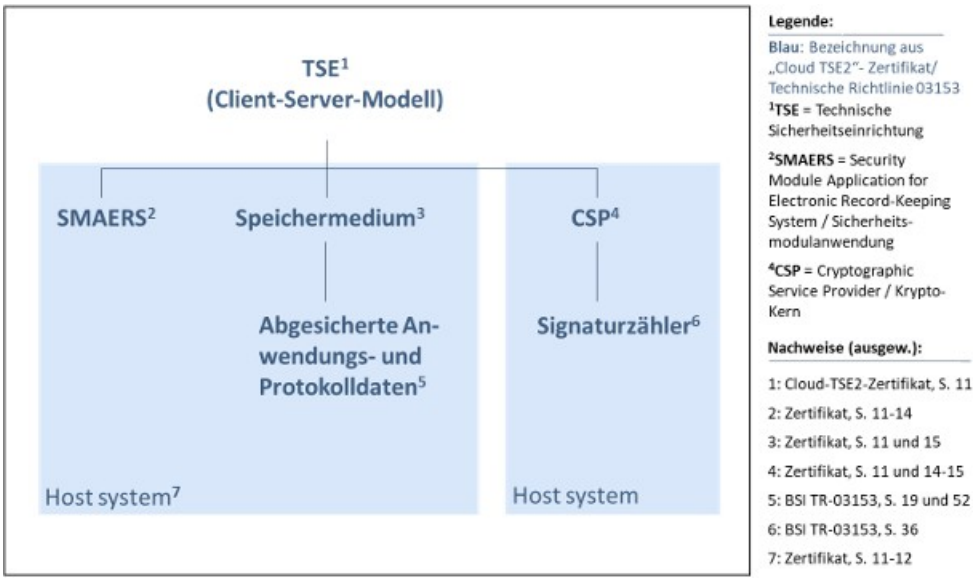
12. According to the claimant, the contested embodiment is a software-based Technical Security Device (TSE) for the field of electronic cash register systems. It serves the correct and tamper-proof recording of tax-relevant data in the context of electronic payment transactions (so-called
“fiscalisation of online cash register systems”). The use of certified security solutions has been a legal requirement since 2020, and their technology and design are strictly regulated.

13. The Technical Security Device (TSE) is intended for a cash register system such as those used in the retail sector. When a customer purchases a product and pays, a transaction is generated via the seller’s cash register system; the steps of this transaction are assigned a transaction number, logged in sequence, signed and permanently stored on the basis of the TSE. Via an interface, tax authorities in particular could obtain the signed receipt data and verify whether the company in question had recorded its tax-relevant transactions correctly and in full. The Technical Security Device (TSE) thus acts as a secure intermediary between the taxable seller and the tax authorities and ensures the integrity of the tax-relevant data recorded in the POS system.

14. The contested embodiment specifically divides the TSE into two system environments, namely

    - a first environment containing the security application, the so-called 'SMAERS' unit ('SMAERS' standing for 'Security Module Application for Electronic Record-keeping Systems'), and a storage medium, and
    - a second environment containing the so-called 'CSP' unit ('CSP' standing for 'Cryptographic Service Provider') with a signature counter.

15. The applicants' TSE is schematically represented as follows:



16. The TSE of the respondents comprises three (relevant in this case) components, namely the SMAERS unit, the storage medium and the CSP unit. The SMAERS unit is located together with the storage medium in a shared host system or Docker container.

17. The SMAERS unit serves to process all tax-relevant data from a cash register transaction. The data is captured by the SMAERS unit, prepared for signing by the CSP unit, and then sent to the CSP unit.

18. The CSP unit serves to sign the data transmitted by the SMAERS unit cryptographically, i.e. by encrypting it and applying a digital signature. It is located in a cloud environment separate from the SMAERS unit and the storage medium to ensure independent signing of individual transactions. The signature thus protects transactions and invoices from subsequent manipulation. In the context of cloud solutions, the CSP is also regularly referred to as 'CSP-L' ('L' stands for 'Light').

19. The signed, secured data is then sent back to the host system or the Docker container of the SMAERS unit and stored there on the storage medium. The storage medium enables the permanent storage of the transaction data.

20. The use of TSEs in electronic cash register systems is required by law and regulated. Due to their significance under tax law, TSE software solutions such as the contested embodiment must be reviewed by a certified testing body and certified by the (German) Federal Office for Information Security (hereinafter “BSI”) before they may be marketed. The relevant regulatory requirements arise primarily from Section 146a of the German Fiscal Code (AO), the Cash Register Security Ordinance and the BSI’s technical guidelines and security profiles based thereon. The contested implementation must therefore ensure that all business transactions in electronic systems – such as customer payment transactions – are recorded “individually, completely, correctly, in a timely manner and in an orderly fashion” (Section 146a(1) AO).

21. The contested implementation has obtained the certificates required for distribution – based on the Technical Guidelines and the protection profiles – from the BSI.

22. This includes, in particular, certification based on the central Technical Guideline BSI TR-03153, Version 1.1.1, which is assessed by the testing body or the BSI as part of the certification process for TSE software solutions. It contains binding technical specifications for the structure, functioning and security requirements of TSEs such as the contested embodiment.

23. By issuing the certificate for the Cloud-TSE-2 software of the first respondent, the testing body and the BSI had confirmed that the contested embodiment complied with all mandatory requirements of the BSI TR-03153 guideline. Compliance with these guideline requirements and the findings in the certification document therefore allowed clear conclusions to be drawn regarding the system architecture of the contested embodiment and thus regarding the likelihood of an infringement of the patent in suit.

24. The certification of the contested embodiment by the BSI clearly demonstrated the realisation of features 6.1–6.4a and 6.5 of the patent in suit in accordance with the feature breakdown in Annex NM AST 13; these are the following features:

    6.1 A distributed system (1) for the secure registration of a sequence of transactions

    6.2 wherein the distributed system (1) comprises a registration device (6) and a signature device (8)

    6.3 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)

    6.4a wherein the signature device (8) comprises a key usage counter

    6.5 wherein each signed transaction record (15) comprises an associated value of the key usage counter at the time of signing

25. With regard to the implementation of features 6.4b and 6.6a as well as 6.6b of the patent application in accordance with the feature breakdown in Annex NM AST 13, namely

    6.4b wherein the signature device (8) comprises a record buffer (24) for buffering signed transaction 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)

Although residual doubts remain, the findings of the expert (commissioned by it) [redacted] (Annex NM AST 20) indicate that the realisation of these features is also highly probable. Finally, the extrajudicial conduct of the first respondent also points to the infringement; although the respondent categorically rejects the allegation of patent infringement, it is nevertheless negotiating a licence for the patent in question and refuses an independent assessment by a neutral body.

26. In summary, whilst there are naturally only limited possibilities for ascertaining the specific configuration of the contested embodiment, it appears highly probable, against the background of the regulatory framework and the technical alternatives, that the contested embodiment implements a gap-filling mechanism in accordance with the patent, insofar as it complies with the legal framework.

27. On this basis, it is highly probable that claim 6 of the patent application is realised by the contested embodiment. For the same reasons, this also applies to the dependent claims 1, 10 and 12. Claim 1 protects, in a mirror-image manner, a method for implementing the distributed system according to claim 6. Claim 10 protects a computer program for implementing the registration device. Finally, claim 12 protects the computer program implementing the signature device. Similarly, it appears likely that sub-claims 7–9 are infringed, as these relate to further details of the specific implementation of the gap-filling mechanism; however, only an expert assessment based on the evidence to be secured could provide clarity as to whether they have in fact been infringed.

28. The respondents are using the patent in suit by operating and marketing the contested embodiment in a division of labour. Whilst the first respondent offers the contested embodiment in Germany, the second respondent enables and promotes this to a significant extent by operating at least parts of the systems within Germany.

29. The first respondent offers the contested embodiment in Germany. As early as in its press release on the occasion of the certification of the contested embodiment in April 2025, the first defendant stated that the “Swissbit Cloud-TSE 2” was “available with immediate effect […]” via its distribution partners (Exhibit NM AST 8).

30. The sales activities already underway are confirmed by the website of the first respondent. There, the first respondent presents the “Swissbit Cloud-TSE 2” with its technical specifications and areas of application and refers to a “flexible subscription model” for the use of the contested embodiment (Annex NM AST

21).

31. The contested product can also be subscribed to directly through a distribution partner of the first defendant, Jarltech Europe GmbH (hereinafter 'Jarltech'). The offers range from a usage period of 3 to 5 years. The first defendant is involved in this offer on several occasions. For instance, the respective offers on Jarltech's website refer to the terms and conditions of the first defendant (Exhibit NM AST 22). At the bottom of Jarltech's offer page, there is also a Swissbit product brochure for the contested embodiment, which, according to the copyright notice, originates from the first defendant. In this brochure, the first respondent comprehensively promotes the "Swissbit Cloud-TSE 2" and states itself that it "offers" the software solution (Exhibit NM AST 23, p. 2 at the bottom).

32. Furthermore, the first defendant is also the holder of the relevant BSI certificate (Exhibit NM AST 14), so that, on the whole, it must be assumed that the first defendant is offering the contested embodiment.

33. The second defendant acts as the German subsidiary and facilitates and promotes the distribution of the contested embodiment by co-developing and operating the necessary systems in Germany.

34. Numerous indications suggest that the infrastructure of the contested embodiment is operated in Germany. For instance, the contested embodiment is described in a YouTube video on the Swissbit YouTube channel, which presents the contested embodiment, as 'Developed, certified and operated in Germany' (Exhibit NM AST 24).

35. Similarly, the contested embodiment is advertised in the product brochure of the first respondent, which was attached to the quotation from Jarltech, with the features 'Made in Germany' and 'hosted in Germany' (Exhibit NM AST 23).

36. The fact that only the second defendant is eligible to operate the contested embodiment in Germany is supported by the fact that only it possesses locations in Germany that can be clearly attributed to such operation, that this corresponds to its business purpose, and that this is evidenced by a relevant TÜV certificate held by the second defendant.

37. The commercial register shows that German sites can be clearly attributed solely to the second defendant – and not to the first defendant (Annex NM AST 9).

38. Furthermore, the operation of at least subsystems of the contested embodiment by the second defendant is specifically evidenced by a German TÜV certification. This certificate expressly applies to the 'operation of a Cryptographic Service Provider Light' (CSP-L) (Annex NM AST 25).

39. It must be assumed that these CSP-Ls are used for the operation of the contested embodiment. The BSI TR-03153 guideline itself describes CSP-Ls as components of cloud-based TSEs only (p. 38 of the guideline, Annex NM AST 17).

40. Furthermore, as far as can be ascertained, the CSP-Ls in the Swissbit Group's product portfolio are relevant only to the contested embodiment, so that the

certified operation of the CSP-Ls by the second defendant establishes a direct link to the use of the contested embodiment (Annexes NM AST 18 and 19).

41. The two respondents would proceed on the basis of a division of labour with regard to the marketing, distribution and operation of the contested embodiment. Whilst the first defendant primarily handles the marketing and distribution of the contested embodiment, the second defendant provides the technical infrastructure for at least parts of the operation of the contested embodiment. The interlocking and integrated cooperation between the respondents in this regard, without a clear separation between them, is evidenced by several indications.

42. For instance, on the 'Swissbit' company website, the first defendant is listed first as the publisher in the legal notice. Immediately following this, however, the second defendant is also listed there under the heading 'Information on the national subsidiary in Germany' (Exhibit NM AST 26).

43. The connection between the respondents is also evident from their German locations. For instance, in addition to Berlin, there is apparently a further German location at Leuchtenbergring 3 in 81677 Munich. This location is also included in the TÜV certificate for the CSP-Ls (Exhibit NM AST 25) and is also attributed to the second defendant on the "Swissbit" website (Exhibit NM AST 27).

44. However, in the entry on the BSI website, the aforementioned Munich location is in turn allocated to the first defendant (Exhibit NM AST 28), so that there is apparently no strict demarcation of business operations, but rather joint action and a joint product offering by the affiliated companies must be assumed.

45. The cooperation between the defendants is also evident at the Berlin site. At the entrance gate to the defendants' Berlin site, only the designation
"Swissbit" is displayed without any distinction between the first or second defendant, and there is also no distinction on the doorbell sign/letterbox:

(Photo Annex NM AST 29)

46. Furthermore, the Swissbit trademark – affixed next to the doorbell sign – is registered in the name of the first defendant (and not, for example, in the name of the second defendant), so that a corresponding confusion exists here as well.

47. The close, division-of-labour relationship is also supported by the fact that the press release regarding Cloud-TSE 2 dated 28 May 2024 on the Swissbit website, as evidenced by the location detail there, originates from Berlin (Exhibit NM AST 14).

48. The activities of the respondents constitute a closely intertwined collaboration based on a division of labour, in which both companies make independent and indispensable contributions to the distribution and operational chain of the 'Swissbit Cloud-TSE 2'.

49. The requested inspection is necessary because, in the absence of alternatives, the applicant cannot fully prove the patent infringement without an inspection. None of the investigative measures taken to date have been able to clarify features 6.4b and 6.6, which the applicant has been unable to prove beyond doubt. This is also due to the nature of the contested embodiment, in which the processes relevant to the inspection take place within the software and – at least in part – within a special, secure infrastructure at the respondents' premises.

50. Nor is it to be expected that a trial purchase of the contested embodiment could contribute to clarifying the matter. For whilst such a purchase would enable the use of the contested embodiment, it is hardly conceivable that conclusions could be drawn from this regarding the specific design of the gap-filling mechanism. Regardless of whether it would even be technically possible or permissible to decompile the software in a purchased product, it is not to be expected that the relevant software components would be made available at all. Rather, it is to be expected that these would run on the respondents' servers, which applies in particular because the features 6.4b and 6.6, which are yet to be determined, relate to the cryptographic core (CSP), which would in any case run on the respondents' servers. From the purchaser's perspective, the use of the contested embodiment therefore presents itself as
a 'black box', i.e. a product which, although used for its intended purpose, cannot be observed or understood from the outside, particularly with regard to the implementation of the gap-filling mechanism.

51. Nevertheless, the applicant had attempted to acquire a contested embodiment via a distributor in order to obtain at least further clues, e.g. from the accompanying documentation. However, even this attempt had failed and the applicant had so far had no means of accessing the contested embodiment for analysis.

52. Nor had searches in publicly accessible sources, such as specialist publications, product documentation or other internet publications, regarding the contested embodiment been able to provide any further clarification regarding features 6.4b and 6.6.

53. The applicant therefore has no means of obtaining further evidence of patent infringement. According to the applicant's submission, however, the necessary findings of fact could easily be made by an expert with access to the respondents' premises in Berlin and Munich. The expert would thus be able to inspect the relevant devices and documents and document his findings.

54. The applicant argues that the order should be issued even without a prior hearing of the respondents. There is a risk that relevant documents and data may be removed or, at the very least, that locating them will be made significantly more difficult. This applies in particular given that the respondents, as closely affiliated sister companies, have a Swiss site in Bronschhofen (according to the extract from the commercial register, Annex NM AST 6) – as the registered office of the first respondent – to which the documents and data could be transferred or through which access to the documents from Berlin could be suppressed.

55. Carrying out the inspection in Switzerland would – if at all – only be possible with considerably greater effort, costs and legal uncertainty, and potentially with a weakened evidential position, as Switzerland is neither a member state of the UPC nor a member of the EU.

56. On 14 November 2025, the respondents filed a protective letter against the applicant and fiskaly Germany GmbH (PL_58/2025) with the Unified Patent Court in the event that the applicant applies for an order for provisional measures. In such an event, the respondents request that any such application be dismissed in its entirety. In the alternative, the respondents request to be heard prior to the ordering of provisional measures, that the panel be supplemented by a technically qualified judge, and that the enforcement of any such order be made conditional upon the provision of security. In support of their case, the respondents stated in their protective letter that the applicant and fiskaly Germany GmbH had so far failed to present any facts that could form the basis for an allegation of infringement in relation to the contested embodiment. Furthermore, the respondents had summarily examined the validity of the patent at issue. On the basis of this examination alone, the patent at issue was found to be invalid. Moreover, the applicant had failed to apply for provisional measures in good time. Finally, the order for provisional measures was also disproportionate.

THE APPLICANT'S APPLICATIONS:

57. The applicant requests that

I. that the following order be made without prior hearing of the respondents:

1. The preservation of evidence and inspection 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) that 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) comprises a

corresponding value of the key usage counter at the time of signing, 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 associated value of a last 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 recent 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 record (10) in response to the detection of a gap between the current value and the associated value of the last signed transaction 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 gap between the compared values, requests a retransmission 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 signature device (8) comprises a key usage counter which 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 signing, wherein the method comprises: 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 last recorded value, and transmitting the loaded at least one previously signed transaction record (23) to the registration device (6).

(Claim 1)

A computer program comprising instructions for causing a registration device (6), comprising a transaction memory (16) for storing signed transaction records (15), each signed transaction record (15) having an associated value of a key usage counter at the time of signing, to perform the following steps: accessing the transaction memory (16) and determining the associated value of the last 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 record (23) is loaded from the signature device (8) from a 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 program comprising instructions for causing a signature device (8), comprising a key usage counter, wherein the 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 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 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 most recently recorded value, and transmitting the loaded at least one previously signed transaction record
(23) to the registration device (6).

by

a) inspection of the German premises of the respondents

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

b) the preservation and disclosure of digital evidence relating to the Swissbit Cloud TSE 2 product, comprising in particular

- the certification documents, including the test report for procedure BSI K-TR-0612-2024 and, in particular, the documents mentioned in sections 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);

- source codes and software documentation, including flowcharts;

- Operational and installation manuals and development documentation, including requirements and specifications;

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

c) Seizure of copies or, alternatively, securing by making copies or photographs of technical documentation, internal development documents and manuals, and documents relating to the design, configuration, certification and deployment of the respondents' Swissbit Cloud-TSE 2;

d) Preparation and submission to the court of a written report (expert report) on the results of the measures set out in points 1(a) to (c) with regard to the realisation of the features of claims 6 and 7 to 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 European Patent EP 4 285 308,

within a period of one month following the implementation of the

measures set out in points 1(a) to (c).

2. to be appointed as a court-appointed expert for the implementation of the measures pursuant to point 1:

   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 discretion, call upon the IT forensic expert [redacted] FAST-DETECT GmbH, Inselkammerstr. 12, 82008 Unterhaching, or alternatively another IT specialist from FAST-DETECT GmbH, to act as an assistant.

3. In addition to the court-appointed expert and his assistant as per point 2, the following UPC representatives of the applicant may be present during the implementation of the measures referred to in paragraph 1(a) to (c):

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

   These UPC representatives are obliged to keep confidential from the applicant and its employees all facts that come to their knowledge during the execution of the entire order in relation to the business activities of the respondents. Representatives, employees or other staff of the applicant may not be present during the execution of the measures referred to in paragraph 1.

4. to order the respondents

   a) to grant the court-appointed expert, his assistant and the UPC representatives of the applicant listed in paragraph 3 access to the premises referred to in paragraph 1(a);

   b) to grant the court-appointed expert and his assistant access to the operating environment of the Swissbit Cloud-TSE 2 and, in particular, to enable the determination of 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; the court-appointed expert and his assistant are permitted to take photographs or film for documentation purposes, to take written notes and/or to use a dictaphone for their notes, and to make copies and printouts at the applicant’s expense;

   c) digital evidence, i.e. the certification documents (including the test report for procedure BSI-K-TR-0612-2024 and, in particular,

in particular the documents mentioned in Chapter 7.3/7.4 of the Conformity Report, including the Secure Platform Concept in version 1.0.2, and the Swissbit Cloud SMA ERS – Guidance Documentation in version 1.0.3); source codes and software documentation, including flowcharts, operating and installation manuals, as well as development documentation, including requirements and specifications; Configuration files, logs and operational data, including documentation on 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; the court-appointed expert and his assistant are permitted to make copies of the digital evidence.

d) to hand over to the court-appointed expert technical documentation, internal development documents, manuals and documents 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 to make copies of these documents;

e) to inform the expert of the exact location of the evidence referred to in points 1
b) and c), and to remove any obstacles to access, such as password protection for access to electronic documents, or to open any locked rooms or cupboards.

5. The court-appointed expert and his assistant are obliged to maintain confidentiality vis-à-vis third parties. The respondents are requested to comment on any confidentiality interests following the submission of the expert report. The applicant's UPC representatives referred to in paragraph 3 shall be given the opportunity to comment on the respondents' submissions. Thereafter, the court shall decide whether and to what extent the expert report and the preserved evidence are to be brought to the applicant's personal attention and whether the duty of confidentiality for the applicant's UPC representatives referred to in paragraph 3 is to be lifted.

6. The applicant is obliged to bear the costs of the inspection and the preservation of evidence, including the preparation of the detailed description. The applicant is required 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.

7. The order is to be served on the respondents in person at the premises referred to in paragraph 1(a) by one of the applicant's UPC representatives referred to in paragraph 3, 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 under point 1 are carried out. Should service on the first respondent at the premises referred to in point 1. a), the order shall be served in accordance with the general rules.

8. In the alternative, insofar as the court deems it necessary to require the provision of security for the costs of the proceedings and other expenses, as well as for any damages for which the applicant might be liable to the respondents, the applicant is to be ordered to provide security in the amount of EUR 10,000.00 or, in the further alternative, in such other amount as the court deems appropriate.

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

10. The measures for inspection and preservation of evidence shall be lifted on application by the respondents or shall otherwise lapse if the applicant has not, within a period of no more than 31 calendar days or 20 working days, whichever is the longer, after the expert report to be prepared in accordance with paragraph 1. d) has been disclosed or the court has decided by a final order not to grant access to that expert report, the applicant has brought an action against the respondents.

II. In the alternative – in the event that the court should consider measures without prior hearing of the respondents to be inappropriate – it is requested that the respondents be granted a period of no more than 10 working days to respond and that the measures requested under Section I. 1. be subsequently implemented in summary proceedings.

REASONS FOR THE ORDER:

58. The admissible application for an order for an inspection and preservation of evidence (R. 192, 199 RoP) is granted to the extent set out in the operative part.

I.

59. The Düsseldorf local division has jurisdiction pursuant to Art. 32(1)(c), 33(1)(b) and 60 of the UPC Agreement. The application has been filed in a permissible manner pursuant to R. 192 of the RoP. In particular, the applicant has also stated that it intends to bring an action on the merits against the respondents before the Düsseldorf local division.

II.

60. Furthermore, the applicant has credibly demonstrated that the patent in suit is likely to be infringed by the respondents (Article 60(1) of the UPC Agreement), although it is dependent on inspection and the preservation of evidence for a final assessment. In view of the circumstances of the case as described, it is possible that the product ‘Swissbit Cloud-TSE 2’ makes use of the technical teaching of the patent in question.

61. The applicant, who has standing as the proprietor of the patent in suit, has plausibly explained that, by issuing the certificate for the Cloud-TSE-2 software to the first respondent, the testing body and the BSI confirmed that the contested embodiment complies with all mandatory requirements of the BSI TR-03153 guideline. The court concurs with the applicant's conclusion that compliance with these directive requirements and the findings in the certification document allow clear inferences to be drawn regarding the system architecture of the contested embodiment and thus regarding the likelihood of an infringement of the patent in suit.

62. Furthermore, the applicant has plausibly explained that the certification of the contested embodiment by the BSI demonstrates the realisation of features 6.1–6.4a and 6.5 of the patent in suit in accordance with the feature breakdown in Annex NM AST 13; these are the following features:

62.1 A distributed system (1) for the secure registration of a sequence of transactions

62.2 wherein the distributed system (1) comprises a registration device (6) and a signature device (8)

62.3 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)

62.4 a wherein the signature device (8) comprises a key usage counter

62.5 wherein each signed transaction record (15) comprises an associated value of the key usage counter at the time of signing

63. With regard to the implementation of features 6.4b, 6.6a and 6.6b of the patent application in accordance with the list of features in Annex NM AST 13, namely

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 record (23) to the registration device (6)

in view of the expert opinion of [redacted] (Annex NM AST 20) that it is plausible that these features are likely to be realised, but that this can only be proven if evidence is preserved and an inspection is carried out as requested. This follows in particular from the nature of the contested embodiment, in which the processes relevant to the inspection take place within the software and – at least in part – in a special, secure infrastructure at the respondents' premises.

64. Furthermore, the court considers it probable, at least to the extent necessary for the order of the requested preservation of evidence and inspection, that

subclaims 7 to 9 and the co-dependent independent claims 1, 10 and 12 have also been infringed. In this regard, too, the court assumes that proof is only possible if preservation of evidence and inspection are carried out as requested, since, as mentioned, the processes relevant to the inspection take place within the software and – at least in part – within a special, secure infrastructure at the respondents' premises.

65. There are no objections to the filing of the application against both respondents in light of the division of labour between the respondents in the marketing, distribution and operation of the contested embodiment. Whilst the first respondent is primarily responsible for the marketing and distribution of the contested embodiment, the second respondent provides the technical infrastructure for at least parts of the operation of the contested embodiment. There is an interlocking and integrated cooperation between the respondents without any clear separation between them. There is therefore standing to be sued against both respondents, and the application is justified in respect of both respondents.

66. In so far as the respondents, in their protective letter primarily directed against the order for provisional measures, dispute an infringement of the patent in suit, this does not preclude the granting of the requested inspection and preservation of evidence order. In their protective letter, the respondents contest the infringement of the patent in suit solely on the grounds that neither the applicant nor fiskaly Germany GmbH has so far presented any specific explanations that could form the basis of the alleged infringement claim raised by the contested embodiment. On the contrary, the applicant and fiskaly Germany GmbH have requested that the respondents answer questions regarding the technical details of the contested embodiment. Accordingly, there has so far been no coherent and well-founded statement from the applicant as to the reasons why it considers that the contested embodiment falls within the scope of protection of the patent at issue. However, it is precisely these gaps in knowledge on the applicant's part that the present proceedings, aimed at inspection and preservation of evidence, are intended to fill. The statements in the protective letter therefore, at best, underpin the applicant's interest in the preservation of evidence. They do not constitute grounds for refraining from issuing an ex parte order solely on the basis of the existence of the protective letter.

67. A closer examination of the validity of the patent in question is not to be carried out within the framework of the present proceedings. The situation may be different only if there are clear indications to cast doubt on the validity of the patent in question, for example following a negative decision on validity (see UPC_CoA_327/2025, Order of 15 July 2025, para. 43 – Maguin v. Tiru). However, no such indications are present. In so far as the respondents appeal in their protective letter of 14 November 2025 to the fact that neither a preliminary objection against the grant of the patent in suit nor invalidity proceedings are currently pending, this is at most an indication of the validity of the patent in suit, but not against it.

68. Apart from that, the purpose of an application for inspection and preservation of evidence differs from that of an action on the merits (see UPC_CoA_239/2025, Order of 28 May 2025, para. 11 – Centripetal v. Palo Alto Networks). The purpose of the measures is to obtain evidence that can be used in proceedings on the merits (see Rules 196.2, 199.2 of the RoP), which also includes the use of the evidence

to decide whether proceedings on the merits or proceedings for provisional measures should be initiated at all (see UPC_CoA_177/2024, Order of 23 July 2024, Headnote 1 – Progress Maschinen & Automation v AWM; UPC_CFI_407/2025 (LD Brussels), Order of 12 November 2025, Headnote 4 – Organon Heist v Genentech). However, the proceedings for the preservation of evidence and inspection are not aimed at a final clarification of disputed issues between the parties (see also UPC_CFI_1325/2025 (LD Düsseldorf), Order of 23 January 2026, para. 17 – Van Loon Beheer v. Inverquark).

69. In light of this, the arguments set out in the protective letter regarding the validity of the patent in suit, in which a lack of inventive step and a lack of disclosure of the patent in suit are argued, should, at most, be examined only briefly. In the Court's view, following a cursory examination, the arguments set out therein do not, in any event, cast such doubt on the validity of the patent as to preclude the granting of the sought order for inspection and preservation of evidence.

III.

70. The applicant has further demonstrated that the application is urgent (Rule 194(2)(a) of the RoP). Furthermore, she has set out grounds for the issuance of an ex parte order (Rules 194(2)(b), (c) and 197 of the RoP).

1.

71. The inspection or preservation of evidence is urgent.

72. The applicant has plausibly demonstrated that the contested embodiment may make use of the technical teaching of patent claims 6 and the dependent claims 7–9 referring thereto, as well as the independent claims 1, 10 and 12. However, sufficient substantiation can only be provided by examining the documents and source codes located on the respondents' premises. According to the applicant's submission, it is not possible for the applicant to gain access to the documents necessary to substantiate the allegation of infringement other than through an inspection. The applicant has not only plausibly explained why it is not to be expected that a test purchase of the contested embodiment would contribute to clarifying the matter, since such a purchase, whilst enabling the use of the contested embodiment, would not allow any conclusions to be drawn regarding the specific design of the gap-filling mechanism. Rather, the applicant has nevertheless attempted to acquire a contested embodiment via a distributor in order to obtain further clues, for example from the documentation. However, such an attempt failed, which is why the applicant has no means of access outside of an inspection to analyse the contested embodiment. In particular, the applicant has plausibly explained that searches in publicly accessible sources, such as specialist publications, product documentation or other internet publications, could not have provided any further clarification regarding the implementation of features 6.4.b. and 6.6. in relation to the contested embodiment. An inspection of the respondents' premises therefore offers the applicant the opportunity to obtain further insights into the design of the contested embodiment through the detailed description to be prepared by an expert on this basis

and to gather evidence.

73. Even though, according to its own submission, the applicant became aware as early as 2025 that the first respondent was offering the contested embodiment in Germany, and consequently sent a letter of claim in September 2025, following which the parties entered into discussions regarding a possible infringement of the patent at issue by the contested embodiment, this does not preclude the sought order for preservation of evidence and inspection. As the Court of Appeal has already confirmed, a distinction must be drawn between the assessment of urgency in connection with an application for preservation of evidence (Rule 194.2(a) of the RoP) and the assessment of urgency in connection with an application for provisional measures (Rule 209.2(b) of the RoP). In exercising its discretion as to whether provisional measures should be ordered, the Court must also take into account any undue delay in applying for provisional measures (Rule 211.4 of the RoP). Neither the UPC Agreement nor the Rules of Procedure impose such a requirement when assessing whether an application for the preservation of evidence should be granted (UPC_CoA_2/2025, Order of 15 July 2025, Headnote 3 – Valinea v. Tiru). The absence of time-sensitive urgency could therefore be problematic at most if waiting would have led to the loss of the interest in preserving evidence. However, there is no evidence of this in the present case.

2.

74. The applicant has demonstrated, in a sufficient and comprehensible manner, grounds for the issuance of an ex parte order (para. 194.2 b), c), 197 RoP). Otherwise, there would be a demonstrable risk that evidence would be destroyed or would no longer be available for other reasons (para. 197.1 Alt. 2 RoP).

75. It is understandable and consistent with common experience that, if the respondents were notified in advance, there would be a risk that relevant documents and data would be removed or, at the very least, that locating them would be made significantly more difficult. This applies in particular given that the respondents, as closely affiliated sister companies, have, in addition to their German sites in Berlin and Munich, a Swiss site in Bronschhofen (as per the extract from the commercial register, Annex NM AST 6) – the registered office of the first respondent – to which the documents and data could be transferred or through which access to the documents from Germany could be suppressed.

IV.

76. In the context of the discretionary decision, the applicant’s interests prevail.

77. The applicant has plausibly demonstrated that the patent in question is likely to be infringed by the respondents and that she is reliant on the inspection and preservation of evidence for a definitive assessment. Conversely, there is no indication that the measures ordered would place a significant burden on the respondents. The applicant’s argument that the intended inspection of the technical systems is minimally invasive and will not fundamentally restrict the operation of the systems appears to the court

credible and reasonable. The confidentiality provisions included in the order take sufficient account of the applicants' confidentiality interests.

V.

78. The Applicant has paid court fee for the application for inspection and preservation of evidence, Rule 192.5 of the RoP.

VI.

79. In accordance with point I.1.a of the application, the inspection was to be ordered, and in accordance with points I.1.b–d of the application, the preservation of evidence was to be ordered with regard to the infringement of the patent in suit by the contested embodiment.

80. The inspection and the associated access to the respondents' two German sites pursuant to point I.1.a of the application serve, on the one hand, to inspect the operating environment of the contested embodiment, including the identification of specific software and hardware versions in use, and, on the other hand, to locate the analogue and digital evidence to be preserved. Both sites are certified, in accordance with the TÜV certification (Annex NM AST 25), to operate CSP-Ls; however, the exact internal distribution between the sites is as yet unknown. The application for an inspection at both sites is therefore justified.

81. In section I.1.b of the application, in accordance with Rule 196.1(d) of the RoP, the securing and disclosure of digital evidence is requested which enables proof of the realisation of the features of claims 6–9, 1, 10 and 12 of the patent application. These include, in particular, specific certification documents, but also the source code and more general technical documentation, as well as data that allows conclusions to be drawn about the operation of the components (configuration files, logs and operational data). The requested disclosure of the digital evidence, including all passwords and access data, is based on the fact that the mode of operation of the contested embodiment relevant to the patent infringement can practically only be established on the basis of internal documents and cannot be ascertained by external observation. The applicant's assertion that, without access to this data, the measure would be futile is credible. This applies mutatis mutandis to the seizure or, in the alternative, the securing of copies of the analogue evidence pursuant to point I.1.c of the application, based on Rule 196.1(c) of the RoP.

82. By preparing and submitting the written report in accordance with point I.1.d of the application, the applicant requests, in accordance with Rule 196.1(a) of the RoP, the preservation of evidence regarding the findings from the inspection and the examination of further evidence by the court-appointed expert. The written expert report serves to preserve the results of the inspection and necessary findings regarding the subject matter of the inspection.

83. The expert proposed in accordance with Section I.2 of the application is, as a patent attorney and trained specialist in information and communication technology – with technical expertise in the fields of information and communication technology, in particular wireless networks and data processing, control and regulation technology, microsystems technology and software – well-suited to assess the matter in dispute. He holds a degree in Electrical Engineering, Information Technology and Computer Engineering

(Exhibit NM AST 34). The court has no reservations about appointing the expert proposed by the applicant. The court further considers the applicant's submission to be credible, namely that there are no known circumstances precluding the appointment of the proposed expert and, in particular, that there is no known relationship between the proposed expert and the parties that would preclude such an appointment. The court also considers it reasonable that the expert proposed by the applicant should, as requested, be able to engage an IT forensic expert at their own discretion for the practical implementation of the measure.

84. The presence of as many as four named UPC representatives of the applicant, as requested under point I.3 of the application, albeit subject to a confidentiality order, is disproportionate. It is not apparent why the presence of one UPC representative each from the legal and patent fields (at each of the two locations of the inspection and preservation of evidence) should not be sufficient. The circle of those present was therefore to be restricted as set out in the order.

85. The obligations of the respondents sought in paragraph I.4 of the application set out the necessary details for the conduct of the inspection and preservation of evidence sought in accordance with paragraph I.1. The court accepts that it is necessary for the expert, his assistant and the representatives listed in section I.3 to be granted access (section I.4.a) and for the expert and his assistant to be granted access to the operating environment of the contested embodiment (section I.4.b). The same applies to the obligation to put the product into operation and to permit the taking of photographs or film footage and the making of notes.

86. In the court's view, the obligations sought under points I.4(c) to (e) of the application relate to detailed aspects necessary for the preservation of evidence, such as the provision and disclosure of digital documents, including the necessary passwords, the handover and authorisation of copies of analogue evidence, and the disclosure of the relevant storage locations.

87. Sections I.5 to I.7 of the applicant's application do not give rise to any concerns. Section I.5 seeks a standard confidentiality order and Section I.6 a standard obligation to bear costs and provide an advance. Section I.7 provides, in an appropriate manner, for service arrangements specific to the inspection.

88. To assist the expert and his assistant in carrying out the preservation of evidence and inspections, the court has made use of the option provided for in Rule 196(5) sentence 2 of the RoP to issue an order for assistance from bailiffs.

89. The confidentiality measures ordered in respect of the parties' legal representatives, the expert and the bailiff take account of the respondents' interests in confidentiality. The same applies to the procedure described following receipt of the expert's report.

90. Furthermore, it was ordered that the report to be prepared by the expert, as well as all other results of the measures to preserve evidence, may only be used in main proceedings against the first respondent and/or the second respondent

(R. 196.2 RoP).

91. The costs of the inspection and preservation of evidence to be carried out by the expert, including the detailed description to be prepared by the expert, are in any event to be borne by the applicant until further notice, as she is seeking the inspection and preservation of evidence. Insofar as the expert does not waive the payment of an advance for his costs, the applicant must pay the expert a reasonable advance, to be determined by the expert, prior to the commencement of the inspection.

92. The order, together with the documents specified therein, is to be served by the bailiff in cooperation with one of the applicant's representatives present during the inspection and preservation of evidence, in accordance with Rule 197.2 of the RoP.

VII.

93. The general threat of coercive measures included in the order gives the court the necessary flexibility to respond to any breaches of this order, taking into account the interests of both parties and the seriousness of the breach.

94. Pursuant to Rule 196.6 of the RoP, the court issues an order requiring the applicant to provide adequate security for the costs of the proceedings and any other costs incurred, being incurred or likely to be incurred by the defendant, which the applicant may be required to bear, as well as for any compensation the applicant may be required to pay for damage incurred or likely to be incurred by the defendant in the event of an order being made without prior hearing of the defendant, provided that no special circumstances preclude this. Even if, unlike in the case of an injunction, the respondents face at most only minor damage as a result of the inspection and preservation of evidence, because the respondents remain entitled to carry out all acts of use in respect of the contested embodiment and it may therefore be justified refrain from ordering the provision of security due to the particular urgency of the inspection and preservation of evidence (see UPC_CFI_260/2025 (LD), order of 26 March 2025, p. 9 et seq. – OTEC Präzisionsfinish v. STEROS; distinguishing from: UPC_CFI_177/2023 (LD), order of 22 June 2023 – myStromer v Revolt), the requirement of security in the case of an ex parte order constitutes the statutory norm. No grounds for refraining from requiring such security in the present case have been put forward or are apparent. In particular, on the basis of the applicant's submissions, it is not apparent that the minor delay in the inspection resulting from the provision of security would impair or jeopardise the applicant's interest in preserving evidence.

95. Insofar as the applicant refers, in paragraph 190 of her application, to a decision on costs pursuant to Rule 211.1(d) of the RoP, the provision in question relates to the order for provisional reimbursement of costs, for which a specific, quantified application is a prerequisite; such an application is lacking in this case. Furthermore, the provision in question relates to the order for provisional measures within the meaning of Part 3 (Rules 205 et seq.) of the Rules of Procedure. The provisions on the preservation of evidence and inspection do not provide for such provisional reimbursement of costs. Conversely, for an analogous application of Rule 211.1(d) of the RoP, there appears to be neither an unintended gap in the rules nor a common interest, without this requiring a final decision in the present case.

The provisions on the preservation of evidence and inspection do not provide for such provisional reimbursement of costs. Conversely, for an analogous application of Rule 211.1(d) of the RoP, there appears to be neither an unintended gap in the rules nor a common interest, without this requiring a final decision in the present case.

ORDER:

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

1. The applicant is permitted, 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) 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 last 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 recent 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 record (10) in response to the detection of a gap between the current value and the associated value of the last signed transaction 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 gap between the compared values, requests a retransmission 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 in 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 signature device (8) comprises a key usage counter which 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 signing, wherein the method comprises: 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 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 1)

A computer program comprising instructions for causing a registration device (6), which comprises a transaction memory (16) for storing signed transaction records (15), each signed transaction record (15) having an associated value of a key usage counter at the time of signing, to perform the following steps: accessing the transaction memory (16) and determining the associated value of the last 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 record (23) is loaded from the signature device (8) from a 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 program comprising

comprises instructions for causing a signature device (8) comprising a key usage counter, wherein the 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 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 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 most recently recorded value, and transmitting the loaded at least one previously signed transaction record (23) to the registration device (6).

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 sections
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 as well as 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 operating environment, including the handover or production of copies and 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 of a detailed description by an expert of the results of the measures referred to in point 1(a) with regard to the realisation of the features of claims 6, 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 the identification 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 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 use of the defendants' Swissbit Cloud-TSE 2 at the claimant's expense, in so far 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) to order the seizure of copies or photographs of technical documentation, internal development documents, manuals and documents 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 carrying out the inspection referred to in paragraph I.
1. a).

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

3. The following is appointed as the court-appointed expert to carry out the measures pursuant to 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 own discretion, call upon the IT forensic expert

[redacted] FAST-DETECT GmbH, Inselkammerstr. 12, 82008 Unterhaching, or alternatively 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 locations specified in paragraph 1.a) of the Order for the inspection are designated as further assistants.

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

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

Representative bodies, employees or other staff of the applicant may not be present during the performance of the measures referred to in paragraph 1.

6. The respondents are ordered to

a) to grant access to the court-appointed expert, his assistants referred to in paragraph 5 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 the determination of 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 in version 1.0.2, and the Swissbit Cloud SMA ERS – Guidance Documentation in version
1.0.3); source codes and software documentation, including flowcharts, operating and installation manuals, as well as development documentation, including requirements and specifications; to provide configuration files, logs and operational data, including documentation on 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 documents relating to the design, configuration, certification and deployment of the defendants' 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 from both third parties and the applicant any facts that come to their knowledge in the course of executing the entire order.

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 as '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 on the respondents in person 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 under 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 service on the first respondent at the premises specified in paragraph 1. a) not be possible, 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 for inspection and preservation of evidence shall be revoked on application by the respondents or shall otherwise lapse 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 prepared by the expert pursuant to paragraph 1(b)
aa) has been disclosed to the applicant or the court has decided by a final order 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 10,000.00 EUR.

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

Issued on 27 April 2026

NAMES AND SIGNATURES

Presiding Judge Thomas	Ronny Thomas signed Digitally by Ronny Thomas Date: 27 April 2026 10:17:59 +02:00
Legally qualified judge Adocker	Thomas Adocker Digitally signed by Thomas Adocker Date: 27 April 2026 10:06:19 +02:00
Legally qualified judge Dr Schumacher	Jule Kathrin Schumacher Digitally signed by Jule Kathrin Schumacher Date: 27 April 2026 10:24:04 +02:00
on behalf of the Deputy-Registrar	LAURA CHANTAL DANIEL Digitally signed by LAURA CHANTAL DANIEL Date: 27 April 2026 10:29:37 +02:00

INFORMATION ON REVIEW AND APPEAL:

The respondents may apply for a review of this order within 30 days of the measures being enforced (Art. 60(6) UPC Agreement, R. 197.3 RoP).

The party adversely affected may appeal against this order within 15 days of its service (Art. 73(2)(a) UPC Agreement, R. 220.1(c) RoP).