

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.,
Petitioner,

v.

TELEFONAKTIEBOLAGET LM ERICSSON,
Patent Owner.

IPR2024-00702
Patent 10,425,817 B2

Before NATHAN A. ENGELS, SHARON FENICK, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

FENICK, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background and Summary

On March 15, 2024, Lenovo (United States) Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) seeking *inter partes* review of claims 1–6 and 8–16 (“the challenged claims”) of U.S. Patent No. 10,425,817 B2 (Ex. 1001, “the ’817 Patent”). On June 28, 2024, Telefonaktiebolaget LM Ericsson (“Patent Owner”) filed a preliminary response to the Petition (Paper 6, “Prelim. Resp.”).

The Board has authority to determine whether to institute an *inter partes* review. See 35 U.S.C. § 314(b) (2018); 37 C.F.R. § 42.4(a). Under 35 U.S.C. § 314(a), an *inter partes* review may not be authorized unless the information in the Petition and any preliminary response “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” For the reasons that follow, we institute an *inter partes* review as to the challenged claims of the ’817 patent on all grounds of unpatentability presented.

B. Real Parties in Interest

Petitioner identifies Lenovo (United States) Inc., Lenovo Holding Company, Inc., Lenovo Group Limited, Motorola Mobility LLC, Motorola Mobility Holdings LLC, Motorola (Wuhan) Mobility Technologies Communication Co., Ltd., and Motorola (Beijing) Mobility Technologies Co., Ltd. as real parties in interest. Pet. 2. Patent Owner identifies Telefonaktiebolaget LM Ericsson and Ericsson Inc. as real parties in interest. Paper 4 (Patent Owner’s Mandatory Notices), 1.

C. Related Matters

Petitioner and Patent Owner each identifies the following pending proceedings as related matters:

Certain Mobile Phones, Components Thereof, and Products Containing Same, Inv. No. 337-TA-1375 (Oct. 11, 2023) (“the ITC proceeding”); and

Telefonaktiebolaget LM Ericsson v. Lenovo (US) Inc. et al., No. 5:23-cv-00569 (E.D.N.C. Oct. 11, 2023).

Pet. 2; Paper 4, 2.

D. The ’817 Patent

The ’817 patent is titled “Subscription Concealed Identifier” and issued on September 24, 2019 from an application claiming priority to a provisional application filed on July 25, 2017. Ex. 1001, codes (45), (54), (60).

The disclosure of the ’817 patent describes an authentication server in a home network of a user equipment (UE) used to obtain a subscription permanent identifier (SUPI) for a subscriber, for example in a 5G system. *Id.* code (57), 8:19–35. The SUPI may be or contain an IMSI (International Mobile Subscriber Identity). *Id.* at 1:22–24, 8:22–35. The SUPI may comprise a Mobile Subscription Identification Number (MSIN), a Mobile Country Code (MCC), and a Mobile Network Code (MNC). *Id.* at 2:24–26.

The UE may be, for example, mobile equipment, a smartphone, a personal computer, or a smart appliance. *Id.* at 6:22–25. The UE is connected to a home network via a serving network. *Id.* at 6:14–18, 6:36–39. The disclosure describes that the confidentiality of the long-term subscription identifier of the UE is important to maintain and that legacy

systems may expose this identifier in clear text over the air interface. *Id.* at 1:22–36.

The '817 patent describes that, in order to maintain the confidentiality of the UE's long-term subscription identifier, a home network public key may be used, with the UE encrypting its subscription identifier with the public key before transmitting it to the home network. *Id.* at 1:37–43, 7:15–26. Embodiments described in the '817 patent include a subscription concealed identifier (SUCI) that is a protected version of a SUPI, and includes a clear-text part and an encrypted part, as seen in Figure 3, reproduced immediately below. *Id.* at 8:36–40.

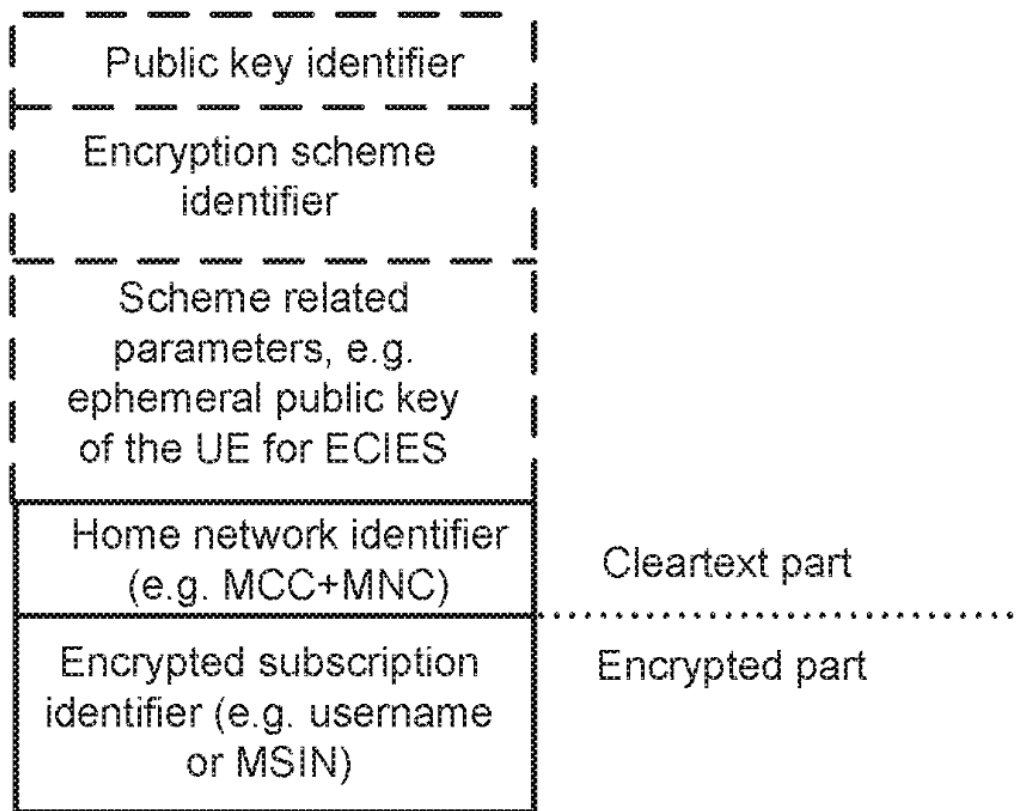


Fig. 3

Id. at 5:43–44. Figure 3 depicts five sections of a SUPI, with an indication that four parts (shown at the top of the figure) are present in clear-text (not

concealed or encrypted) and one part (depicted in the bottommost portion of the figure) is encrypted. *Id.*, Fig. 3, 8:59–61. As shown in Figure 3, the SUCI may include, in clear-text, a home network identifier, for example the MCC and MNC of a home network. *Id.* at 8:41–43. The clear-text part shown in Figure 3 also includes a public key identifier, encryption scheme identifier, and encryption-scheme related parameters useful for decrypting the encrypted part of the SUCI. *Id.* at 8:44–47. This may include an ephemeral public key of the UE or other parameters for use in the Elliptic Curve Integrated Encryption Scheme (ECIES) or another encryption scheme. *Id.* at 8:47–50.

The encryption may be a null encryption scheme, where the output of encryption is the same as the input to encryption, for example if the UE has not been provisioned with the public key of the home network. *Id.* at 9:10–13, 10:17–20, 15:7–11, 15:19–21.

The system may include an authentication server, which may be an AMF (Access and Mobility Management Function), SEAF (Security Anchor Function), or AUSF (Authentication Server Function) in a home network of a UE, which obtains the subscription identifier from a SUCI received by that authentication server. *Id.* at 6:42–44, 16:56–61, 19:6–28. The system may also include a de-concealing server, which may be a SIDF (Subscription Identifier De-concealing Function), which receives a SUCI from an authentication server, performs decryption, and provides a subscription identifier for a UE to the authentication server. *Id.* at 6:55–56, 11:11–18, 19:44–62. In one example, different SIDFs may exist that handle different encryption schemes, and the AUSF may determine an SIDF to use to handle a received SUCI. *Id.* at 10:45–64.

E. Illustrative Claim

Challenged claims 1, 9, 10, and 15 are the independent claims. Claim 1 is illustrative and is reproduced below with bracketed identifiers corresponding to those used in the Petition and with some spacing and indentation changes for readability.

1. [Preamble] A method performed by an authentication server in a home network of a user equipment (UE) for obtaining a subscription permanent identifier (SUPI), [1b] wherein the SUPI is a globally unique identifier allocated to a subscriber and the SUPI comprises a home network identifier identifying a home network of the subscriber and a subscription identifier identifying a subscription within the home network, [1c] the method comprising:

the authentication server receiving a subscription concealed identifier (SUCI) generated by the UE, [1d] wherein the SUCI comprises an encrypted part and a clear-text part, and wherein

- a) the encrypted part of the SUCI generated by the UE comprises the subscription identifier identifying the subscription within the home network, but the encrypted part of the SUCI generated by the UE does not include the home network identifier and
- b) the clear-text part of the SUCI generated by the UE comprises
 - i) the home network identifier
 - ii) an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI, and
 - iii) a public key identifier for a public key of the home network, but the clear-text part of the SUCI generated by the UE does not comprise the subscription identifier;

[1e] the authentication server determining a de-concealing server to use to decrypt the encrypted part of the SUCI;

[1f] the authentication server sending the SUCI to the de-concealing server; [1g] and

after the authentication server sends the SUCI to the de-concealing server, the authentication server receiving the SUPI in response.

Ex. 1001 20:63–21:26.

F. Evidence

Petitioner relies on the following patent evidence.

Name	Patent Document	Exhibit
Togawa et al.	US 8,005,219 B2	1006
Forsberg et al.	US 2013/0003971 A1	1005
Nair et al.	US 2018/0324585 A1	1004

Petitioner relies on the following non-patent literature evidence.

Name	Non-Patent Literature Title	Author	Exhibit
5G-Ensure D3.1	Deliverable D3.1 5G-PPP security enablers technical roadmap (early vision)	Jouni Hiltunen et al.	1010

Petitioner additionally relies on a declaration of Harry Bims, Ph.D., Ex. 1002. Patent Owner relies on a transcript of a deposition of Dr. Bims taken in the ITC proceedings. Ex. 2001.

G. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–6 and 8–16 would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §¹	Reference(s)/Basis
1–6 and 8–16	103	Nair, Forsberg
1–6 and 8–16	103	Nair, Forsberg, Togawa
8, 14	103	Nair, Forsberg, 5G-Ensure D3.1
8, 14	103	Nair, Forsberg, Togawa, 5G-Ensure D3.1

II. ANALYSIS

A. Legal Standards

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). This burden never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (citing *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in *inter partes* review).

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are “such that the subject matter as a whole would have been obvious at the time the

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, 125 Stat. 284 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the ’817 patent has an effective filing date after March 16, 2013, the AIA version of § 103 applies.

invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved based on underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). We analyze the asserted grounds with the principles stated above in mind.

B. Level of Ordinary Skill in the Art

Petitioner, citing Dr. Bims’s declaration, asserts that, “[a] person of ordinary skill in the art (“POSITA”) in the subject matter of the ’817 patent would have had a master’s degree in electrical engineering, computer engineering, or computer science, or equivalent and at least three years of experience in the field of telecommunications or wireless systems,” and that “[a]dditional education might compensate for less experience, and vice-versa.” Pet. 10–11 (citing Ex. 1002 ¶ 22).

Patent Owner asserts that one of ordinary skill would have had “a bachelor’s degree in electrical engineering, computer engineering, or computer science with (1) at least three years of experience in the field of telecommunications or wireless systems; and/or (2) an advanced degree in

electrical engineering, computer engineering, or computer science in the field of telecommunications or wireless systems.” Prelim. Resp. 16.

We do not discern a meaningful difference between the two parties proposals. Petitioner’s proposal appears consistent with the problems and solutions in the ’817 patent and prior art of record and is supported by expert testimony. We note, however, that the open-ended language “at least” expands the range of experience indefinitely with no upper bound. Upon this preliminary record and for the purposes of institution, we adopt Petitioner’s definition of the level of skill with the exception that we delete the words “at least.”

C. Claim Construction

Neither party makes a claim construction proposal or indicates that any claim requires construction. Pet. 11; *see generally* Prelim. Resp.

We note that an argument was raised that presents an implicit construction question regarding whether a flag which “only identifies if encryption [is] ‘on’ or ‘off’” (Prelim. Resp. 24) teaches or suggests “an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI” (as recited in limitation 1d of claim 1 and identically in claims 9, 10, and 15). We address that argument below, in Sections II.D.3.c.ii and iii of this Decision.

With that exception, we do not discern that any claim terms require construction at this point in the proceeding for the purpose of institution. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (only those terms that are in controversy need be construed, and only to the extent necessary to resolve the controversy) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

D. Obviousness over Nair and Forsberg

Petitioner asserts that the challenged claims are obvious over Nair in combination with Forsberg. Pet. 18–59. Patent Owner asserts that Nair is not prior art, that the proposed combination of Nair and Forsberg does not teach the subject matter of the claims, and that Nair teaches against the proposed combination with Forsberg. Prelim. Resp. 17–37.

1. Nair

Nair is a published application titled “Privacy Indicators for Controlling Authentication Requests,” and was published on November 8, 2018. Ex. 1004, codes (43), (54). Nair claims priority to Provisional Application No. 60/502,266 (Ex. 1008, “Nair Provisional”) filed on May 5, 2017. *Id.* at code (60).

Nair describes providing privacy features in communications systems, including by a home network operator providing its public key to all home network subscribers, in order to allow the subscribers to use that public key to encrypt their subscriber identity, e.g. the MSIN part of a subscriber IMSI. *Id.* at code (57), ¶ 35. The remainder of the IMSI, the MNC and MCC are not encrypted because they are needed by the serving network to route to the correct home network. *Id.* ¶ 35.

Figure 6 of Nair, reproduced below, depicts a message flow for a user equipment authentication procedure. *Id.* ¶¶ 24, 77.

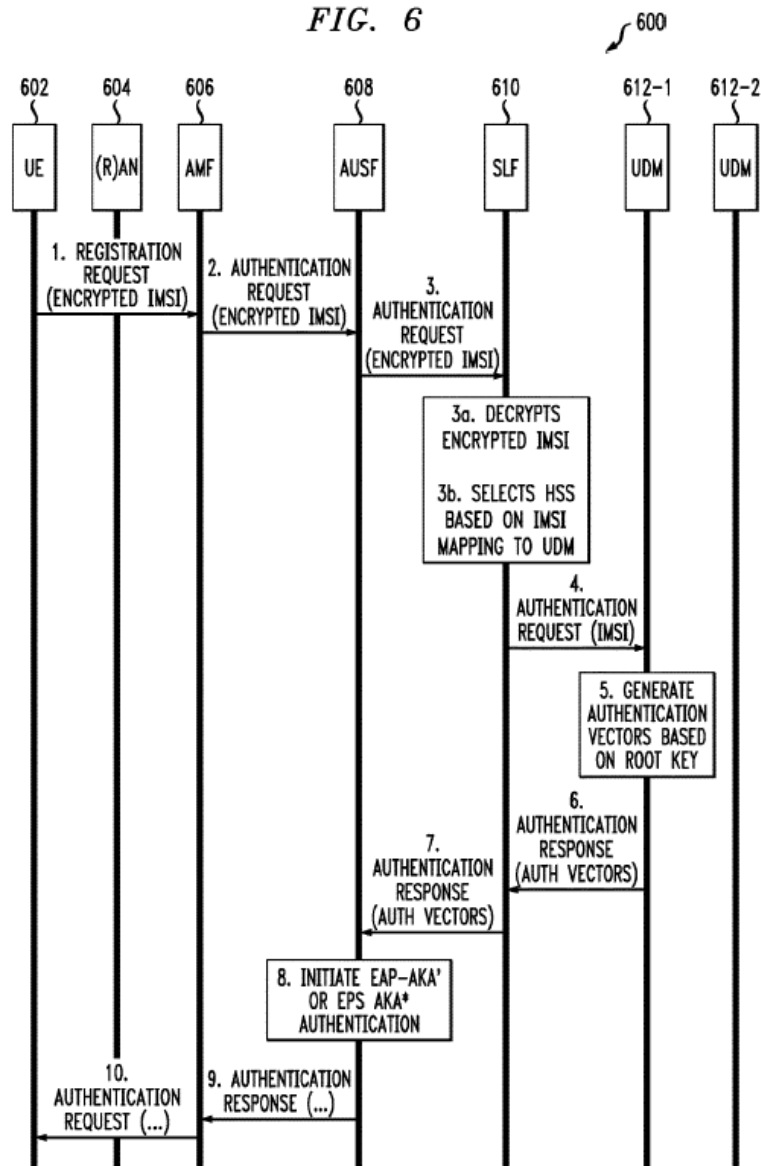


Figure 6 illustrates high-level UE authentication procedure 600 in ten steps, with messages passed between UE 602, Access and Mobility Management Function (AMF) 606, AUSF 608, Server Location Function (SLF) 610, and User Data Management (UDMs) 612-1 and 612-2. *Id.* ¶¶ 33, 36, 53, Fig. 6. UE 602 communicates with AMF 606 via radio access network (“(R)AN”) 604. *Id.* ¶ 44, Fig. 6.

Nair discloses that:

In step 1 of the high-level UE authentication procedure flow of FIG. 6, UE 602 sends a registration request (encrypted IMSI) through (R)AN 604 to AMF 606. . . In step 2, AMF 606 then sends an authentication request (encrypted IMSI) to AUSF 608. In step 3, AUSF 608 sends the authentication request (encrypted IMSI) to SLF 610. In step 3a, SLF 610 decrypts the encrypted IMSI. . . In step 3 b, SLF 610 selects an HSS [Home Subscriber Server] based on IMSI mapping to UDM. In step 4, SLF 610 sends the authentication request (IMSI) to the selected UDM, which as indicated in FIG. 6 is UDM 612-1. In step 5, UDM 612-1 generates authentication vectors (AVs) based on a root key. In step 6, UDM 612-1 sends an authentication response (AVs) to SLF 610, and in step 7, SLF 610 sends the authentication response (AVs) to AUSF 608. In step 8, AUSF 608 initiates EAP [Extensible Authentication Protocol] AKA' [Authentication and Key Agreement] authentication or EAP AKA* [Authentication and Key Agreement with increased home control] authentication. In step 9, AUSF 608 sends the authentication response to AMF 606. In step 10, AMF 606 sends an authentication request to UE 602 through (R)AN 604.

Id. ¶ 78; *see also id.* ¶¶ 33, 72, 73 (acronyms).

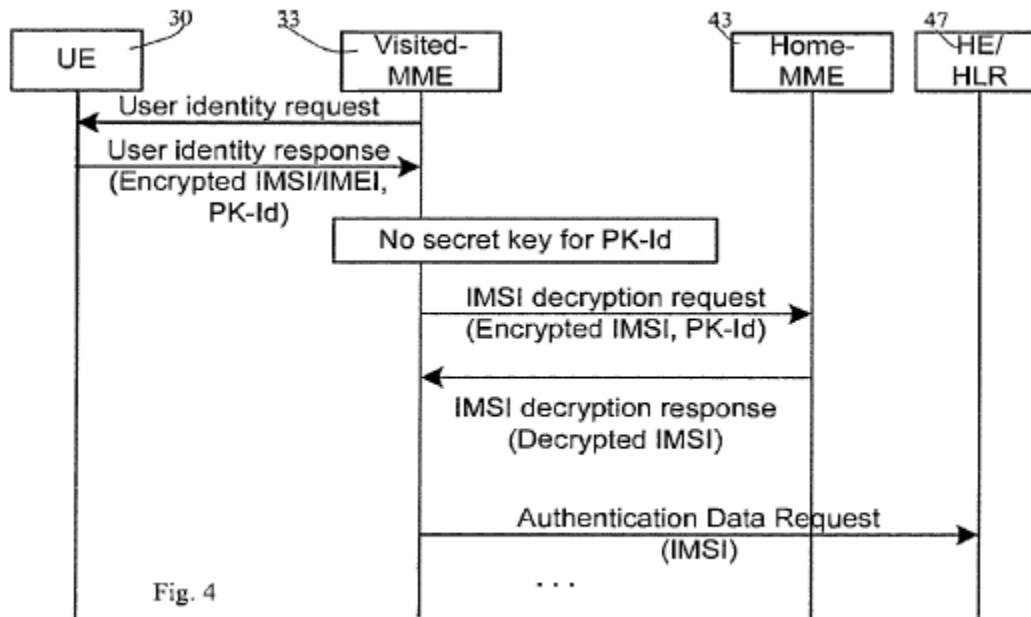
Nair describes that UE's request includes a flag that explicitly indicates whether the subscription identifier is privacy-protected. *Id.* ¶¶ 10, 41. Nair additionally describes an implicit privacy indicator that is conveyed, instead of through a flag, via the "fact that the message is encrypted with a particular encryption algorithm." *Id.* ¶ 42. Nair describes that the explicit flag may indicate whether the subscription identifier is encrypted or not encrypted ("null-encryption") but that having an indication would save processing time. *Id.* ¶¶ 42, 43.

2. Forsberg

Forsberg is a published application titled "Identifiers in a Communication System," and was published on January 3, 2013. Ex. 1005, codes (43), (54). Forsberg describes that individual subscribers in a

communications network may be provided with a permanent identifier such as an IMSI, which should be protected when communicated, e.g. over an air interface in a RAN. *Id.* ¶¶ 10–13.

Forsberg describes a UE communicating with a mobile management entity (MME) of a visited network, and how a MME of the home network may be consulted in order for the visited network’s MME to retrieve the IMSI for the UE in order to prepare an authentication data request. *Id.* ¶¶ 41, 44–46, Figs. 1, 2. Forsberg depicts the messaging procedure in its Figure 4, reproduced below. *Id.* ¶¶ 39, 48.



As shown in Figure 4, messages are passed between UE 30, Visited-MME 33, Home-MME 43, and home-environment home location register (HE/HLR) 47. *Id.* ¶¶ 48–54. First, Visited-MME 33 sends a message (Figure 4’s “User identity request”) to UE 30 to request the user identity. *Id.* ¶ 48. UE 30 responds by returning a message (Figure 4’s “User identity response (Encrypted IMSI/IMEI, PK-Id)”) including a partially-encrypted

IMSI, in which the MSIN is encrypted, to Visited-MME 33. *Id.* ¶ 49. Information regarding the public key identifiers may also be included. *Id.* If Visited-MME 33 does not have the information necessary to decrypt the encrypted portions of the IMSI (indicated in Figure 4 by “No secret key for PK-Id”), Visited-MME 33 contacts Home-MME 43 for decryption assistance (Figure 4’s “IMSI decryption request (Encrypted IMSI, PK-Id”). *Id.* ¶ 51. Visited-MME 33 may determine the correct Home-MME 43 using the MCC and MNC of the IMSI. *Id.* ¶ 53. Home-MME 43 can decrypt the MSIN of the IMSI and send it back to Visited-MME 33 (Figure 4’s “IMSI decryption response (Decrypted IMSI)”). *Id.* ¶ 54. Visited-MME 33 can then “continue the intended operation, for example by sending a request for authentication data in [Figure 4’s message ‘Authentication Data Request (IMSI)’] to an appropriate register maintaining subscriber data.” *Id.*

3. Analysis of Claim 1

a. Nair As Prior Art

Petitioner asserts that Nair is prior art to the ’817 patent because of the priority claim in Nair to the Nair Provisional. Pet. 4–5. Petitioner provides parallel citations to the Nair Provisional with many of its citations to Nair, which it argues demonstrate that the Nair Provisional describes the subject matter relied upon in the Petition. *Id.* at 5.

i. Nair Provisional’s Support for a Claim in Nair

Patent Owner argues that the Petition is deficient because it does not show that the disclosure in the Nair Provisional supports at least one claim in Nair, even though Nair is subject to the AIA and Patent Owner concedes that the Board’s precedential opinion in *Penumbra* concludes we do not need to make such a determination regarding support for at least one claim to reach a prior art determination under the AIA. Prelim. Resp. 23–24 n.6; *Penumbra*,

Inc. v. RapidPulse, Inc., IPR2021-01466, Paper 34 at 32 (PTAB Mar. 10, 2023) (precedential). Following that precedent, we decline to require a showing of support in the Nair Provisional for at least one claim in Nair and instead only require that the ministerial requirements for claiming priority were met. *See Penumbra*, Paper 34 at 32–33. Petitioner argues that the “ministerial requirements” described in *Penumbra* have been met. Pet. 4–5 (noting that Nair contains a priority claim to the Nair Provisional, was filed within 12 months of the Nair Provisional, and includes a common inventor). Patent Owner does not contest that these requirements have been met, and upon our examination, we agree that they appear to have been met. Ex. 1004, codes (22), (60), (72); Ex. 1008, 1, 4, 38. Thus, on the present record and for the purposes of institution, the disclosures of Nair are prior art, to the extent that the relied-upon disclosures are included in the Nair Provisional.

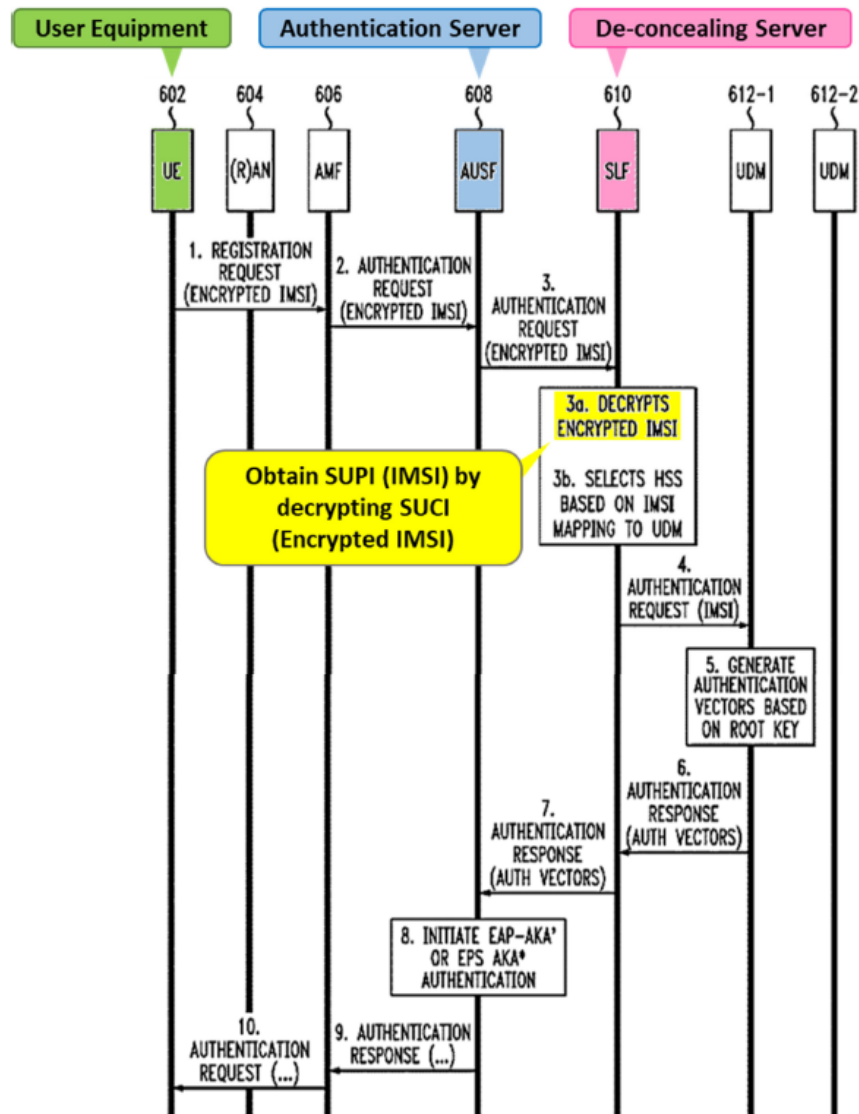
ii. Nair Provisional’s Date for Cited Portions of Nair

Patent Owner also argues that the Petition relies on material in Nair that was added after the filing of the Nair Provisional, and that this material cannot be properly relied on as prior art. Prelim. Resp. 19–23. We address these specific arguments regarding material Petitioner references from Nair (and the Nair Provisional) below, in our analysis with respect to the respective limitations of claim 1 these citations relate to.

b. Preamble² and Limitation 1b: “A method performed by an authentication server in a home network of a user equipment (UE) for obtaining a subscription permanent identifier (SUPI), [1b] wherein the SUPI is a globally unique identifier allocated to a subscriber and the SUPI comprises a home network identifier identifying a home network of the subscriber and a subscription identifier identifying a subscription within the home network,”

Petitioner argues that Nair’s AUSF teaches the authentication server of the preamble and that Nair’s IMSI teaches claim 1’s “SUPI.” Pet. 23–29. With reference to the latter contention, Petitioner points to the disclosures in the ’817 patent the SUPI “may be IMSI-based.” *Id.* at 23 n.1 (citing Ex. 1001, 8:20–24). Petitioner provides a version of Nair’s Figure 6, reproduced below, annotated with labels and coloring corresponding to recitations of the claim to illustrate its argument.

² We refer to claim 1 using Petitioner’s labels, but we do not make any determination regarding whether this portion is properly the entire preamble of claim 1, i.e., whether the portion of claim 1 designated by Petitioner as limitation 1b is not part of the preamble of claim 1. The parties do not present arguments regarding whether the preamble of claim 1 is limiting, and we do not provide a determination regarding this, as we determine that Petitioner’s assertions sufficiently show, for the purposes of institution, that Nair teaches the subject matter of each portion of the claim.



Pet. 24 (citing Ex. 1002 ¶ 56). In this annotated version of Figure 6 of Nair, AUSF 608 is annotated as “Authentication Server” and SLF 610 as “De-concealing Server.” *Id.* Petitioner argues that Nair discloses a method performed by its AUSF in which an authentication request is sent by the AUSF to an SLF and the SLF obtains the un-encrypted IMSI through decryption. Pet. 23–26 (citing Ex. 1004 ¶¶ 24, 33, 77, 78, Fig. 6; Ex. 1008, 4:18–22, 5:23–30, 13:17–18, Fig. 6; Ex. 1002 ¶¶ 55–61). Petitioner additionally argues that the IMSI in Nair teaches the claimed SUPI, as it is a

globally unique identifier assigned to a subscriber and comprises a mobile country code and a mobile network code. Pet. 26–29 (citing Ex. 1004 ¶¶ 32, 35, 38; Ex. 1008, 4:14–17, 4:23–31, 5:24–29; Ex. 1002 ¶¶ 62–65).

Patent Owner makes no arguments specific to this portion of the claim. While Patent Owner does not argue, with respect to this portion of the Petition, that the citations to Nair include paragraphs that were added subsequent to the filing of the Nair Provisional, we note that paragraph 78 of Nair, cited by Petitioner in this portion of the Petition, does not appear in the Nair Provisional. *Compare* Ex. 1004 ¶¶ 77–78, *with* Ex. 1008, 13:17–20. However, paragraph 78 of Nair does not appear to add materially to Figure 6 of Nair (which is similar in content to Figure 6 of the Nair Provisional) beyond a description of that figure. *Compare* Ex. 1004 ¶ 78, *with id.* Fig. 6; *compare* Ex. 1004, Fig. 6, *with* Ex. 1008, Fig. 6. Even so, we do not consider paragraph 78 in our determination with respect to this portion of claim 1.

On this record and for the purposes of institution, Petitioner sufficiently shows Nair teaches the (Petitioner-designated) preamble and limitation 1b of claim 1 in Nair’s disclosure of an AUSF that receives an authentication request including an encrypted IMSI and requests that an SLF decrypt the encrypted IMSI. Ex. 1004, Fig. 6; Ex. 1002 ¶¶ 55–59. Petitioner also sufficiently shows that Nair teaches that the IMSI includes an encrypted subscriber identity (e.g. MSIN), which is a subscription identifier, and MNC and MCC portions, which identify the correct home network. Ex. 1004 ¶¶ 32, 35, 38; Ex. 1002 ¶¶ 63–65. Therefore, on this record, and for the purposes of institution, we determine Petitioner has a reasonable likelihood of prevailing in showing that Nair teaches the subject matter of the (Petitioner-designated) preamble and limitation 1b of claim 1.

c. Limitations 1c and 1d: “[1c] the method comprising: the authentication server receiving a subscription concealed identifier (SUCI) generated by the UE [1d] wherein the SUCI comprises an encrypted part and a clear-text part, and wherein a) the encrypted part of the SUCI generated by the UE comprises the subscription identifier identifying the subscription within the home network, but the encrypted part of the SUCI generated by the UE does not include the home network identifier and b) the clear-text part of the SUCI generated by the UE comprises i) the home network identifier ii) an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI, and iii) a public key identifier for a public key of the home network, but the clear-text part of the SUCI generated by the UE does not comprise the subscription identifier”

i. Petitioner’s Contentions

Petitioner argues that Nair teaches limitation 1c of claim 1 in its disclosure that the UE sends a registration request with an encrypted IMSI to the AMF and that the AMF sends an authentication request with the encrypted IMSI, which is received by the AUSF. Pet. 29–30 (citing Ex. 1004 ¶¶ 24, 77–78, Fig. 6; Ex. 1008, 4:28–5:1, 13:17–20, Fig. 6; Ex. 1002 ¶¶ 66–67).

With respect to limitation 1d’s recitations that the SUCI comprises an encrypted part and a clear-text part, the encrypted part of the SUCI comprising the subscription identifier identifying the subscription within the home network, and the clear-text part of the SUCI comprising a home network identifier and not comprising a subscriber identifier, Petitioner argues that Nair teaches these portions of limitation 1d of claim 1 in its disclosure that the MSIN portion of the IMSI is encrypted, and that the MNC and MCC are needed by the serving network and would not be

encrypted. Pet. 31–33, 41 (citing Ex. 1004 ¶¶ 35, 38, 43, 73; Ex. 1008, 4:28–5:1, 5:24–26, 6:25–28; Ex. 1002 ¶¶ 70–72, 88).

With respect to limitation 1d’s recitation that “the clear-text part of the SUCI . . . comprises . . . ii) an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI,” Petitioner argues that Nair teaches an “identity privacy flag” or “privacy indicator” that indicates whether the MSIN is encrypted. Pet. 33–34 (citing Ex. 1004 ¶¶ 35, 41, 42; Ex. 1008, 6:17–18; Ex. 1002 ¶¶ 73–81). Petitioner further argues that Nair discloses both (1) an explicit privacy indicator (a flag or field) that informs the recipient that a particular encryption algorithm has been used, and (2) an implicit indication of encryption, whereby the recipient “is informed of the encryption scheme ‘by the fact that the message is encrypted with a particular algorithm.’” *Id.* at 34 (citing Ex. 1004 ¶¶ 42–43; Ex. 1002 ¶ 74).

In its arguments regarding a teaching of an explicit privacy indicator, Petitioner argues that Nair’s privacy flag indicates the particular encryption scheme because both the UE and SLF must know which scheme is required when encryption is indicated, citing Dr. Bims’s testimony that, because the UE and SLF must have this common understanding, one of ordinary skill would have understood Nair’s privacy indicator to indicate the encryption scheme. Pet. 34–35 (citing Ex. 1002 ¶ 76). Petitioner further notes that the ’817 patent describes a null-encryption scheme where “the input equals the output” and in which a field with one value that indicates null-encryption and another that indicates use of a non-null-encryption scheme. *Id.* at 36 (citing Ex. 1001, 3:27–28 (“the encryption scheme may be a null-encryption scheme”), 9:11–13, 10:17–20, 15:7–9 (describing using null-encryption where there is no privacy key), Figs. 4, 5, 15; Ex. 1002 ¶ 78). Petitioner

argues that Nair’s privacy indicator is similarly an identifier that indicates whether null-encryption or another scheme is used. *Id.* (citing Ex. 1002 ¶ 78).

With respect to limitation 1d’s recitation that “the clear-text part of the SUCI . . . comprises . . . iii) a public key identifier for a public key of the home network,” Petitioner asserts that this is taught by a combination of Nair and Forsberg. Pet. 18–22, 38–41. Petitioner argues that Nair and Forsberg relate to the same field of invention and are directed at the same problem (Pet. 18–19 (citing Ex. 1002 ¶ 46)); that Nair discloses multiple HSSs with different keys, and that one would have looked to Forsberg to support these multiple keys (*id.* at 19–20 (citing Ex. 1004 ¶¶ 35, 36, 37; Ex. 1002 ¶¶ 47–48)); and that the combination would be obvious in view of Nair’s teachings regarding multiple keys (*id.* at 20–21 (citing Ex. 1002 ¶¶ 47–48)). Petitioner further argues, with the support of Dr. Bims’s testimony, that one of ordinary skill would have recognized that Forsberg’s public key identifier could be used to improve Nair’s similar system and would have had a reasonable expectation of success in the combination. *Id.* at 21–22 (citing Ex. 1002 ¶ 53).

Petitioner argues that one of ordinary skill would have looked to Forsberg’s teaching of including a public key identifier with an encrypted MSIN and a clear-text MCC and MNC to augment Nair’s transmission of an IMSI including an encrypted MSIN. *Id.* at 38–41 (citing Ex. 1005 ¶¶ 49, 51, 55, 56, 58; Ex. 1002 ¶¶ 47, 49–50, 82–87).

ii. Patent Owner’s Contentions

Patent Owner argues that certain portions of Nair relied on by Petitioner are not supported by the Nair Provisional. Prelim. Resp. 19–22. Specifically, Patent Owner argues that the Nair Provisional only describes a

“privacy flag” that is used to determine whether a message is encrypted. Prelim. Resp. 20 (citing Ex. 1008, 6:17–30). Patent Owner argues and shows that paragraph 42 of Nair, relied upon by Petitioner for portions of its arguments relating to the recited “encryption scheme identifier” of claim 1, was not present in the Nair Provisional. *Id.* at 20–22. This paragraph, Patent Owner argues, is the one that introduces the concept of an “implicit” privacy indicator and names the “privacy flag” to be an “explicit” privacy indicator as described in the Petition. *Id.* at 20, 28–29.

Patent Owner additionally argues that Nair does not “expressly disclose” an encryption scheme identifier and that Nair’s privacy flag does not identify the encryption scheme that the UE uses to encrypt the subscription identifier in Nair. *Id.* at 24. Patent Owner asserts that Nair’s privacy indicator is “just a switch” and does not identify the encryption scheme used to encrypt the subscription identifier in its transmission. *Id.* at 25 (citing Ex. 1004 ¶ 43). Thus, Patent Owner argues, there is no need for Nair’s request to identify an encryption scheme or encryption keys. *Id.* at 25–26. Patent Owner argues that an “on”/ “off” indicator such as the one in Nair does not *identify* an encryption scheme. *Id.* at 26 (citing Ex. 1001, claim 10). Patent Owner argues that Nair “uses the privacy indicator as a switch to . . . attempt decryption using known decryption keys,” but that the indicator does not identify the encryption scheme actually used by the UE. *Id.* at 27 (citing Ex. 1004 ¶ 43), 29. Nair, according to Patent Owner, does not disclose the use of multiple encryption schemes and thus would not need to include an identifier of an encryption scheme. *Id.* at 29–32.

Patent Owner additionally presents deposition testimony from Dr. Bims from the ITC proceedings in which, Patent Owner contends, Dr. Bims admits that “Nair does not expressly disclose an encryption scheme

identifier.” *Id.* at 24, 26–27 (citing Ex. 2001, 123:12–14). Thus, Patent Owner argues, Dr. Bim’s declaration testimony here is called into question.

Patent Owner also argues that no motivation has been provided to add a field to the Nair transmission to provide public key information as in Forsberg. *Id.* at 34–36. Patent Owner contends that Petitioner did not adequately show how Nair would use the information regarding a public key identifier and that Nair and Forsberg have different architectures and the combination of these architectures was not adequately addressed in the Petition. *Id.* at 35–36.

iii. Analysis

On the present record and for the purpose of institution, we agree with Patent Owner that Petitioner cannot rely on paragraph 42 of Nair because it does not appear that any material in the Nair Provisional relates to these disclosures. Thus, we decline at this time to consider Petitioner’s argument that one of ordinary skill in the art would have found the Nair “implicit privacy indicator” described in that paragraph to teach or suggest an “encryption scheme identifier” as recited in claim limitation 1d.

However, as Patent Owner concedes, Nair does teach a privacy indicator that “conveys whether encryption is ‘on’ or ‘off’” and, on the present record, this appears to be supported by the portions of Nair cited by the Petitioner and the portions of the Nair Provisional that are identical to these portions. Prelim. Resp. 25; *see* Pet. 33–34 (citing Ex. 1004 ¶¶ 35 (corresponding to Ex. 1008, 4:28–5:6), 41 (corresponding to Ex. 1008, 6:17–18), 43 (corresponding to Ex. 1008, 6:19–30); Ex. 1008, 6:17–18, 9:23–24; Ex. 1002 ¶¶ 73, 78). Thus, we do consider Petitioner’s arguments that this privacy indicator as described in the Nair Provisional (later described in Nair as an “explicit” privacy indicator in contrast with the “implicit” indicator)

teaches or suggests the “encryption scheme identifier” of claim 1. We determine, for the purposes of institution and on this record, that it does.

While, as Patent Owner contends, on the present record Nair does not disclose that the “identity privacy flag” is more than an on or off indicator regarding encryption, on the current record, Dr. Bims’s testimony is uncontroverted that one of ordinary skill in the art would have understood that this flag would have identified an encryption scheme used to encrypt the subscription identifier, because the receiving entity (Nair’s SLF) would have understood from a value of the flag that the IMSI received was encrypted and what encryption scheme was used. Pet. 34–35 (citing Ex. 1002 ¶ 76). Additionally, we note Dr. Bims’s testimony discussing the “null-encryption scheme” disclosed in the ’817 patent, which explains that the privacy flag described in Nair and the Nair Provisional “indicates whether the null-encryption scheme or the other scheme is used” and thus identifies an encryption scheme. *Id.* at 6 (citing Ex. 1002 ¶ 78). At this preliminary stage, Dr. Bims’s alleged admission in the ITC proceedings regarding the “*express disclosure*” of Nair does not appear to contradict his testimony regarding what Nair *teaches or suggests*. See Ex. 2001, 123:12–14 (emphasis added).³

³ In any event, Dr. Bims has not yet been “subject to cross-examination about [the] prior statement,” so the statement has uncertain evidentiary value at this preliminary stage. See Fed. R. Evid. 801(d)(1) (“(d) A statement that meets the following conditions is not hearsay: (1) A Declarant-Witness’s Prior Statement. The declarant testifies and is subject to cross-examination about a prior statement, and the statement: (A) is inconsistent with the declarant’s testimony and was given under penalty of perjury at a trial, hearing, or other proceeding or in a deposition[.]” (bold omitted)).

To the extent that Patent Owner implies that a proper claim construction for “encryption scheme identifier” could not encompass a flag such as the one in Nair and the Nair Provisional, on the present record we do not see how the intrinsic evidence (including the intrinsic evidence discussed by Petitioner) or extrinsic evidence supports such a limitation on the proper construction of the relevant claim limitation; the parties are, of course welcome to address it in the proceeding as it continues.⁴ *See* Pet. 36 (citing Dr. Bims’s testimony regarding the disclosures of the ’817 patent).

We also find that, on the present record, Petitioner sufficiently shows a motivation for the proposed combination of Nair and Forsberg. Uncontroverted on the present record, Forsberg teaches that certain home networks utilize multiple public/private key pairs and describes using a public key in messages from a UE including encrypted subscriber information in order to allow decryption of the encrypted information. Pet. 15–16, 38–39. (citing Ex. 1005 ¶¶ 48–51, 53–55, Fig. 4). Patent Owner presents attorney argument that there is no motivation to add a public key identifier to Nair because, in Nair only one key is described and there is no disclosure in Nair of multiple keys. Prelim. Resp. 35. On the current record, Dr. Bims’s testimony that Nair teaches managing multiple key pairs to support multiple HSSs is uncontroverted. Ex. 1002 ¶ 47 (cited at Pet. 19–

⁴ We request that any claim construction arguments the parties rely upon appear in a clearly designated section of briefing and note that such arguments should “point out the specific portions of the specification, prosecution history, and relevant extrinsic evidence” to be considered, with explanations of the relevancy of that evidence to the arguments presented. *See* Patent Trial and Appeal Board Consolidated Trial Practice Guide, 84 Fed. Reg. 64,280, at 46, 49 (Nov. 2019) (available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>).

20). Additionally, even if Patent Owner is correct that Nair’s disclosures do not teach or suggest multiple key pairs, the record includes Dr. Bims’s testimony that the combination would be motivated in order to allow use of Nair’s teachings in networks that did use multiple keys, such as those disclosed in Forsberg. Ex. 1002 ¶¶ 47, 49–50, 87 (cited at Pet. 39–41). Lastly, we do not see, on the present record, that the architectures of Nair and Forsberg are different in a way which would require additional detail, as argued by Patent Owner, to be supplied to support Petitioner’s contentions regarding the combination. *See* Prelim. Resp. 35–36. As we here determine to institute, additional arguments and evidence regarding any deficiency can be raised in the proceeding.

For these reasons, on this record, and for the purposes of institution, we determine Petitioner has a reasonable likelihood of prevailing in showing that Nair and Forsberg teaches the subject matter of limitations 1c and 1d of claim 1.

d. Limitations 1e–1g: “[1e] the authentication server determining a de-concealing server to use to decrypt the encrypted part of the SUCI; [1f] the authentication server sending the SUCI to the de-concealing server; [1g] and after the authentication server sends the SUCI to the de-concealing server, the authentication server receiving the SUPI in response”

i. Petitioner’s Contentions

We focus on Petitioner’s contentions regarding Figure 6 of Nair.

Petitioner argues that Nair teaches the authentication server’s “determination” of limitation 1e and “sending” of limitation 1f in the AUSF which sends an authentication request to an SLF. Pet. 41, 43 (citing Ex. 1004 ¶ 78, Fig. 6; Ex. 1008, 5:9–10, 5:24–26, 13:18–20, Fig. 6; Ex. 1002 ¶¶ 92–93). Petitioner further argues that Nair discloses a cellular network

with multiple SLFs, and cites Dr. Bims’s testimony that one of ordinary skill in the art would have understood that the AUSF had to make a determination regarding which SLF to send the request to, or that having the AUSF make that determination would have been obvious. *Id.* at 41–42 (citing Ex. 1004 ¶¶ 57, 67, 85; Ex. 1008, 10:14–20; Ex. 1002 ¶¶ 89–90).

For limitation 1g, where the authentication server receives the SUPI in response to its transmission, Petitioner argues that the combination of Nair, which describes a response from the SLF (which decrypts the IMSI) including authentication vectors, and Forsberg, which describes the decrypting Home-MME sending a cleartext version of the IMSI to the Visited-MME, teaches or suggests this element. Pet. 21, 43–44 (citing Ex. 1004 ¶ 78, Fig. 6; Ex. 1008, 5:8–9, 9:17–20, Fig. 6; Ex. 1005, ¶¶ 47, 51, 54, Figs. 3, 4; Ex. 1002 ¶¶ 52, 95, 97). Petitioner argues that this is done in Forsberg to aid in authentication, and would have been used for the same result in the combination, with predictable results. *Id.* at 44.

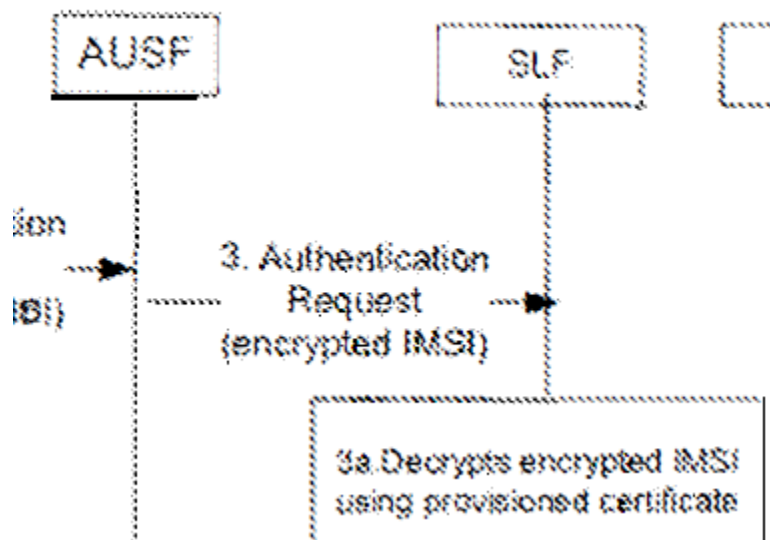
ii. Patent Owner’s Contentions

Patent Owner argues that certain portions of Nair relied upon by Petitioner are present in Nair and not in the Nair Provisional. Prelim. Resp. 22–23. Patent Owner notes that Petitioner cites paragraphs 47, 51, 54, 57, 67, 72–76, 78, and 85 with respect to these limitations. *Id.* Patent Owner argues that these disclosures are “lacking from the Nair Provisional, which only discloses the figures and one or two sentences for each figure that do not describe in detail the steps within the figures, including what parts of the alleged SUCI are decrypted and how.” *Id.* at 23.

iii. Analysis

With respect to these limitations, on the present record we determine that the portions of Nair relied upon are present in the Nair Provisional. For

example, paragraphs 57, 67, and 85 of Nair are listed by Petitioner as lacking in the Nair Provisional, but these paragraphs appear to correspond to 10:14–20, 12:24–28, and 14:14–22 of the Nair Provisional. Additionally, while paragraph 78 of Nair does not have a corresponding written disclosure in the Nair Provisional, the material relied upon from that paragraph appears to hew closely to the content present in Figure 6 of the Nair Provisional. For example, Petitioner’s quoted portion of paragraph 78 of Nair (“In step 3, AUSF 608 sends the authentication request (encrypted IMSI) to SLF 610. In step 3a, SLF 610 decrypts the encrypted IMSI.”) appears to correspond completely with the words and illustrated material in Figure 6 of the Nair Provisional, the relevant portion of which is reproduced immediately below.



Ex. 1008, Fig. 6.

On the present record, we do not find, for these limitations, use of material from Nair that should not have the benefit of the Nair Provisional’s date, and we reach the same conclusion regarding the sufficiency of Petitioner’s arguments even if we do not consider paragraph 78 of Nair but only the cited Figure 6.

On the present record, and for the purposes of institution, we determine the Nair and Forsberg combination sufficiently teaches or suggests an authentication server that determines a de-concealing server and sends the encrypted SUCI in Nair's AUSF and SLF sent the encrypted IMSI, and in the receipt in response by the AUSF of authentication vectors, and in Forsberg's teaching regarding including in such a response a cleartext version of the IMSI for use in a visited MME.

For these reasons, on this record, and for the purposes of institution, we determine Petitioner has a reasonable likelihood of prevailing in showing that Nair and Forsberg teach the subject matter of limitations 1e, 1f, and 1g of claim 1.

e. Conclusion

For the reasons above, we determine that, on the present record, Petitioner has shown that there is a reasonable likelihood that it will prevail in showing that the proposed combination of Nair and Forsberg teaches or suggests the subject matter of claim 1.

4. Claims 2–6 and 8–16

Because Petitioner demonstrates a reasonable likelihood of success in proving that at least one claim of the '817 patent is unpatentable, we institute on all of the challenged claims and on all grounds of unpatentability asserted for each claim in the Petition. See 37 C.F.R. § 42.108(a). Therefore, at this stage of the proceeding, it is not necessary for us to provide an assessment of every challenge raised by Petitioner. We have reviewed the challenges relating to Nair and Forsberg with respect to claims 2–6 and 8–16 and have no specific comments for the parties to consider in their briefing regarding these claims.

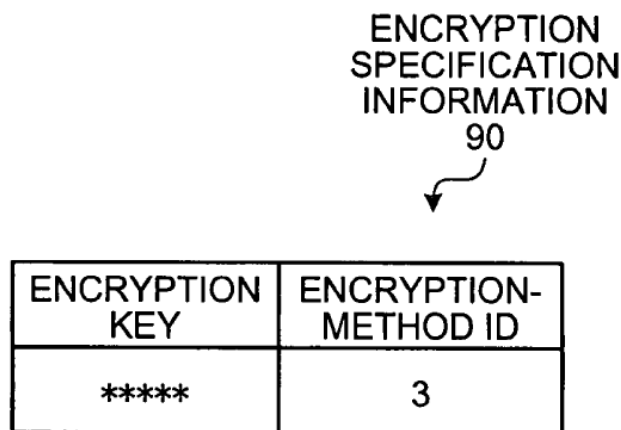
E. Additional Grounds

As mentioned, we institute on all challenged claims and all grounds asserted for each claim. However, we provide additional commentary on the grounds including Togawa.

1. Togawa

Togawa is titled “Data Decryption Apparatus and Data Encryption Apparatus,” and was issued on August 23, 2011. Ex. 1006, codes (45), (54). Togawa describes transmitting encryption specification information for use in decrypting transmitted encrypted data. *Id.* at 2:31–3:40. Togawa specifically describes embedding encryption information in a voice signal. *E.g., id.* at 9:15–18, 12:42–45, 23:11–14. Togawa presents in Figure 13, reproduced immediately below, an example of encryption specification information to be transmitted in a voice signal. *Id.* at 4:15–17, 23:17–19.

FIG. 13



Togawa discloses:

FIG. 13 is a diagram showing an example of encryption specification information 90 to be transmitted in the form of being embedded in a voice signal. As shown in FIG. 13, the encryption specification information 90 includes information on

an encryption key and an encryption-method ID. The encryption key is an encryption key for use in encryption of user data. The encryption-method ID is the identity that identifies an encryption method for use in encryption of the user data . . . Hence, the apparatuses that exchange data can be notified of the encryption specification appropriately with each other, which allows secure and efficient data exchange therebetween.

Id. at 23:17–25, 23:36–39.

2. Togawa in Combination with Nair and Forsberg

Among other arguments regarding the propriety of the combination of Togawa with Nair and Forsberg (Pet. 56–63) Petitioner argues that one of ordinary skill would have been motivated to use (and would have had a reasonable expectation of success in using) Togawa’s improvement of an encryption identifier that can identify more than one type of encryption scheme, integrating this with the authentication method of Nair. Pet. 60–61 (citing Ex. 1002 ¶ 136). Petitioner argues that the inclusion of an encryption identifier “frees the de-concealing server from first having to figure out which decryption [sic] scheme was used to encrypt the message and which decryption technique to apply to decrypt the message” and this would avoid wasted resources “deciphering” the encryption technique manually. *Id.* at 61–62 (citing Ex. 1002 ¶¶ 137–138). Petitioner asserts that motivation of one of ordinary skill in the art would have been to allow Nair’s de-concealing SLF to “manage the implementation of multiple non-null encryption methods.” *Id.* at 62 (citing Ex. 1002 ¶ 139). Petitioner argues that, even if Nair does not teach an “encryption scheme identifier” (e.g. as recited in limitation 1d of claim 1) that indicates which of a plurality of non-null-scheme encryption scheme is used, the combination of Nair and Forsberg would teach or suggest such an identifier. *Id.* at 63–65 (citing Ex. 1002 ¶ 141).

For grounds including Togawa, Patent Owner describes the Petition as “assum[ing] that Nair does not disclose an encryption scheme identifier,” and argues that the claims require an identification of “an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI.” Prelim. Resp. 33–34 (citing Ex. 1001, claim 10). Patent Owner argues that Togawa only teaches an encryption identifier of a scheme used to encrypt user data rather than to encrypt a subscription identifier. *Id.*

Without providing a complete analysis of the Togawa grounds, we note preliminarily that Patent Owner’s argument appears to be based on an assumption that no part of Nair’s “privacy indicator” is relied upon in these grounds, which appears to be incorrect. *See* Pet. 60–61 (describing “improv[ing] Nair’s privacy indicator with Togawa” to provide “a known improvement to an encryption identifier.”) Preliminarily, we do not find compelling the argument that a known improvement to an encryption scheme identifier would not have been considered by one of ordinary skill in the art because of a difference in the data being encrypted.

However, we note that Petitioner’s argument appears to rely on an assumption that one of ordinary skill in the art would have seen in Nair an issue with “deciphering the encryption technique manually.” Pet. 61–62 (citing Ex. 1002 ¶¶ 137–138). Preliminarily, we note that this argument appears susceptible to Patent Owner’s contention that “[t]here is no disclosure of supporting multiple encryption schemes in Nair.” Prelim. Resp. 26 (discussing a ground not including Togawa); *see* Ex. 1002 ¶ 76 (“Nair’s privacy indicator indicates the particular encryption scheme since both Nair’s UE and SLF must know which encryption scheme is required when the privacy indicator is flagged.”)

We do not need to, and do not, reach a determination regarding whether Petitioner has sufficiently shown a likelihood of succeeding in the challenges involving Togawa. Our discussion above is for the benefit of the parties as we institute on all grounds, and is preliminary and based on the limited record before us.

III. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that *inter partes* review of all challenged claims of U.S. Patent No. 10,425,817 B2 is *instituted* with respect to all grounds of unpatentability set forth in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is given of the institution of a trial commencing on the entry date of this Decision.

IPR2024-00702
Patent 10,425,817 B2

For PETITIONER:

Robert Appleby
W. Baker
robert.appleby@kirkland.com
todd.baker@kirkland.com

For PATENT OWNER:

Scott Hejny
Christian Hurt
Ericsson_Lenovo_IPRs@mckoolsmith.com
shejny@mckoolsmith.com
churt@mckoolsmith.com