

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.
Petitioner

v.

TELEFONAKTIEBOLAGET LM ERICSSON,
Patent Owner

Case No. IPR2024-00702
Patent No. 10,425,817

PATENT OWNER PRELIMINARY RESPONSE

Mail Stop “PATENT BOARD”
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND	2
A.	Technology	2
B.	The '817 Patent	4
C.	Petitioner's Prior Art References	8
1)	Nair.....	8
2)	Forsberg	11
3)	Togawa.....	13
4)	5G-Ensure Deliverable D3.1, "5G-PPP security enablers technical roadmap"	14
D.	Person of Ordinary Skill in the Art (POSITA)	16
E.	Related Proceedings	16
III.	THE BOARD SHOULD NOT INSTITUTE <i>INTER PARTES</i> REVIEW	17
A.	The Petition Fails to Establish a Reasonable Likelihood That Any Challenged Claim is Unpatentable.....	17
1)	The Petition Fails to Show That Nair is Prior Art	17
2)	Nair Fails to Teach the Claimed "Encryption Scheme Identifier," As Dr. Bims Admitted.....	24
3)	Togawa Fails to Disclose the Claimed Encryption-Scheme Identifier	33
4)	The Petition Fails to Show Obviousness	34
IV.	CONCLUSION.....	37

TABLE OF AUTHORITES

	Page(s)
CASES	
<i>Dynamic Drinkware, LLC v. National Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	23, 24
<i>Modine Mfg. Co. v. U.S. Int'l Trade Comm'n</i> , 75 F.3d 1545 (Fed. Cir. 1996)	31
<i>Paice LLC v. Ford Motor Co.</i> , 881 F.3d 894 (Fed. Cir. 2018)	31
<i>Penumbra, Inc. v. RapidPulse, Inc.</i> , IPR2021-01466, Paper No. 34, 32 (P.T.A.B. Mar. 10, 2023)	19, 24
<i>PersonalWeb Techs., LLC v. Apple, Inc.</i> , 917 F.3d 1376 (Fed. Cir. 2019)	27
<i>Telefonaktiebolaget LM Ericsson v. Lenovo (US) Inc.</i> , 5:23-CV-00569 (E.D.N.C. Oct. 11, 2023)	16
STATUTES	
35 U.S.C. § 102 (a)(2)	23
35 U.S.C. § 102(a)(1)	23
35 U.S.C. § 103	23

LIST OF EXHIBITS

Ex. Number	Title
2001	Excerpts of the May 31, 2024 Deposition Transcript of Harry V. Bims, Ph.D.
2002	Security in 5G Networks – How 5G networks help Mitigate Location Tracking Vulnerability
2003	3GPP TSG-SA WG3 Meeting #88 Tdoc S3-172106
2004	U.S. Provisional App. No. 62/536,632

I. INTRODUCTION

Patent Owner Telefonaktiebolaget LM Ericsson (“Ericsson” or “Patent Owner”) respectfully requests that the Board deny institution of the Petition. The inventions in the ’817 Patent spring from Ericsson’s inventive contributions to fifth-generation cellular technology (known as “5G”). These inventions were new, and the Petition does not assert otherwise. The Petition instead contends that the ’817 Patent claims would have been obvious through a mix-and-match of unrelated references. The Petition, however, fails to show obviousness, and the Board can deny institution for three independent reasons.

First, the Petition fails to show that the teachings of its primary reference (Nair) are prior art to the ’817 Patent. Nair is a published patent application whose filing date post-dates the unchallenged priority date of the ’817 Patent. To get around that problem, the Petition relies on the filing date of Nair’s provisional patent application. But the provisional application does not contain the subject matter from Nair that the Petition relies on for key claim elements: the Petition relies on new matter added to Nair after the ’817 Patent’s priority date.

Second, the Petition fails to show that the references disclose the encryption-scheme-identifier element present in each Challenged Claim: “an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI.” Petitioner’s references either indicate whether

or not encryption is used (Nair) or teach encrypting data in voice signals, not subscription identifiers (Togawa). Those are not the claimed encryption-scheme identifier. And Petitioner's expert recently admitted that Nair does not expressly disclose this claim element (and the Petition does not allege inherency).¹

Third, the Petition fails to show obviousness. Nair teaches away from the combinations the Petition proposes, a fact that the Petition does not address. Nair is a simple system that indicates if a message is encrypted or not and then decrypts the message using a known key—it has no need or ability to support multiple encryption schemes or include key identifiers or encryption methodologies in its message. And there is no evidence that Nair's system could have been modified in the manner the Petition proposes and still work.

For these reasons, and those below, Patent Owner respectfully requests that the Board deny institution.

II. BACKGROUND

A. Technology

The '817 Patent involves techniques to securely communicate subscriber

¹ Ex-2001, 123:12–14. Petitioner's expert also admitted that Forsberg does not expressly disclose an encryption-scheme identifier, and the Petition does not allege that Forsberg discloses that limitation. *Id.*, 123:15–17.

identifiers, specifically in next-generation cellular systems (such as 5G). Before the Patent, cellular systems lacked adequate privacy and security protections for subscriber information. Ex-1001, 1:24–36. A network operator, for example, may assign a subscriber a long-term identifier, such as an IMSI (the acronym for “International Mobile Subscriber Identity”). *E.g., id.*, 1:22–35. The subscriber’s device may need to send the long-term identifier over the air in a wireless network (*e.g.*, to identify the subscriber to the network operator). *Id.* This transmission posed a security risk because earlier cellular systems exposed “the long-term subscription identifier in clear text over the air interface,” *i.e.*, without encryption. *Id.*

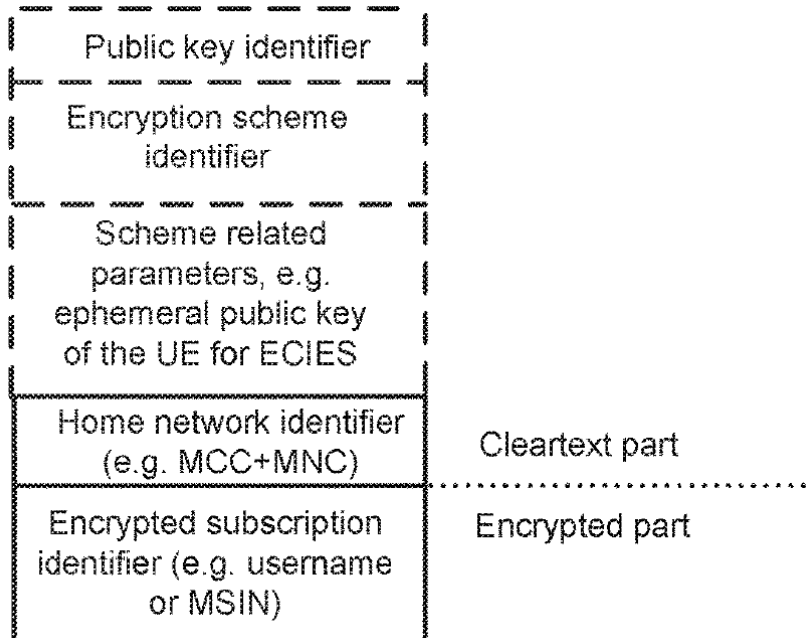
Conventional systems addressed security by transmitting short-term identifiers that would change periodically instead of the long-term identifier. Ex-1001, 1:24–31 (describing examples in 4G/LTE systems such as “GUTI (Globally Unique Temporary ID) and C-RNTI (Cell-Radio Network Temporary Identifier)”). These legacy mechanisms, however, could still expose long-term subscription identifiers in clear-text form if requested: “For example, so-called ‘IMSI catchers’ could ask the long-term identifier from the UE [the “User Equipment”], *e.g.*, using identifier request/response messages.” *Id.*, 1:31–36.

Exposing the long-term identifier was a security vulnerability in 3G and 4G systems that remained unsolved. Those generations of networks did not “enforce any encryption on this information transmitted during this process, giving malicious

actors an easy way to intercept the information.” Ex-2002, 1. “The most troubling consequence” of the security vulnerability, researchers concluded, “is that it can allow an adversary to track the device across the network[.]” *Id.* This danger highlighted “the need for a new approach for 5G networks” when it came to security. *Id.*, 7. The ’817 Patent, which was incorporated into the 5G standards, provides a solution to this security problem.

B. The ’817 Patent

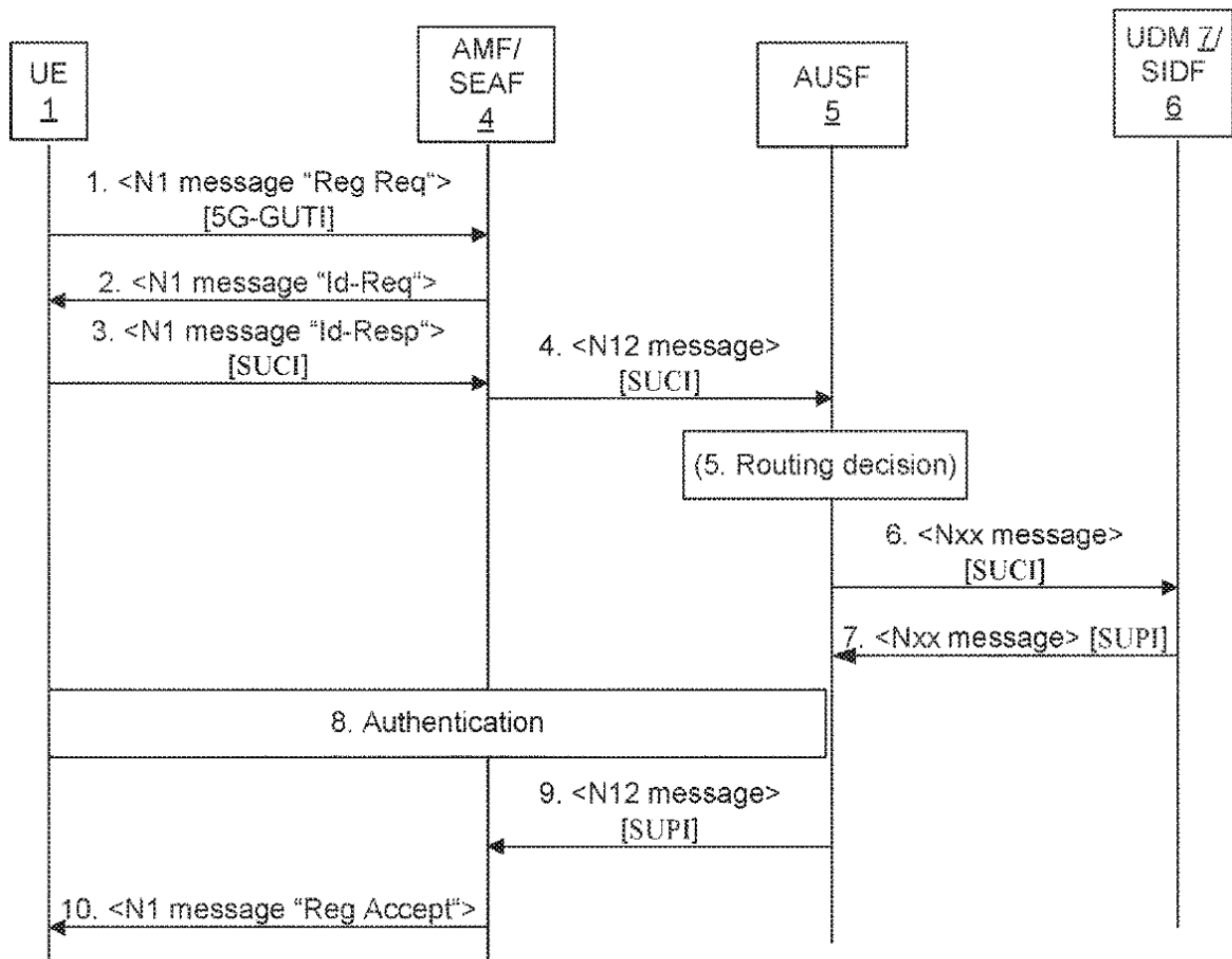
The Patent describes a way to conceal the subscription permanent identifier (called a “SUPI”) via a subscription concealed identifier (called a “SUCI”). Figure 3 of the ’817 Patent depicts an example SUCI.



The SUCI shown above includes two parts: a clear-text part (which includes a home network identifier and other data fields), shown in the top part of the Figure;

and an encrypted part (which includes the encrypted SUPI), shown in the bottom part of the Figure. Ex-1001, 8:41-42. Before the Patent, the term “SUCI” was not used in the art and the concept did not exist.

The ’817 Patent describes that a user equipment (known as a “UE”) generates the SUCI. Ex-1001, 8:62–63. The UE then transmits the SUCI to a mobile network for authentication. *Id.*, 10:25–11:36. Figure 6 depicts this process.



As Figure 6 shows, the UE first sends a registration request to the Authentication and Mobility Management Function (“AMF”) and Security Anchor

Function (“SEAF”) (step 1). Ex-1001, 10:38–43. If the AMF/SEAF fails to recognize the UE, the AMF/SEAF responds with an identifier request (step 2). *Id.*, 10:38–43. The UE “responds to the identifier request message with an identifier response message comprising a SUCI” (step 3), which is delivered to the Authentication Server Function (“AUSF”) on the UE’s home network (step 4) for authentication. *Id.*

The AUSF receives the SUCI and then uses information encoded in the SUCI to determine which Subscription Identifier De-concealing Functions (“SIDFs”) to use to decrypt at least part of the SUCI (step 5). Ex-1001, 10:48–50. For example, the AUSF may use the public-key identifier carried in the SUCI to identify the correct SIDF. *Id.*, 10:50–52. The AUSF then sends the SUCI to the selected SIDF (step 6). *Id.*, 11:11–12. The SIDF decrypts the SUCI to obtain the corresponding SUPI and then returns the SUPI to the AUSF (step 7). *Id.*, 11:17–18. The AUSF and the UE exchange authentication messages (step 8) and the. *Id.*, 11:21–23. The AUSF then returns the SUPI to the AMF/SEAF (step 9). *Id.*, 11:21–23, 11:32–34. Lastly, the AMF/SEAF accepts the registration of the UE and sends a registration acceptance message to the UE (step 10). *Id.*, 11:34–36.

Claim 10 of the ’817 Patent recites a method for concealing the subscription identifier and lists out how the SUCI is generated:

A method performed by a user equipment (UE) for concealing a subscription permanent identifier (SUPI) , 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, the method comprising:

the UE generating a subscription concealed identifier (SUCI) which comprises an encrypted part and a clear-text part, wherein a) the encrypted part of the SUCI generated by the UE comprises the subscription identifier identifying the subscription within a 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; and

the UE transmitting the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the encrypted part.

The '817 Patent claims priority to U.S. Provisional Patent Application No. 62/536,632, filed on July 25, 2017. *Id.*, (60). The Petition does not dispute the priority date of the '817 Patent. *See, e.g.*, Ex-1002, ¶ 20 (asserting date of invention is July 27, 2017 based on the filing date of the provisional application). Petitioner's expert likewise admitted during parallel proceedings in the International Trade Commission ("ITC") that he was "not challenging the priority date of the '817 Patent as July 25, 2017." Ex-2001, 114:25–115:3.

Ericsson developed the inventions reflected in the '817 Patent as part of its involvement in developing 5G. During the development of 5G, "[o]ne of the most pressing privacy concerns" related to the "untraceability of IMSI or SUPI." Ex2003,

1. Securing that information was “arguably one of the major privacy enhancements in 5G compared to LTE [also known as 4G].” *Id.* Ericsson disclosed its inventions reflected in the ’817 Patent to the 5G standards bodies (such as the Third Generation Partnership Project, known as “3GPP”), who adopted Ericsson’s invention into the 5G standard. Researchers have lauded the ’817 Patent’s SUCI-based approach as a “step in the right direction” to combatting the security vulnerabilities from 3G and 4G and providing “excellent protection” of subscriber information. Ex-2002, 7.

C. Petitioner’s Prior Art References

Petitioner relies on four references: Nair, Forsberg, Togawa, and 5G-Ensure. This section provides a brief summary of each reference.

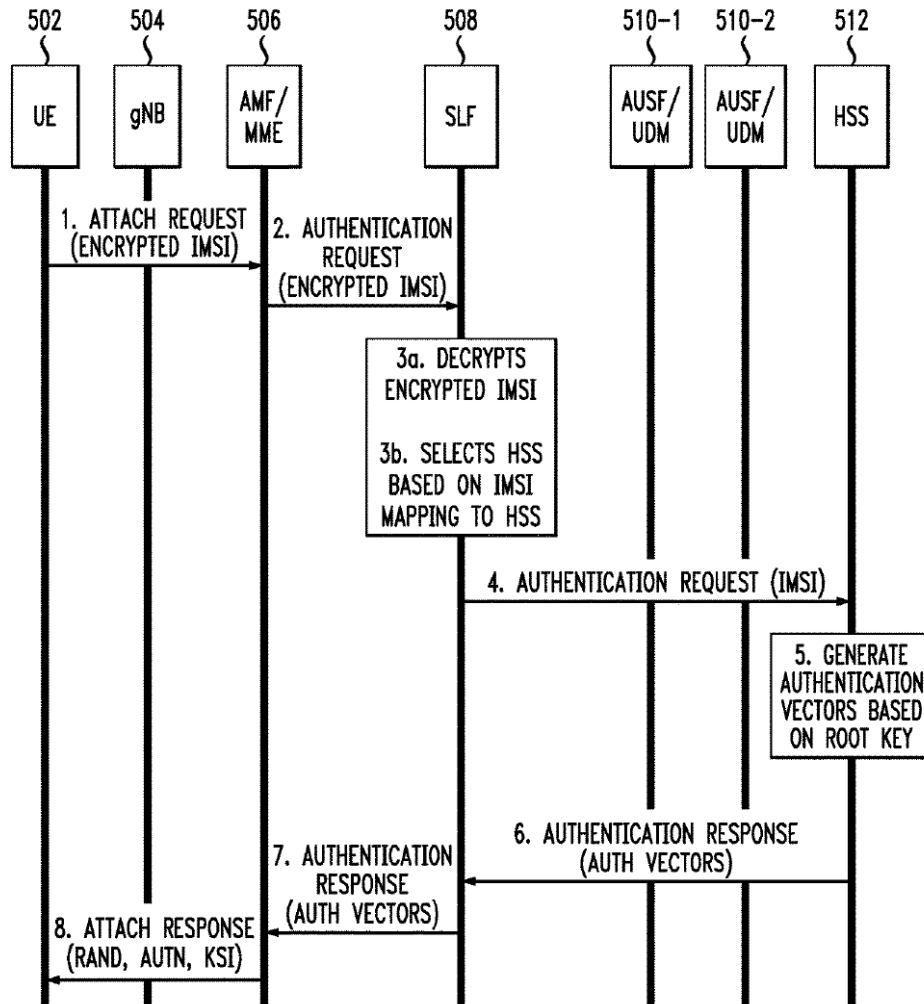
1) Nair

Petitioner primarily relies on U.S. Pat. App. Pub. No. 2018/0324585 (“Nair”). Ex-1004.² Nair provides for a privacy indicator for controlling authentication requests. *Id.*, (54). Figure 5 shows one embodiment of Nair’s system. *Id.*, Fig. 5, [0074]–[0076].

² The Petition fails to show that Nair’s teachings on which the Petition relies are prior art to the ’817 Patent, as detailed below.

FIG. 5

500



As Figure 5 depicts, the process starts with a UE sending an “attach request” that includes an encrypted IMSI to a device called an Access and Mobility Management Function / Mobile Management Entity (or “AMF/MME”). Ex-1004, Fig. 5, [0074]–[0076]. An “attach request” refers to a request by the UE to “attach” to a particular network, such as a 5G network. *Id.*, [0048], [0054],

In the next step, the AMF/MME sends an authentication request (which

contains the encrypted ISMI) to a Server Location Function (called an “SLF”). Ex-1004, Fig. 5, [0074]–[0076]. The SLF then performs two steps. It first decrypts the encrypted ISMI (at step 3a). *Id.*, Fig. 5, [0074]–[0076]. This yields the unencrypted ISMI. *Id.* Based on that ISMI, the SLF determines the HSS (the “Home Subscriber Server”) for that subscriber, *i.e.*, based on the subscriber’s home network. *Id.* The SLF then sends the unencrypted ISMI to the HSS (through an AUSF/UDM, which refers to an “Authentication and Security Function” / “User Data Management”). *Id.* The HSS then generates authentication vectors and sends an authentication response that ultimately results in the UE receiving an attach response. *Id.*

Nair discloses that the “attach request” may include “one or more privacy indicators comprising a flag indicating whether the subscription identifier in the attach request is privacy-protected.” Ex-1004, [0010], [0014]; *see also id.*, [0041] (“[T]he 5G UE, if it wants to protect its privacy, adds an identity privacy flag (*i.e.*, privacy indicator) to indicate that the MSIN is provided in encrypted form.”).

Nair explains that the privacy indicator acts as a switch to save a processing step (*i.e.*, the “first attempt” to resolve a request that is encrypted). Ex-1004, [0043].

It could be suggested that the HSS or SLF, even without this privacy indicator, will figure out after the first attempt to solve the request and, if encrypted, to attempt the decryption. But one key reason to have such an indication specified is that this saves processing time and fewer resources are needed. Thus, in this first illustrative embodiment, the SLF can make the decision on the processing by looking at this flag. If not set, the SLF will

assume the provided IMSI is unencrypted If the flag is set, the SLF will recognize that the provided IMSI is encrypted and use the network private key to decrypt the MSIN part to form the real unencrypted IMSI If no SLF is used, the same principle can be used by the HSS / UDM. That is, HSS / UDM has to check whether the 5G UE has set a flag and then decide whether decryption is needed.

Nair thus teaches that its privacy indicators indicate whether encryption is used; they do not identify an encryption scheme. Petitioner’s expert (Dr. Bims) admitted at his deposition in the ITC that Nair does not expressly disclose an encryption scheme identifier. Ex-2001, 123:12–14.

Nair also does not disclose that the attach request includes a public key identifier, a fact that is undisputed. Ex-2001, 123:1–4 (testifying that “Nair does not expressly disclose public key identifiers”); Pet. 38–41 (relying on Forsberg for a “public key identifier”). Nair instead discloses that the receiving device (such as the SLF) already has the keys needed for the decryption. Ex-1004, [0035], [0038].³

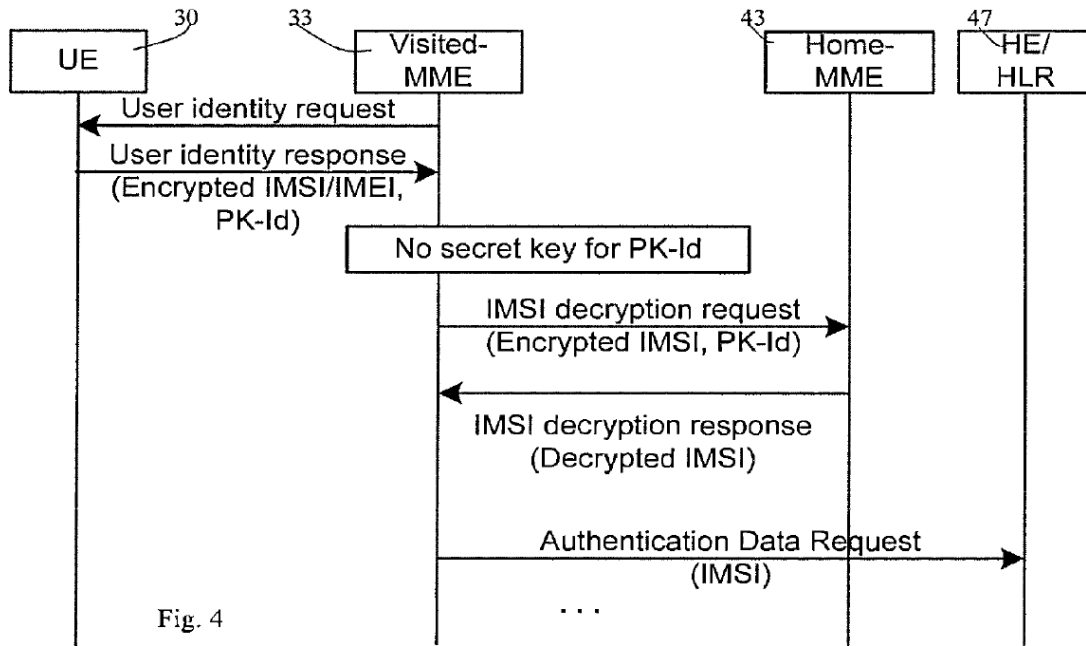
2) Forsberg

As a secondary reference, the Petition relies on U.S. Pat. App. Pub. No. 2013/0003971 (“Forsberg”). Forsberg relates to “Identifiers in a Communication

³The Petition (at 5–6) is also incorrect that Nair incorporates “in its entirety” two 3GPP specifications (TR 33.899 V1.1.0 and TS 23.501 V0.4.0) for the purposes of Nair’s invention, as detailed below.

System.” Ex-1005, (54). The Patent Office considered Forsberg during prosecution of the ’817 Patent. Ex-1001, (56).

Forsberg shows its general process below in connection with Figure 4.



In a visiting network (*i.e.*, a network other than the UE’s home network), an MME sends a user identity request to the UE. Ex-1005, Fig. 4, [0048]–[0056]. The UE then provides the MME with a response that includes an encrypted IMSI/IMEI (which are acronyms for “International Mobile Subscriber Identity” and “International Mobile Equipment Identity”). *Id.* After receiving the encrypted identifier, the MME determines if it is able to decrypt it. *Id.*, Fig. 2, [0043]–[0046]. If so, the MME decrypts the identifier; if not, the MME determines if there is another network entity that can decrypt the identifier (*e.g.*, another MME), requests assistance from the other entity, and obtains a decrypted identifier. *Id.*

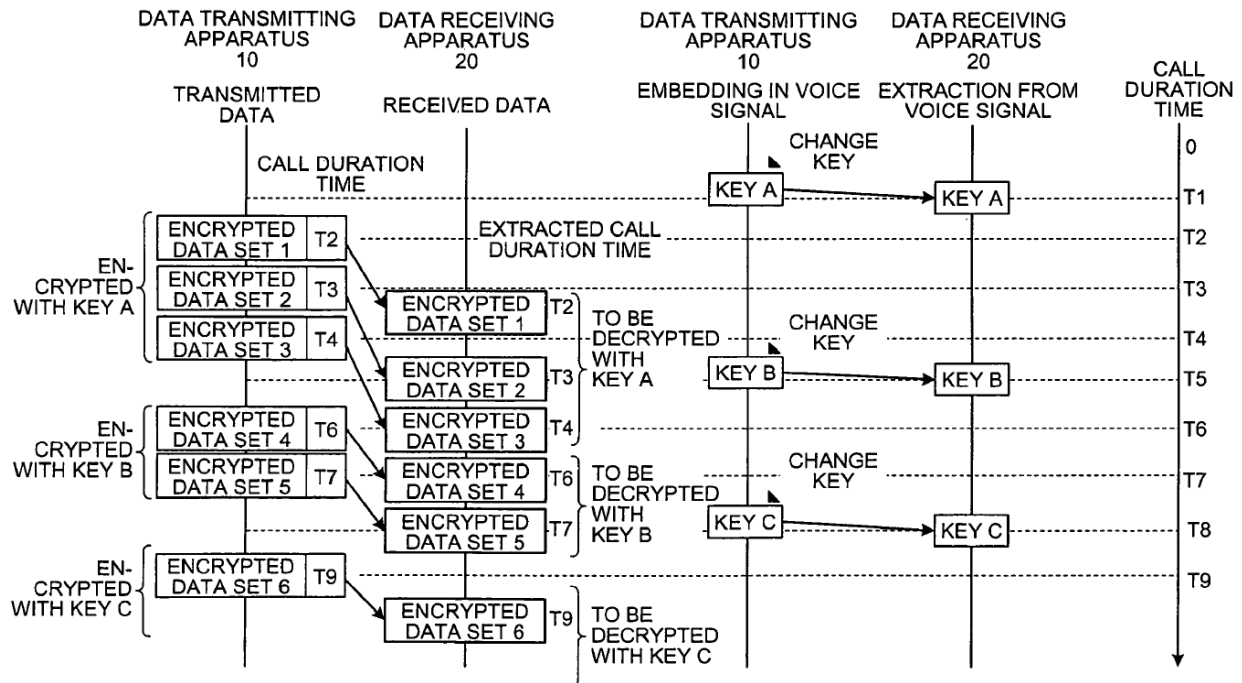
Like Nair, Forsberg recognizes that privacy is important. But Forsberg does not expressly disclose an encryption-scheme identifier, as Dr. Bims admitted at his deposition. Ex.-2001, 123:15–17. The Petition also does not rely on Forsberg as disclosing the encryption-scheme identifier. *See* Pet., 33–41.

3) Togawa

The Petition also relies on, as a secondary reference, U.S. Pat. No. 8,005,219 (“Togawa”). Togawa attempted to create “a technique that allows an integrated communications service for carrying out data communications of user data, as well as two-way communications of multimedia information, to transmit user data securely and efficiently.” Ex-1006, 2:21–25. The reference does not relate to LTE or 5G (or next-generation cellular networks in general).

In general, Togawa teaches embedding encrypted data within a voice signal (*e.g.*, Encrypted Data Set 1–6) that the receiving device can decrypt with one or more keys that change over time (*e.g.*, Key A, Key B, and Key C). Ex-1006, Fig. 1, 4:29–7:45; *see also* Fig. 8, 12:15–14:7 (showing system in which the receiving apparatus initiates the key change).

FIG. 1



Togawa describes a system that, after determining if a predetermined time period has elapsed, changes the encryption key (*e.g.*, from Key A to Key B) and transmits the encryption key in an embedded voice signal. Ex-1006, Fig. 4, 10, 8:21–9:7, 16:45–17:27; *see also* Figs. 5, 11 (depicting steps for receiving the embedded key); *id.*, 9:8–34; 17:28–18:5.

4) 5G-Ensure Deliverable D3.1, “5G-PPP security enablers technical roadmap”

For two dependent claims, the Petition relies on 5G-Ensure Deliverable D3.1 5G-PPP Security Enablers Open Specifications (Early Version) (“5G-Ensure”) as a secondary reference. 5G-Ensure arose from a European Union-funded group of projects. The reference reflects a desire to enable privacy more generally for users

in the then-upcoming 5G Standard. 5G-Ensure discusses the high-level concept of encrypting subscriber identifier information in 5G networks. Ex-1010, 32–34.

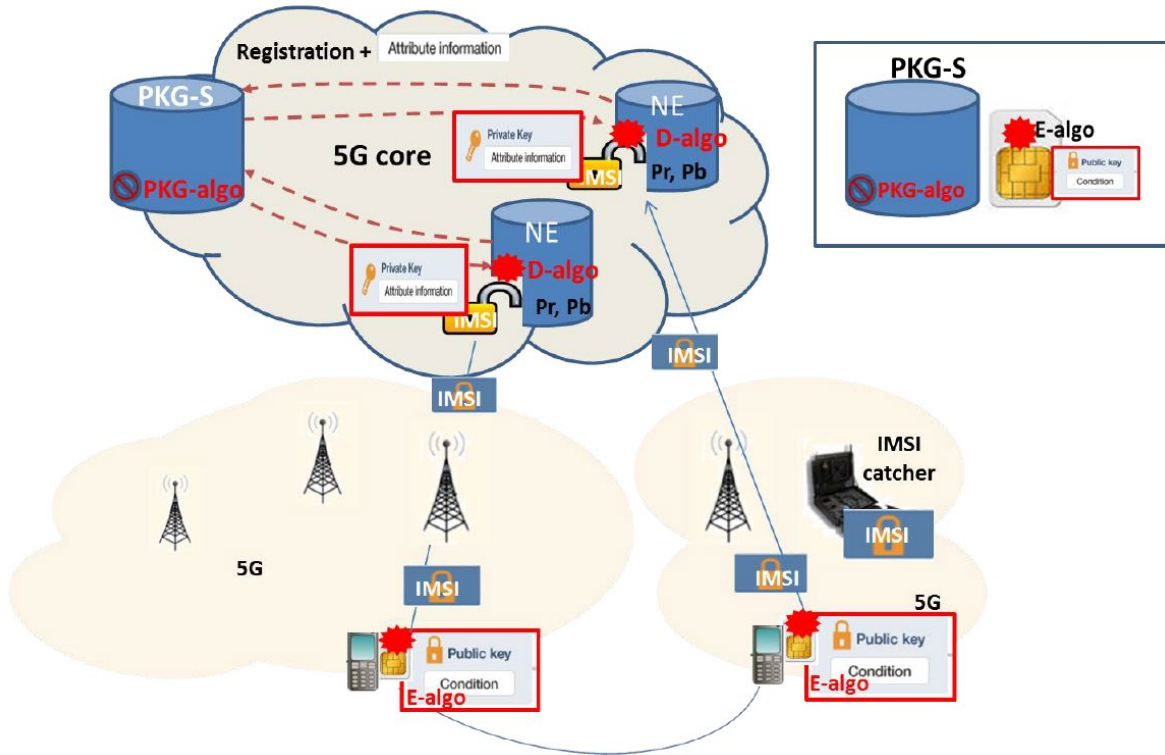


Figure 5: High level components of the feature "Encryption of Long Term Identifiers"

5G-Ensure D.31 does not describe the messaging scheme to use for this proposal. It also does not detail the structure of the transmitted subscriber information, such as which parts are clear-text, which parts are encrypted, and what other encryption-related metadata resides in the message (*e.g.*, fields identifying an encryption scheme or a public key). The reference also does not provide specific detail of the servers involved in the process. The Patent Office considered a later version of 5G-Ensure during prosecution of the '817 Patent. Ex-1001, (56).

D. Person of Ordinary Skill in the Art (POSITA)

For the purpose of this POPR only, Patent Owner submits that POSITA is one having 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. Patent Owner submits that the Board can deny institution under any definition of a POSITA.

E. Related Proceedings

Patent Owner filed proceedings in the ITC against Petitioner, asserting that Petitioner's 5G smartphones infringe the '817 Patent. That proceeding is set for a hearing the week of July 15, 2024.⁴

In the ITC, Petitioner has asserted invalidity based on the same references here—Nair, Forsberg, Togawa, and 5G-Ensure—and is raising those references at the ITC trial in mid-July. Petitioner also relied on the same expert witness (Dr.

⁴ Patent Owner also filed suit in the Eastern District of North Carolina, alleging that Petitioner infringes the '817 Patent. *Telefonaktiebolaget LM Ericsson v. Lenovo (US) Inc.*, 5:23-CV-00569 (E.D.N.C. Oct. 11, 2023). The allegations relating to the '817 Patent are stayed pending the outcome of the ITC investigation (Dkt. 72).

Bims) in the ITC that it relies on in this proceeding.

Ericsson deposed Dr. Bims in the ITC case on May 31, 2024. At his deposition, Dr. Bims made a number of admissions relevant to this proceeding, including that Nair does not expressly disclose an encryption scheme identifier. Ex-2001, 123:12–14

III. THE BOARD SHOULD NOT INSTITUTE *INTER PARTES* REVIEW

A. The Petition Fails to Establish a Reasonable Likelihood That Any Challenged Claim is Unpatentable

1) The Petition Fails to Show That Nair is Prior Art

All four grounds in the Petition hinge on Nair. The Petition, however, fails to show that Nair is prior art.

a) It is Uncontested That the '817 Patent is Entitled to a July 25, 2017 Effective Filing Date

The '817 Patent claims priority to a July 25, 2017 provisional application (U.S. Provisional App. No. 62/536,632, Ex-2004). Ex-1001, (60). The Petition does not challenge the July 25, 2017 effective filing date of the '817 Patent. Dr. Bims likewise assumes that the effective filing date of the '817 Patent is July 25, 2017. Ex-1002, ¶ 20. Dr. Bims also testified, as part of his invalidity analysis in the ITC, that he was not challenging the July 25, 2017 priority date of the '817 Patent. Ex-2001, 114:25-115:3.

Indeed, the July 25, 2017 provisional application and '817 Patent contain virtually identical disclosures. *Compare e.g.*, Ex-1001, Figs. 1–22 *with* Ex-2004,

Figs. 0–22. The provisional application discloses the same SUCI as the '817 Patent. The SUCI in the provisional application includes an encrypted part that includes an encrypted SUPI (such as an MSIN) and does not include a home-network identifier. *E.g., id.*, Fig. 2, [0014]–[0017]. The SUCI also includes and a clear-text part that includes a public-key identifier, an encryption-scheme identifier (such as identifying an ECIES encryption scheme), and a home-network identifier (which can include a Mobile Country Code and a Mobile Network Code). *E.g., id.*

The provisional application likewise discloses that the UE generates the SUCI, including using a tamper-resistant, secure hardware component. *E.g., id.*, Figs. 6, 8 [0029]–[0030], [0033]–[0035]. And it discloses that the UE transmits the SUCI to an authentication server that analyzes the SUCI to determine an appropriate de-concealing server (of many potential servers) and then forwards the SUCI (along with a request for an authentication vector) to a de-concealing server capable of decrypting the encrypted part of the SUCI. *E.g., id.*, Figs. 5, 12, 13 [0024]–[0028], [0049]–[0069], [0075]–[0080]. The authentication server then receives the SUPI from the de-concealing server. *E.g., id.* The provisional application teaches that the authentication server receives the SUCI as part of the registration procedure for a UE and via an authentication request from a Security Anchor Function. *E.g., id.*, Figs. 5, 12, 13 [0005], [0023]–[0024], [0027]–[0028], [0049]–[0051], [0053], [0056]–[0068]. And the provisional application teaches that the UE transmits the

SUCI to the authentication server in response to an identifier request message received from the AMF as part of registering the UE with the cellular network. *E.g., id.* The effective priority date is July 25, 2017.

b) The Petition Relies on New Matter Added to Nair After July 25, 2017

The Petition relies on material from Nair that was added after July 25, 2017 and thus does not qualify as prior art. The Nair non-provisional application was filed on October 26, 2017, after the July 25, 2017 effective filing date of the '817 Patent. To qualify as prior art, Nair's disclosure must be entitled to the May 5, 2017 filing date of the Provisional Patent App. No. 62/502,266 (the "Nair Provisional," Ex-1008). The Petition fails to make that showing.

The Nair Provisional fails to adequately "describe[] the subject matter' relied upon" in Nair, as the Board's precedent requires. *Penumbra, Inc. v. RapidPulse, Inc.*, IPR2021-01466, Paper No. 34, 32 (P.T.A.B. Mar. 10, 2023) (precedential) (quoting AIA 35 U.S.C. 102(d)(2)). The Nair Provisional does not describe the "explicit" privacy indicator (such as a "flag or field") or the "implicit" or "null scheme" privacy indicator (*i.e.*, "the fact that the message is encrypted with a particular encryption algorithm") in paragraph 42 of Nair that the Petition relies on for the claimed SUCI element. Pet., 34–28 (citing Ex-1004, [0042]); Ex-1002, ¶¶ 73–81 (same). Indeed, Dr. Bims admitted at his ITC deposition that the Nair Provisional does not include the "null scheme," "implicit," or privacy indicator

“field” disclosures that are in paragraph 42 Ex-2001, 118:17–120:25.

While the Petition extensively relies on paragraph 42 of the Nair non-provisional application for the encryption-scheme identifier, the only portions of the Nair Provisional that the Petition cites describes the “privacy indicator” as a “privacy flag” that the system can “make the decision on the processing by looking at this flag.” “If the flag is set,” the system will recognize that the message is encrypted and “use the network private key to decrypt” the message. Ex-1008, 6:17–30 (cited by Pet., 34, 36).⁵ That section does not describe the “explicit” privacy indicator that is a “field” or the “implicit” or “null scheme” privacy indicator that the Petition relies upon.

Nor has Petitioner (or Dr. Bims) performed an analysis that the Nair Provisional supports paragraph 42 from Nair. But a side-by-side depiction of what the Petition cites from Nair Provisional and the Nair Non-Provisional shows that all of Nair’s paragraph 42 lacks support from the provisional and is new matter.

⁵ The Petition also cites page 8, lines 1–3. Pet., 38. That sentence states “If the subscription identifier is encrypted, the size of the message field for the encrypted IMSI may be different from today's 4G IMSI field (depending on the solution class chosen),” Ex-1008, 8:1–3, which does not speak to the privacy indicator at all.

Nair Provisional (Ex-1008)	Nair Non-Provisional (Ex-1004)
(6:17–18) In a first illustrative embodiment, the 5G UE, if it wants to protect its privacy, adds an identity privacy flag (i.e., privacy indicator) to indicate that the MSIN is provided encrypted.	[0041] In a first illustrative embodiment, the 5G UE, if it wants to protect its privacy, adds an identity privacy flag (i.e., privacy indicator) to indicate that the MSIN is provided in encrypted form. [0042] It is to be appreciated that the privacy indicator, in addition to being an “explicit” privacy indicator such as a flag or field, can alternatively be an “implicit” privacy indicator. By implicit privacy indicator, it is meant that the privacy feature is conveyed by the UE to a network element/function via the algorithm used to encrypt the message. Thus, the network element/function receiving the message from the UE is informed of the privacy feature by the fact that the message is encrypted with a particular encryption algorithm. This also applies to a null-encryption scheme. In a null-encryption scheme, the input equals the output, and the SUPI (Subscription Permanent Identifier of the UE) is unencrypted, i.e., a format-preserved scheme. One could interpret this as the SUPI (or IMSI) is always encrypted, but if no privacy is “switched on,” then the null-encryption is used. Thus, the privacy indicator would implicitly reside in the algorithm scheme used (e.g., null-encryption or an algorithm that actually encrypts a message).
(6:19–30) It could be suggested that the HSS or SLF, even without this	[0043] It could be suggested that the HSS or SLF, even without this privacy

Nair Provisional (Ex-1008)	Nair Non-Provisional (Ex-1004)
privacy indicator, will figure out after the first attempt to solve the request and, if encrypted, to attempt the decryption. But one key reason to have such an indication specified is that this saves processing time and less resources are needed. Thus, in this first illustrative embodiment, the SLF can make the decision on the processing by looking at this flag. If not set, the SLF will assume the provided IMSI is unencrypted, will do the IMSI-to-HSS resolution, and will forward to the correct HSS/UDM, i.e., compatibility with 4G operation is maintained. If the flag is set, the SLF will recognise that the provided IMSI is encrypted and use the network private key to decrypt the MSIN part to form the real unencrypted IMSI, perform the IMSI to-HSS resolution and then forward the Authentication Request to the correct HSS/UDM. If no SLF is used, the same principle can be used by the HSS/UDM. That is, HSS/UDM has to check whether the 5G UE has set a flag and then decide whether decryption is needed.	indicator, will figure out after the first attempt to solve the request and, if encrypted, to attempt the decryption. But one key reason to have such an indication specified is that this saves processing time and fewer resources are needed. Thus, in this first illustrative embodiment, the SLF can make the decision on the processing by looking at this flag. If not set, the SLF will assume the provided IMSI is unencrypted, will do the IMSI-to-HSS resolution, and will forward to the correct HSS/UDM, i.e., compatibility with 4G operation is maintained. If the flag is set, the SLF will recognize that the provided IMSI is encrypted and use the network private key to decrypt the MSIN part to form the real unencrypted IMSI, perform the IMSI-to-HSS resolution and then forward the Authentication Request to the correct HSS/UDM. If no SLF is used, the same principle can be used by the HSS/UDM. That is, HSS/UDM has to check whether the 5G UE has set a flag and then decide whether decryption is needed.

The Nair Provisional likewise does not disclose the functionality of what the Petition asserts meets the claimed “authentication server” and “de-concealing server” elements. For these elements, the Petition relies on the disclosure from the Nair non-provisional application describing Figures 4, 5, and 6. Pet., 41–44 (citing Ex.1004, [0047], [0051], [0054], [0057], [0067], [0072]–[0076], [0078], [0085]).

That disclosure is 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. Ex.1008, 13:10–20.

FIG. 4 illustrates a high-level UE authentication procedure 400 in 5G using encrypted IMSI, SLF and multiple UDM. Performing the IMSI decryption at the SLF instead of the UDM helps to maintain the core authentication functions unchanged, in accordance with one illustrative embodiment.

FIG. 5 illustrates a procedure 500 for a mixed core architecture of UDM and HSS to support 4G LTE and 5G networks, in accordance with one illustrative embodiment. IMSI decryption at SLF helps to manage both cores.

FIG.6 illustrates a high-level UE authentication procedure 600 in 5G using encrypted IMSI, SLF and multiple UDM, in accordance with an illustrative embodiment. Performing the IMSI decryption at the SLF instead of the UDM helps to maintain the core authentication functions unchanged.

Because the Petition relies on material that only appears in the Nair Non-Provisional Application—new matter added after the '817 Patent's effective filing date—those portions of Nair cannot be used to invalidate the claims. 35 U.S.C. §§ 102(a)(1), (a)(2), 103 (requiring the prior art disclosure occur "before the effective filing date of the claimed invention") (emphasis added).⁶

⁶ In addition, the Petition does not attempt to show that the disclosure in the Nair Provisional supports at least one claim in Nair. *See, e.g., Dynamic Drinkware, LLC*

2) Nair Fails to Teach the Claimed “Encryption Scheme Identifier,” As Dr. Bims Admitted

For Grounds 1 and 3, the Petition exclusively relies on Nair for the encryption-scheme-identifier element of the claimed SUCI. The claims require that the SUCI itself includes “an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI.” Nair’s privacy indicator lacks this element because it only identifies if encryption was “on” or “off,” and the receiving device—with the encryption key it already has—attempts to decrypt the message based on what it assumes the scheme to be. The privacy flag itself does not identify the encryption scheme that the UE actually used to encrypt the subscription identifier. Dr. Bims also admitted that Nair does not expressly disclose an encryption scheme identifier (and the Petition lacks an allegations that Nair inherently discloses this element). Ex-2001, 123:12–14.

v. National Graphics, Inc., 800 F.3d 1375, 1381 (Fed. Cir. 2015). Patent Owner understands that the Board has concluded that *Dynamic Drinkware* does not apply to patents subject to the AIA. *Penumbra*, IPR2021-01466, Paper No. 34, 32. Patent Owner respectfully submits that *Dynamic Drinkware* applies here because of the similarities in the statutory language between pre- and post- AIA Sections 102 and 119.

a) Nair Discloses a “Privacy Indicator”—Not an Encryption Scheme Identifier

Nair teaches that the privacy indicator operates as a flag or switch—it conveys whether encryption is “on” or “off” (*e.g.*, a “0” or “1” flag). Ex-1004, [0010], [0014]; [0041]; [0043]. It does not identify an encryption scheme, let alone the scheme “used by the UE to encrypt the subscription identifier in the SUCI.” Ex-1001, claim 10.

Nair explains why its privacy indicator is just a switch and does not actually identify the encryption scheme used to encrypt the subscription identifier in the SUCI. Nair’s system uses the privacy indicator to determine if it should attempt decryption (*e.g.*, if the indicator has one value, attempt decryption; else, skip the decryption step). Ex-1004, [0043] (describing use of indicator); *see also id.* (further describing the system’s use of the indicator as a “check” for a value and then “decid[ing] whether decryption is needed”). There is no disclosure in Nair that the indicator is used beyond that simple check.

Nair uses the privacy indicator to determine if the system should attempt to decrypt the attach request. Indeed, Nair teaches that the receiving device (*e.g.*, the SLF) already has all of the information needed for the decryption, *see, e.g.*, Ex.1004, [0035], [0038], which the Petition acknowledges (at 35). There is thus no need for Nair’s request to identify an encryption scheme (and any additional information, such as encryption keys) because the receiving device already has the keys to decrypt

the message. The Petition does not allege that Nair discloses a key identifier in the request. Pet. 38–41 (relying on Forsberg for a “public key identifier”). Dr. Bims likewise testified that “Nair does not expressly disclose public key identifiers.” Ex-2001, 123:1–4. And the lack of a key identifier in the transmission reinforces that Nair’s privacy indicator is an “on”/“off” indicator, not an “encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI.” Ex-1001, claim 10 (emphasis added).

Likewise, there also is no disclosure in Nair that, based on the privacy indicator, the receiving device looks up the particular encryption scheme used (and the necessary keys required to complete the decryption). One would expect to see such disclosure if, in fact, the privacy indicator did identify an encryption scheme. There is no disclosure of supporting multiple encryption schemes in Nair, and the Petition does not identify any such teaching.

b) Dr. Bims Admitted That Nair Does Not Disclose an Encryption Scheme Identifier

In the ITC, Petitioner also asserts that Nair invalidates the ’817 Patent claims and relies on Dr. Bims’s expert testimony. At his deposition, however, Dr. Bims agreed that “Nair does not expressly disclose an encryption scheme identifier.”

Q. Do you agree that Nair does not expressly disclose an encryption scheme identifier?

A. Yes.

Ex-2001, 123:12–14.⁷ This testimony should end the inquiry from these Grounds. The Petition does not allege that Nair inherently discloses this element. *See, e.g.,* Pet., 33–38. This is for good reason: inherency is a high bar—requiring a showing that “the natural result flowing from the operation as taught would result in the performance of the questioned function,” *PersonalWeb Techs., LLC v. Apple, Inc.*, 917 F.3d 1376, 1382 (Fed. Cir. 2019) (citation omitted)—and Nair does not clear it. As detailed above, Nair shows that its system does not identify an encryption scheme from the privacy indicator. It only uses the privacy indicator as a switch to save a step when processing a request (*i.e.*, attempt decryption using known decryption keys or process the request without attempting decryption). Ex-1004, [0043].

*c) Nair’s Paragraph 42—New Matter That Post-Dates the
’817 Patent—Does Not Support the Petition*

The Petition almost exclusively relies on paragraph 42 of Nair to claim that Nair discloses or renders obvious the encryption-scheme-identifier limitation. Pet., 33–38. But Nair does not actually disclose what the Petition alleges, as Dr. Bims later testified. And paragraph 42 is new matter in Nair that post-dates the unchallenged priority date of the ’817 Patent and is not prior art.

⁷ Dr. Bims also admitted that “Forsberg does not expressly disclose an encryption scheme identifier.” Ex.-2001, 123:15–17. The Petition does not rely on Forsberg as disclosing the encryption-scheme-identifier limitation. Pet. 33–38.

The Petition first misquotes paragraph 42, asserting that Nair teaches that the privacy indicator is an encryption scheme identifier because it “informs the element receiving the SUCI of the ‘particular encryption algorithm’ used to encrypt the MSIN.” Pet., 34, 36–37 (quoting Ex-1004, [0042] and citing Ex-1008, 6:17–18). But the paragraph says the opposite: it describes an “implicit” privacy indicator in which the receiving system “is informed of the privacy feature” by virtue of “the fact that the message is encrypted with a particular encryption algorithm,” as recited below. Ex-1004, [0042].

It is to be appreciated that the privacy indicator, in addition to being an “explicit” privacy indicator such as a flag or field, can alternatively be an “implicit” privacy indicator. By implicit privacy indicator, it is meant that the privacy feature is conveyed by the UE to a network element / function via the algorithm used to encrypt the message. Thus, the network element / function receiving the message from the UE is informed of the privacy feature by the fact that the message is encrypted with a particular encryption algorithm. This also applies to a null-encryption scheme. In a null-encryption scheme, the input equals the output, and the SUPI (Subscription Permanent Identifier of the UE) is unencrypted, i.e., a format-preserved scheme. One could interpret this as the SUPI (or IMSI) is always encrypted, but if no privacy is “switched on,” then the null-encryption is used. Thus, the privacy indicator would implicitly reside in the algorithm scheme used (e.g., null-encryption or an algorithm that actually encrypts a message).

This section does not teach that the privacy indicator includes an encryption-scheme identifier; it simply states that the receiving device can infer that the privacy

indicator is set “by the fact that the message is encrypted with a particular encryption algorithm.” Ex-1004, [0042]. Nor does Nair disclose that the privacy indicator identifies a null encryption scheme, as the Petition alleges (at 36). Nair again states the opposite: when the message is un-encrypted (the “null encryption scheme”), the SLF can then infer that the privacy indicator was set “no.” *Id.* At no point does Nair teach that the privacy indicator itself identifies the encryption scheme used by the UE to encrypt the SUCI.

The Petition’s reliance (at 34 and 36) on the “field” from paragraph 42 is likewise incorrect. Regardless of the specific format of the privacy indicator (*e.g.*, a one-bit “flag” versus a multi-bit “field”), Nair discloses that the privacy indicator conveys the same information: it is a “yes”/“no” of whether encryption was used and does not identify the encryption scheme actually used by the UE. That a “field” could potentially have multiple bits does not mean it identifies an encryption scheme. And it does not provide a motivation to include an encryption-scheme identifier within Nair’s request—the reference provides no reason to do so and actually teaches away from that approach: Nair’s SLF already has the public and private keys needed for decryption, and the reference does not envision or disclose multiple encryption schemes.

Undeterred, the Petition claims (at 38) that Nair discloses in paragraph 42 that “multiple non-null-encryption schemes existed.” Paragraph 42 does not say that

(and neither does the Nair Provisional). Apparently recognizing that deficiency, the Petition points to 3GPP TR 33.899, asserts it was “incorporated by reference,” and thus argues that Nair’s system encompasses multiple encryption schemes. Pet., 38.

This claim is also wrong. Nair shows that the material the Petition relies on as “incorporated by reference” does not apply to Nair’s system at all—and certainly does not apply to Nair’s privacy indicator. Nair mentions TR 33.899 in the following two sentences in the background section. Ex-1004, [0007]; Ex-1008, 2:4–9.

Privacy is broadly addressed in 5G Technical Report (TR) 33.899, V1. 1.0, entitled "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14)," the disclosure of which is incorporated by reference herein in its entirety. In particular, TR 33.899 identifies subscription (UE) privacy as one of the most important security areas to be addressed in 5G networks.

These sentences do not identify any specific pages or section numbers within the 500-plus page technical report that could apply to Nair’s system, let alone the specific pages the Petition now relies on. *E.g.*, Pet., 38 (citing pages 360 and 374); *id.*, 50, 51 (citing page 341); *id.*, 51 (citing pages 285, 344, and 376-377); *id.*, 55 (citing page 323); *id.*, 57 (citing pages 119 and 120). Nor does the “incorporation” suggest that aspects of the privacy indicator could be used in systems that utilize multiple encryption schemes—and none of the pages cited by the Petition refer to an encrypted SUCI or similar concepts.

To the contrary, the incorporation is for “background.” As a result, Nair shows that TR 33.899 does not apply any specific aspect Nair’s invention (including the privacy indicator). *Paice LLC v. Ford Motor Co.*, 881 F.3d 894, 908 (Fed. Cir. 2018) (“The applicability of a document’s disclosed features and the incorporation of the document itself are distinct concepts, and one does not imply the other.”); *Modine Mfg. Co. v. U.S. Int’l Trade Comm’n*, 75 F.3d 1545, 1553 (Fed. Cir. 1996) (“[I]ncorporation by reference does not convert the invention of the incorporated patent into the invention of the host patent.”).

At most, TR 33.899 shows that, in general, there were multiple types of encryption. But that does not mean that Nair discloses multiple encryption schemes in its system or that its system could have been modified to include an encryption-scheme identifier. Again, that approach is contrary to Nair’s system. Indeed, the Petition’s reliance on TR 33.899 reinforces that the Petition fails to demonstrate unpatentability based on Nair: the reference purposefully teaches a privacy indicator (a “yes”/“no”) where a central system already has the key needed to decrypt the request, even though Nair (according to the Petition) knew of multiple encryption schemes. This shows that Nair teaches away from using multiple encryption schemes (and using a scheme identifier); it opted for a simpler system instead.

Similarly, the Petition’s claim (at 35) that Nair could include an encryption scheme identifier “so that the SLF could select the correct decryption scheme on its

first attempt to decrypt and thereby reduce processing time and resource consumption” is at odds with Nair itself. Nair does not disclose multiple encryption schemes, and thus, there is no disclosure in Nair of “select[ing] the correct decryption scheme on its first attempt.” Instead, Nair discloses that the “first attempt” is determining if to decrypt the message or not using known keys—not identifying which encryption scheme to use. Ex-1004, [0043]. There is no reason to identify the encryption scheme in Nair’s message because nothing in Nair indicates that the SLF would use that information for any purpose. There is no disclosure of looking up encryption schemes, utilizing different keys for different schemes, receiving a public key associated with the encryption scheme in the message, or the like.

Beyond the substance of paragraph 42, the Petition fails to show that the material in paragraph 42 pre-dates the ’817 Patent. The portion of the Nair Provisional that the Petition cites as supporting paragraph 42 only describes an “identity privacy flag (i.e., privacy indicator) to indicate that the MSIN is provided encrypted” and that the system uses to attempt decryption based on if the flag is set. Pet. 35, 37 (citing Ex-1008, 6:17–30). This does not disclose the “implicit” indicator, “null scheme,” “field,” or “multiple encryption schemes” that the Petition extensively relies upon. This lack of disclosure reinforces that Nair, including at least paragraph 42, is not prior art to the ’817 Patent.

3) Togawa Fails to Disclose the Claimed Encryption-Scheme Identifier

For Grounds 2 and 4, the Petition assumes that Nair does not disclose an encryption-scheme identifier. The Petition instead relies on Togawa for this limitation. Pet., 63–64. Togawa, however, does not teach this element.

The Petition (at 62–63) points to a single disclosure in Togawa that encryption-specific information (90 in the Figure below) “includes information on an encryption key and an encryption-method ID.” Ex-1004, Fig. 13, 23:17–25.

**ENCRYPTION
SPECIFICATION
INFORMATION**
90
↓

ENCRYPTION KEY	ENCRYPTION- METHOD ID
*****	3

This disclosure does not teach the encryption-scheme-identifier limitation or render it (or the claims) obvious. The claims require the encryption-scheme-identifier to identify a specific thing: “an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI.” Ex-1001, claim 10 (emphasis added). But the Petition does not allege that Togawa encrypts subscriber information or that the method ID identifies an encryption scheme used to encrypt subscriber information. And there is no teaching in Togawa to that effect: Togawa

states that the encryption-method ID “identifies an encryption method for use in encryption of the user data” embedded in the voice signal. Ex.1006, Fig. 13, 23:17–25 (emphasis added). The Petition does not dispute that user data in a voice signal, such as multimedia video, is different than subscriber information (like the SUPI).

Because the Petition fails to show that Togawa discloses an encryption scheme identifier as claimed, the combination of Nair and Togawa (and Forsberg and 5G-ENSURE) fail to teach the claimed encryption-scheme identifier. At most, the combination would include an identifier that identifies the encryption method used to encrypt user data in a voice signal, not the subscriber information. That combination does not meet the encryption-scheme-identifier limitation.

4) The Petition Fails to Show Obviousness

The Petition also fails to show obviousness based on the combination of references in each ground: Nair and Forsberg (and Nair, Forsberg, and 5G-Ensure); and Nair, Forsberg, and Togawa (and Nair, Forsberg, and Togawa and 5G-Ensure).

The Petition first fails to show that a POSITA would have been motivated to combine Nair and Forsberg—a requirement for all four grounds. The Petition exclusively relies on Forsberg as teaching the public-key-identifier limitation of the Challenged Claims. Pet., 38–41. The Petition does not assert that Nair (or Togawa) teaches that limitation. *See id.*, 38–41, 63–65. The Petition asserts that a POSITA reading Nair would have “been motivated to seek methods of managing multiple

public keys as taught by Forsberg.” *Id.*, 40–41.

The Petition, however, ignores that Nair teaches against that combination. Nair discloses that the receiving device (*e.g.*, the SLF) already has the public key and private key needed to decrypt the message, as detailed above. There would thus have been no motivation to modify Nair to include another field in the request when the receiving device already has the public key information. And the Petition fails to point to a motivation in Nair or Forsberg. There is no disclosure in Nair of multiple or different keys, looking up encryption schemes, or managing keys.

Similarly, the Petition does not explain how Nair would work if the request included a public-key identifier given the limitations of Nair’s architecture. There is no disclosure in Nair, as detailed above, about how Nair’s systems would handle a field that includes a public-key identifier given that Nair’s architecture does not provide for identifying, processing, or utilizing encryption schemes or a public-key identifier contained in Nair’s requests. Instead, as detailed above, Nair is about the SLF already having the public and private key it needs to decrypt the message. Nair does not disclose any mechanism to utilize information about the actual encryption scheme used, *e.g.*, it does not disclose a way to receive and process the information to implement the decryption of the encrypted part of the SUCI. There is also no mapping between the elements of Forsberg (*e.g.*, the visited and home MMEs) to the elements in Nair’s system (*e.g.*, the AMF/MME, AUSF, SLF, and HSS) that would

indicate how a POSITA could even incorporate the functionality of Forsberg into Nair. These are different architectures, and the Petition does not explain how a POSITA would have bridged the gap between the two systems. Because the Petition does not show that it would have been obvious to a POSITA to combine Nair and Forsberg, the Board can deny institution on all grounds on this basis alone.

In addition, for Grounds 2 and 4, the Petition fails to show it would have been obvious to combine Nair, Forsberg, and Togawa. The Petition claims that a POSITA would combine Nair with Togawa to “manage the implementation of multiple non-null encryption methods and capitalize on the encryption indicator benefits as taught by Nair.” Pet., 62. But Nair does not implement “multiple non-null encryption methods,” as explained above. And, as detailed above, Nair teaches away from modifying the privacy indicator to support multiple encryption methods: Nair discloses a simple system in which a central SLF already has the encryption keys and the privacy indicator simply acts as an “on”/“off” indicator.

The Petition also does not provide a reason that a POSITA would have looked to Togawa (a decade-old, unrelated system) for inspiration. Togawa, in general, is about encrypting data communications that are embedded in pre-LTE-era voice communications (*e.g.*, texts, pictures, and videos sent to flip phones). It teaches a different type of system in which the key changes periodically over different segments of data. Togawa is not about securing subscriber information in general,

it does not relate to next-generation cellular networks (such as 5G), and it does not relate to securing subscriber information through the cellular infrastructure.

The Petition also does not explain how combining Nair's system with Togawa would have a reasonable expectation of success. There is no disclosure in Nair, as detailed above, about how it would handle a field that includes an encryption-method ID given that Nair's architecture does not provide for identifying, processing, or utilizing encryption schemes. Instead, as detailed above, Nair is about the SLF already having the key it needs for decryption and lacks a mechanism to utilize information about the encryption scheme used. Because the Petition does not show that it would have been obvious to a POSITA to combine Nair, Forsberg, and Togawa, the Board can deny institution of Grounds 2 and 4 on this basis.

IV. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Board deny institution of the Petition.

Respectfully submitted,

Date: June 28, 2024

/s/ Scott W. Hejny
Scott W. Hejny
Reg. No. 45,882
shejny@mckoolsmith.com
Christian J. Hurt
Reg. No. 63,659

churt@mckoolsmith.com

McKool Smith, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
Telephone: (214) 978-4000
Fax: (214) 978-4044

Attorneys for Patent Owner
Telefonaktiebolaget LM Ericsson

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER PRELIMINARY RESPONSE** specified in 37 C.F.R. § 42.24 have 7,999 words, in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24(b)(1). This word count was prepared using Microsoft Word 2016.

Respectfully submitted,

Date: June 28, 2024

/s/ Scott W. Hejny
Scott W. Hejny
Reg. No. 45,882

CERTIFICATION OF SERVICE

The undersigned hereby certifies that the above-captioned **PATENT OWNER PRELIMINARY RESPONSE** is being served on counsel for petitioner via electronic mail on June 28, 2024, in its entirety on the following counsel of record for Respondent:

Robert A. Appleby
W. Todd Baker
John R. Rhine

rappleby@kirkland.com
todd.baker@kirkland.com
john.rhine@kirkland.com

Lenovo_PTAB@kirkland.com

/s/ Scott W. Hejny
Scott W. Hejny
Reg. No.45,882
MCKOOL SMITH, P.C.
300 Crescent Court, Suite 1500
Dallas, TX 75201
Tel.: 214-978-4241
Fax: 214-978-4044