

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.
Petitioner

v.

TELEFONAKTIEBOLAGET LM ERICSSON,
Patent Owner

U.S. PATENT NO. 10,425,817

Case IPR2024-TBD

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,425,817**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES	2
	A. Real Parties-In-Interest.....	2
	B. Related Matters.....	2
	C. Lead And Back-Up Counsel	3
	D. Service Information.....	4
III.	PAYMENT OF FEES	4
IV.	CERTIFICATION OF STANDING	4
V.	OVERVIEW OF CHALLENGE AND RELIEF REQUESTED.....	4
	A. Prior Art References.....	4
	B. Relief Requested.....	7
VI.	THE '817 PATENT.....	8
	A. Summary of the Specification.....	8
	B. Person of Ordinary Skill in the Art	10
VII.	CLAIM CONSTRUCTION	11
VIII.	OVERVIEW OF PRIOR ART	11
	A. Nair	11
	B. 3GPP TR 33.899 V1.1.0 (Release 14)	13
	C. 3GPP TS 23.501 V0.4.0 (Release 15).....	14
	D. Forsberg.....	14
	E. Togawa	16

F.	5G -Ensure Deliverable D3.1, “5G-PPP security enablers technical roadmap” (early version)	17
IX.	SPECIFIC GROUNDS FOR PETITION UNDER 37 C.F.R. § 42.104(B)	18
A.	Ground 1: Claims 1-6 and 8-16 Are Rendered Obvious By Nair in Combination with Forsberg.....	18
1.	Motivation to Combine Nair And Forsberg.....	18
2.	Independent Claim 1	23
3.	Dependent Claim 2	44
4.	Dependent Claim 3	47
5.	Dependent Claim 4	47
6.	Dependent Claim 5	48
7.	Dependent Claim 6	50
9.	Dependent Claim 8	51
10.	Independent Claim 9	52
11.	Independent Claim 10	54
12.	Dependent Claim 11	55
13.	Dependent Claim 12	55
14.	Dependent Claim 13	56
15.	Dependent Claim 14	58
16.	Independent Claim 15	58
17.	Dependent Claim 16	59
B.	Ground 2: Claims 1-6 and 8-16 Are Rendered Obvious By Nair in Combination with Forsberg and Togawa.....	59
1.	Motivation to Combine Nair, Forsberg, and Togawa.....	59
2.	Independent Claim 1	63
3.	Independent Claims 9, 10, and 15.....	65
4.	Dependent Claims 2-6, 8, 11-14, and 16-17.....	65
C.	Grounds 3 and 4: Claims 8 and 14 are Rendered Obvious By The References of Grounds 1 and 2, in Further Combination with 5G-Ensure D3.1.....	66
1.	Claims 8 and 14.....	66
X.	SECONDARY CONSIDERATIONS	68

XI.	PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION.....	69
A.	The <i>Advanced Bionics</i> Test Favors Institution—§ 325(d).....	69
B.	The <i>Fintiv</i> Factors Favor Institution—§ 314(a).....	70
XII.	CONCLUSION.....	72

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Advanced Bionics, LLC v. Med-El Elektromedizinische Gerate GMBH,</i> IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020).....	70
<i>Advanced Display Sys., Inc. v. Kent State Univ.,</i> 212 F.3d 1272 (Fed. Cir. 2000)	27
<i>Apple Inc. v. Aire Technology Ltd.,</i> No. IPR2022-01136, Paper 11 (P.T.A.B. Jan. 4, 2023)	71
<i>Apple Inc. v. Seven Networks, LLC,</i> IPR2020-00235, Paper 10 (P.T.A.B. July 28, 2020).....	71
<i>Certain Mobile Phones, Components Thereof, and Products Containing Same,</i> Inv. No. 337-TA-1375, Complaint (U.S.I.T.C. Oct. 11, 2023).....	3
<i>In re Dance,</i> 160 F.3d 1339 (Fed. Cir. 1998)	18
<i>NanoCollect Biomedical, Inc. v. Cytonome/ST, LLC,</i> IPR2020-00551, Paper 19 (P.T.A.B. Aug. 27, 2020).....	71
<i>NVIDIA Corp. v. Invesas Corp.,</i> IPR2020-00602, Paper 11 (P.T.A.B. Sept. 3, 2020).....	71
<i>Ormco Corp. v. Align Tech., Inc.,</i> 463 F.3d 1299 (Fed. Cir. 2006)	68
<i>Sand Revolution II, LLC, v. Continental Intermodal Grp. Trucking LLC,</i> IPR2019-01393, Paper 24 (P.T.A.B. June 16, 2020)	71, 72
<i>Wyers v. Master Lock Co.,</i> 616 F.3d 1231 (Fed. Cir. 2010)	69

All emphases are added unless otherwise noted.

LIST OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 10,425,817 to Torvinen, <i>et al.</i> (“the ’817 patent”)
1002	Declaration of Harry V. Bims, Ph.D.
1003	<i>Curriculum Vitae</i> of Harry V. Bims
1004	U.S. Patent Publication No. 2018/0324585 (“Nair”)
1005	U.S. Patent Publication No. 2013/0003971 (“Forsberg”)
1006	U.S. Patent No. 8,005,219 (“Togawa”)
1007	3GPP TR 33.899, <i>Study on the security aspects of the next generation system</i> , Version 1.1.0 (Release 14)
1008	U.S. Provisional Patent Appl. No. 62/502,266 (“the ’266 provisional” or “Nair provisional”)
1009	Certified File History of U.S. Patent No. 10,425,817 (“the ’037 Application”)
1010	5G-ENSURE Deliverable D3.1 5G-PPP security enablers technical roadmap (early version)
1011	V. Gayoso Martínez, <i>et al.</i> , <i>A Survey of the Elliptic Curve Integrated Encryption Scheme</i> , 2 J. Computer Sci. & Eng. 7 (Aug. 2010)
1012	U.S. Patent Publication No. 2016/0094988 to Lee
1013	3GPP TS 23.501, <i>System Architecture for the 5G System</i> , Version 0.4.0 (Release 15)
1014	3GPP TS 33.501, <i>Security Architecture and Procedures for 5G System</i> , Version V0.2.0 (Release 15)
1015	3GPP TS 23.003, <i>Numbering, Addressing, and Identification</i> , Version 15.0.0 (Release 15)

Petition for *Inter Partes* Review of U.S. Patent No. 10,425,817

1016	Declaration of Friedhelm Rodermund
1017	Declaration of Nathaniel E Frank-White

Petitioner Lenovo (United States) Inc. (“Petitioner”) requests *inter partes* review (“IPR”) of claims 1-6 and 8-16 (the “Challenged Claims”) of U.S. Patent No. 10,425,817 (“the ’817 patent”) (Ex. 1001), owned by Telefonaktiebolaget LM Ericsson (“Patent Owner”). Petitioner seeks a determination that the Challenged Claims are unpatentable.

I. INTRODUCTION

The ’817 patent’s claims are directed to encrypting a portion of a mobile phone user’s identification number when that number is transmitted across the air to a base station. Ex. 1001, 1:50-61. In the prior art and today, every mobile user is assigned a unique number called an International Mobile Subscriber Identity, or “IMSI.” *Id.*, 1:22-24. The IMSI comprises several fields: a Mobile Country Code (“MCC”) that identifies the user’s home country, a Mobile Network Code (“MNC”) that identifies the user’s carrier, and a Mobile Subscription Identifier Number (“MSIN”) that identifies the user. *Id.*, 2:24-31. If a bad actor were to retrieve a user’s IMSI—or specifically the MSIN that identifies the user—that actor could impersonate the user. *Id.*, 1:22-36. In certain prior art systems in which the IMSI was sent over the air unencrypted (or in “clear text”), bad actors could intercept the IMSI (and the MSIN) using a device called an “IMSI catcher.” *Id.*, 1:22-36. The ’817 patent proposes the most obvious approach to solving this problem: encrypt the MSIN before sending the IMSI over the air. *Id.*, 1:50-61.

Because the problem of IMSI catchers was well known, there existed many prior-art proposals to encrypt the MSIN. *Id.*, 1:37-43. Examples include the schemes disclosed by U.S. Patent Publication No. 2018/0324585 to Nair (Ex. 1004) and U.S. Patent Publication No. 2013/0003971 to Forsberg (Ex. 1005). These references, in combination with the other references discussed in this petition, render obvious the Challenged Claims of the '817 patent. Accordingly, IPR should be instituted and the Challenged Claims cancelled as unpatentable.

II. MANDATORY NOTICES

A. Real Parties-In-Interest

Petitioner identifies the following real parties-in-interest: 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.

B. Related Matters

The '817 patent is at issue in the following matters:

- (i) *Certain Mobile Phones, Components Thereof, and Products Containing Same*, Inv. No. 337-TA-1375 (Oct. 11, 2023); and
- (ii) *Telefonaktiebolaget LM Ericsson v. Lenovo (US) Inc. et al.*, C.A. No. 5:23-cv-00569 (E.D.N.C. Oct. 11, 2023).

The '817 Patent has previously been at issue in the following matters:

- (i) *Certain Mobile Telephones, Tablet Computers with Cellular Connectivity, and Smart Watches with Cellular Connectivity, Components thereof, and Products Containing Same*, Inv. No. 337-TA-1299, Comm’n Notice, 87 Fed. Reg. 10384 (Feb. 24, 2022);
- (ii) *Ericsson Inc. et al v. Apple Inc.*, C.A. No. 6:22-cv-00060 (W.D. Tex., Jan. 17, 2022); and
- (iii) *Ericsson Inc. et al v. Samsung Electronics, Co., Ltd. et al*, C.A. No. 2:22-cv-00380 (E.D. Tex. Dec. 10, 2020)

Ericsson purports to have “asserted the respective foreign counterparts of the ’817 Patent against Apple in the in the following countries: Brazil (BR 112020001538-5), Germany (EP 3659314), and the Netherlands (EP 3659314). *See* respectively, case nos. 0010616-60.2022.8.19.0001 (2nd Rio de Janeiro State Business Court); 2 O 29/22 (Mannheim); 2 O 54/22 (Mannheim); and C/09/632862 (District Court in The Hague).” *Certain Mobile Phones, Components Thereof, and Products Containing Same*, Inv. No. 337-TA-1375, Complaint at ¶ 50 (U.S.I.T.C. Oct. 11, 2023).

C. Lead And Back-Up Counsel

Lead Counsel	Back-Up Counsel
Robert A. Appleby (Reg. No. 40,897) Kirkland & Ellis LLP, 601 Lexington Avenue, New York, NY 10022, Telephone: 212.446.4800 Facsimile: 212.446.4900	W. Todd Baker (Reg. No. 45,265) Kirkland & Ellis LLP, 1301 Pennsylvania Avenue, N.W., Washington, D.C. 20004 Telephone: 202.389.3135 Facsimile: 202.389.5200

Petitioner concurrently submits a Power of Attorney pursuant to 37 C.F.R. §42.10(b).

D. Service Information

Petitioner consents to electronic service to the following email address:

Lenovo_PTAB@kirkland.com.

III. PAYMENT OF FEES

The undersigned authorizes the Office to charge the fee per 37 C.F.R. § 42.15(b) for this Petition to Deposit Account No. 506092. Review of 17 claims is requested. The undersigned further authorizes payment for any additional fees that may be due in connection with this Petition to be charged to the above-referenced deposit account.

IV. CERTIFICATION OF STANDING

Petitioner certifies pursuant to 37 C.F.R. §42.104(a) that the '817 patent is available for IPR and that Petitioner is not barred or estopped from requesting an IPR of the Challenged Claims on the grounds identified herein.

V. OVERVIEW OF CHALLENGE AND RELIEF REQUESTED

A. Prior Art References

Petitioner's challenge is based on the following prior-art references:

- **Nair** - U.S. Patent Publication No. 2018/0324585 to Nair (Ex. 1004) is prior art to the '817 patent under 35 U.S.C. § 102(a)(2) and was effectively filed on May 5, 2017. Nair is a published application under 35 U.S.C. § 122(b) of U.S. Patent Application No. 15/794,856. *See* Ex. 1004 at cover. Although the '856 application itself was filed October 27, 2017, it is entitled to claim priority to

Provisional Application No. 62/502,266 (“the ’266 provisional”) filed May 5, 2017), because it (1) contains a priority claim to the ’266 provisional, (2) was filed within 12 months of the filing of the ’266 provisional, and (3) contains a common inventor (Suresh P. Nair). *See id.*; Ex. 1008. Accordingly, Nair was effectively filed May 5, 2017. See 35 U.S.C. § 102(d)(2). Moreover, the ’266 provisional “describes the subject matter” from Nair relied upon in this Petition, which Petitioner demonstrates below by providing, for each citation to Nair (Ex. 1004), a parallel citation to the corresponding disclosure of the ’266 provisional (Ex. 1008) that describes the same subject matter. Nair was not cited during prosecution.

- **3GPP TR 33.899 V1.1.0 (Release 14)** - 3GPP TR 33.899, *Study on the security aspects of the next generation system*, Version 1.1.0 (Release 14) (Ex. 1007, or “TR 33.899”) was published as early as March 2017 and no later than April 13, 2017, and is expressly incorporated by reference in its entirety into Nair, *see* Ex. 1004, ¶[0007]; Ex. 1008, 2:4-9; Ex. 1016 (Declaration of Friedhelm Rodermund), ¶¶ 43–49 (TR33.899 “was available to all 3GPP members and the general public by April 13, 2017”). TR 33.899 V1.1.0 is prior art under 35 U.S.C. §§ 102(a)(1) and, as incorporated into Nair, 102(a)(2). TR 33.899 was cited during prosecution but it was not discussed or applied by the Examiner. Ex. 1009, 95, 131, 192, 199.

- **5G-Ensure Deliverable D3.1, “5G-PPP security enablers technical roadmap”** (Ex. 1010, or “5G-Ensure D3.1”) was published on March 11, 2016. 5G-Ensure D3.1 is prior art under 35 U.S.C. §§ 102(a)(1). 5G-Ensure D3.1 was published and freely available on the 5G Ensure website . . . by March 18, 2016, at the latest.” Ex. 1016, ¶¶ 61–64. A copy of 5G-Ensure D3.1 was captured by the Wayback Machine on May 2, 2016.¹ Ex. 1017.
- **Forsberg** - U.S. Patent Publ. No. 2013/0003971 (Ex. 1005, or “Forsberg”) was filed on September 13, 2012 and was published on January 3, 2013. Forsberg is accordingly prior art under 35 U.S.C. §§ 102(a)(1) and 102(a)(2). Forsberg was cited but not discussed during prosecution. Ex. 1009, 94, 191, 199.
- **Togawa** - U.S. Patent No. 8,005,219 to Togawa (Ex. 1006, or “Togawa”) was filed on July 23, 2007 and issued Aug. 23, 2011. Togawa is prior art under 35 U.S.C. §§ 102(a)(1) and 102(a)(2). Togawa was not before the Patent Office during prosecution.

¹http://web.archive.org/web/20160502230835/http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.1-5G-PPPSecurityEnablersTechnicalRoadmap_early_vision.pdf

- **3GPP TS 23.501 V0.4.0**, entitled “3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 15),” (Ex. 1013, or “TS 23.501”) was published in April 2017, and is expressly incorporated by reference in its entirety into Nair, *see* Ex. 1004, ¶¶0006]; Ex. 1008, 1:26-30. TS 23.501 V0.4.0 is prior art under 35 U.S.C. §§ 102(a)(1) and, as incorporated into Nair, 102(a)(2). TS 23.501 V0.4.0 was “published and freely available on 3GPP’s ftp server by April 20, 2017.” Ex. 1016 ¶¶ 50-57.

B. Relief Requested

Petitioner requests IPR and cancellation of on the following grounds, supported by the Declaration of Harry V. Bims, Ph.D. (Ex. 1002).

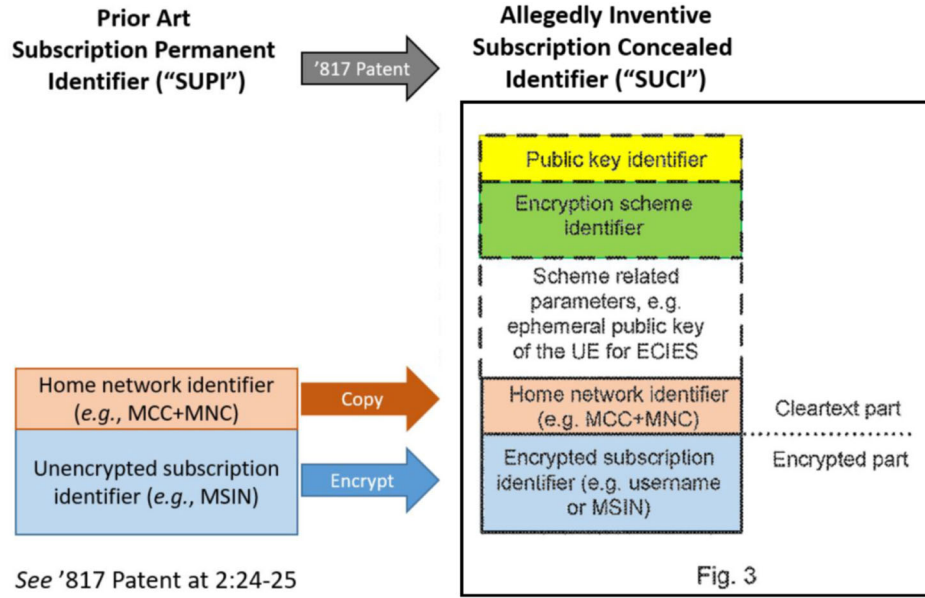
Ground	Basis	Challenged Claims	Reference(s)
1	§103	1-6 and 8-16	Obvious over Nair in light of Forsberg
2	§103	1-6 and 8-16	Obvious over Nair in light of Forsberg and Togawa
3	§103	8, 14	Obvious over Nair in light of Forsberg and 5G-Ensure D3.1
4	§ 103	8, 14	Obvious over Nair in light of Forsberg, Togawa, and 5G-Ensure D3.1

VI. THE '817 PATENT

A. Summary of the Specification

The '817 patent acknowledges the known importance of maintaining the confidentiality of a user equipment's ("UE") "long-term subscription identifier" to keep the user's identity secure. Ex. 1001, 1:22-36. The '817 patent discloses a Subscription Permanent Identifier ("SUPI") and cites a user's IMSI, which was known in the art, as an exemplary SUPI. *Id.*, 1:22-36-43; Ex. 1002, ¶ 24. When a UE, such as a mobile phone, transmits the IMSI through the air in unencrypted or clear text devices called "IMSI catchers" could retrieve the IMSI and thereby allow bad actors to impersonate a subscriber. *Id.*, 1:33-36. The '817 patent admits a known solution to this problem was to encrypt the user's SUPI. *Id.*, 1:22-43; Ex. 1002, ¶ 24).

The '817 patent explains the SUPI is converted into a Subscription Concealed Identifier ("SUCI"), which contains the user-specific field (MSIN) of the SUPI/IMSI in encrypted form. *Id.*, 1:50-61, 5:22-23, 8:62-66, Fig. 3; Ex. 1002, ¶ 25.



Ex. 1002, ¶ 25.

Figure 3 (above) shows the SUCI has both an “encrypted part” and a “cleartext part.” *Id.*, 1:52-56, 8:39-40; Ex. 1002, ¶ 26. The encrypted part contains the MSIN portion of the IMSI (blue above). *Id.*, 2:26-28, 8:62-66. The clear-text part of the SUCI contains the MCC and MNC portions of the IMSI (collectively, “home network identifier”), *id.*, 2:24-29, 7:28-29, 8:41-43. The SUCI also contains other fields in the clear-text part including a field called the “encryption scheme identifier” (green), which indicates the encryption method used to encrypt the MSIN. *Id.*, 2:38-44, 8:44-50. The clear-text portion of the SUCI also contains a “public key identifier.” *Id.*, 1:62-63, 2:1-50, Fig. 3.

The authentication process is shown in Figure 6. *Id.*, 5:47, 10-25-37. During the authentication process, the UE generates a SUCI and transmits it to a server known as the “Authentication and Management Function” (“AMF”). *See id.*, Fig. 6

(step 3), 10:43-45. The AMF then forwards the SUCI to the Authentication Server Function (“AUSF”). *See id.*, Fig. 6 (step 4), 10:45-48. Upon identification of the home network, the AUSF sends an authentication request, along with the SUCI, to a de-concealing server within the UE’s home network. *Id.*, Fig. 6 (step 6), 2:16-19, 11:11-12. The de-concealing server decrypts the SUCI using the scheme indicated by the encryption scheme identifier, and the key identified by the public key identifier to revealing the UE’s SUPI. *Id.*, 2:32-44, 11:17-18.

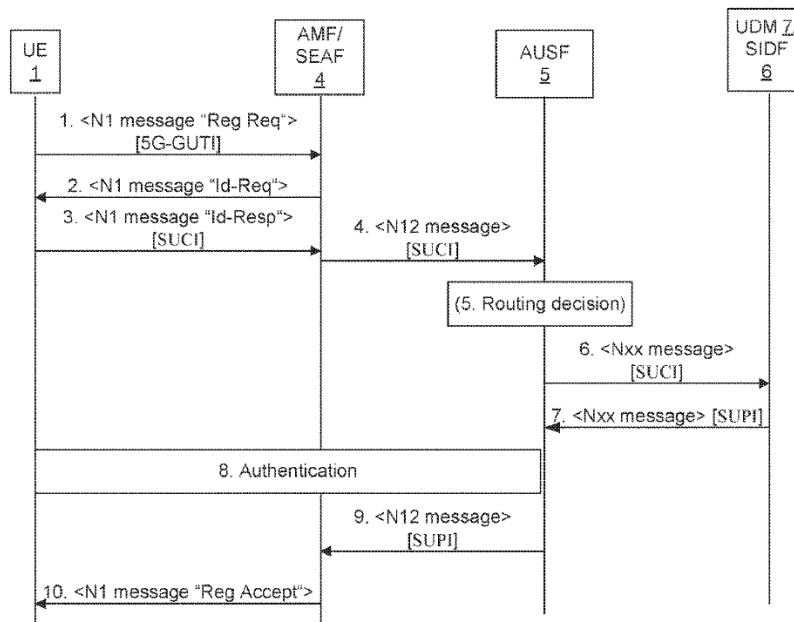


Fig. 6

B. Person of Ordinary Skill in the Art

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. Ex. 1002, ¶ 22. Additional education might compensate for less experience, and vice-versa. *Id.*

VII. CLAIM CONSTRUCTION

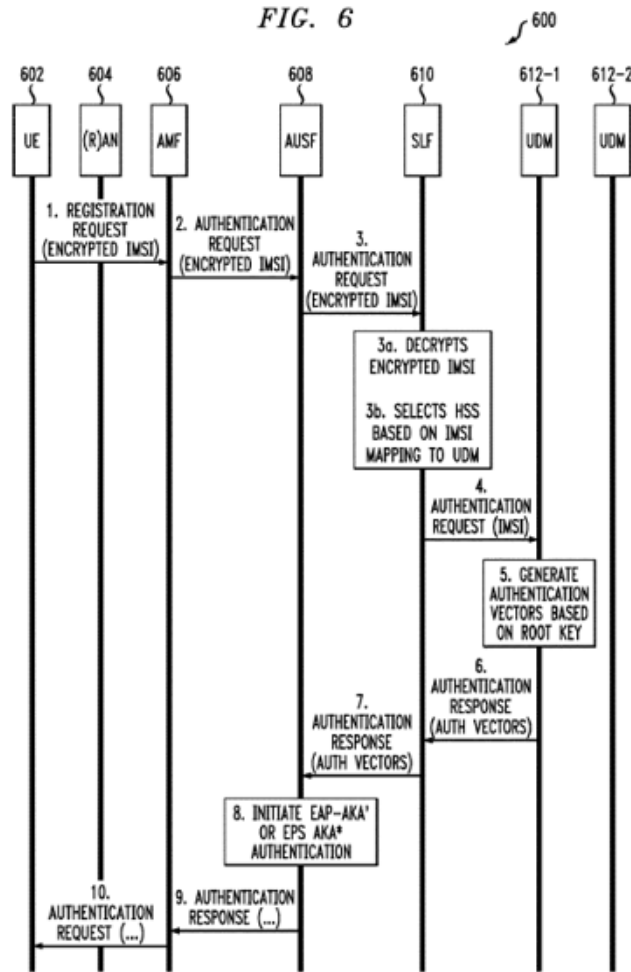
Petitioner submits that the Board does not need to construe any terms to resolve the arguments presented herein.

VIII. OVERVIEW OF PRIOR ART

A. Nair

Nair describes a process for protecting a UE's SUPI during a UE authentication process by encrypting the user-specific information of a UE's IMSI (MSIN), while keeping the remaining information of the IMSI (MNC+MCC) in clear-text so that the transmission can be routed to the correct home network. *Id.*, ¶[0035].

As shown in Nair's Figure 6, a registration request comprising the UE's partially-encrypted IMSI is first transmitted to an Authentication and Security Function (AUSF) along with one or more privacy indicators. *Id.*, ¶[0078].



Ex. 1004, Fig. 6; *see also* Ex. 1008, Fig. 6. The request is then forwarded to a Server Location Function (SLF), which uses the privacy indicators to determine the applicable privacy features (for example, whether the IMSI is encrypted by public key encryption) and decrypt the IMSI. *Id.*, ¶[0078]; *see also id.*, ¶¶[0009-0010], [0013-0014]. Once the SLF, which is a trusted part of the home operator's domain and stores the home network's private key, determines that the IMSI is privacy protected, it determines the appropriate privacy features to process and decrypt the privacy-protected message to obtain the UE's IMSI. *Id.*, ¶¶[0038], [0043].

B. 3GPP TR 33.899 V1.1.0 (Release 14)

TR 33.899, which is incorporated into Nair by reference (Ex. 1004 ¶[0007]; Ex. 1008, 2:4-9), teaches a method of concealing a UE's IMSI using an Elliptic Curve Integrated Encryption Scheme (ECIES). Ex. 1007, §5.7.4.15.1 at 376. ECIES, uses Elliptic Curve Cryptography (ECC) and a symmetric encryption function whereby public and private key pairs are used to generate the encryption key. *Id.*, 285; *see also* Ex. 1011, Abstract. TR 33.899's Figures 5.7.4.15.2-1 and 5.7.4.15.2-2, reproduced below, depict the encryption and decryption processes using ECIES. *Id.*, Figure 5.7.4.15.2-1, Figure 5.7.4.15.2-2.

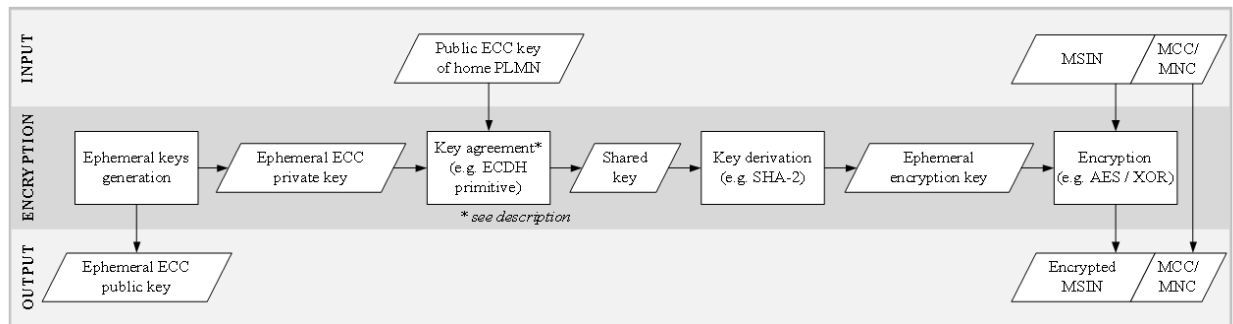


Figure 5.7.4.15.2-1: Encryption at the UE side (based on ECIES)

Id.

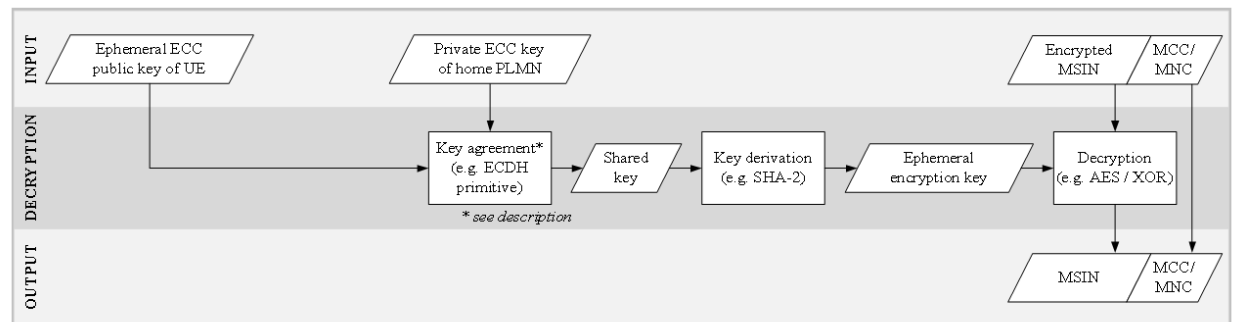


Figure 5.7.4.15.2-2: Decryption at the network side (based on ECIES)

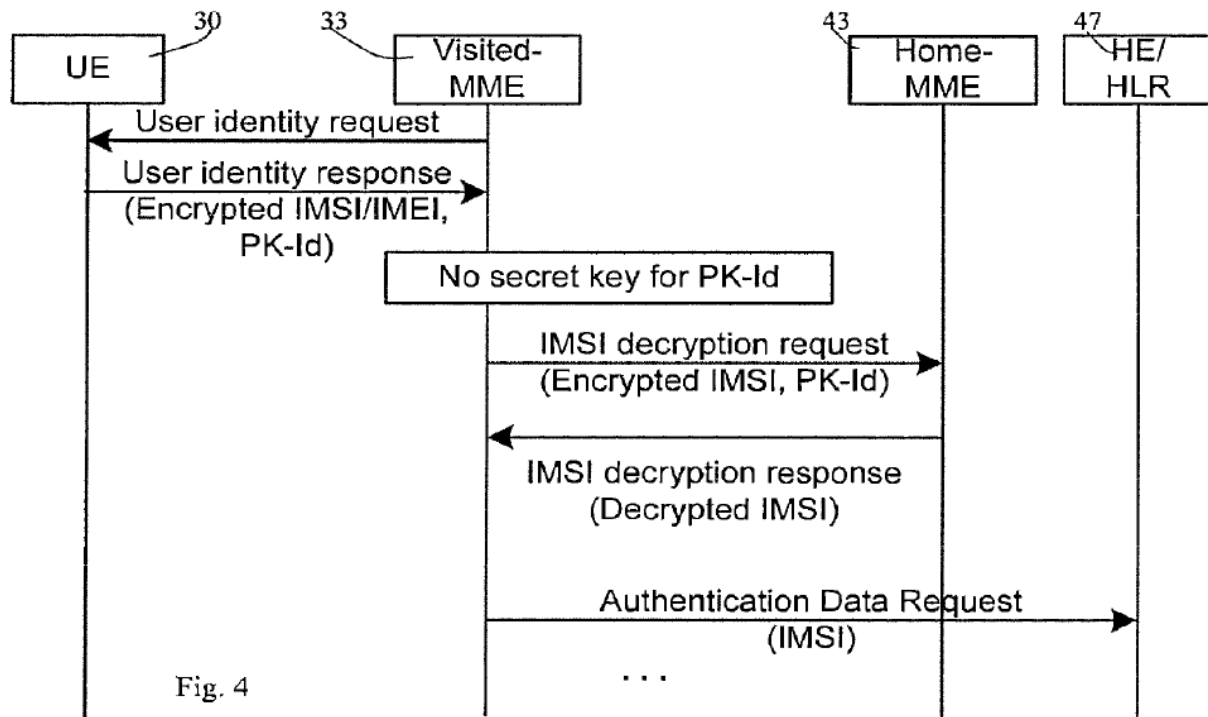
Id.

C. 3GPP TS 23.501 V0.4.0 (Release 15)

TS 23.501, which is incorporated into Nair by reference (Ex. 1004 ¶[0006]; Ex. 1008, 1:26-30), teaches allocating a globally unique Subscriber Permanent Identifier (SUPI) to each UE in a 5G network for determining the UE's home network. Ex. 1013, §5.9.2 at 63. TS 23.501 identifies multiple “valid SUPI types” for use in a 5G network, including: (1) IMSI and (2) a Network Access Identifier (NAI). *Id.* TS 23.501 explains that “[i]n order to enable roaming scenarios, the SUPI shall contains [sic] the address of the home network (e.g. the MMC and MNC in the case of an IMSI based SUPI).” *Id.* It teaches that a “representation of the IMSI [may] [] be contained within the NAI for the SUPI e.g. when used over a non-3GPP Access Technology” and that “[b]y using NAI, it will be possible to also use non-IMSI based SUPIs” in 5G networks. *Id.*

D. Forsberg

Forsberg describes a technique for securing the identity of a UE for transmittal over a network during the process of registering and authenticating the UE for attachment to a communications network. Ex. 1005 ¶[0019]. Forsberg's Fig. 4, reproduced below, depicts a message flow of the UE authentication procedure in one embodiment. *Id.* ¶[0039], Fig. 4.

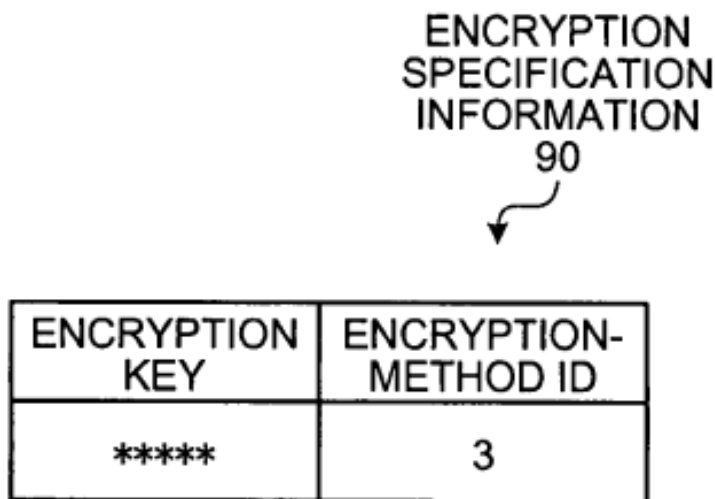


Forsberg discloses a UE that receives a user-identity request from an authentication server (Visited-MME 33 in Figure 4) as part of the process of registering with a communications network. *Id.*, ¶[0048]. The UE responds by sending its identity (including its encrypted IMSI and a public key identifier) to the authentication server. *Id.*, ¶[0049]. The authentication server decrypts the encrypted portions of the UE identity if it is part of the UE's home network. *Id.*, ¶[0050]. Otherwise, the authentication server uses the information in the UE's response (including the UE's associated mobile country code (MCC) or the mobile network code (MNC)) to locate and contact the UE's home network for decryption of the UE's identity. *Id.*, ¶¶[0051], [0053]. The first authentication server (Visited-MME 33) transmits the encrypted IMSI to an authentication server in the UE's home

network (Home-MME 43). *Id.*, ¶[0051]. In response, the home network's authentication server decrypts the UE's IMSI and transmits the unencrypted IMSI back to the first authentication server for use in completing the UE authentication process. *Id.*, ¶[0054], Figs. 2-4.

E. Togawa

Togawa teaches an encryption apparatus and a decryption apparatus for encrypting and decrypting data in accordance with an encryption specification, whereby information on the encryption specification is embedded within transmitted data as shown in Togawa's Fig. 13. Ex. 1006, Fig. 13, 23:17-19 ("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."). Togawa further teaches that the encryption apparatus and decryption apparatus are used in connection with encrypting calls as used in mobile devices. *Id.*, 4:38-42.



Id., Fig. 13.

The embedded information in the transmitted data includes identifying information for both an “encryption key” used to encrypt the transmitted data and an “encryption-method ID.” *Id.*, 23:19-23. Like the encryption scheme identifier of the ’817 patent, the “encryption-method ID” identifies the encryption scheme or method used to encrypt the data. *Id.*, 23:23-25, 23:28-33; 26:31-39.

F. 5G -Ensure Deliverable D3.1, “5G-PPP security enablers technical roadmap” (early version)

5G-Ensure D3.1 teaches a method of protecting user identifiers (*e.g.*, IMSIs) by using encryption. Ex. 1010, 32-33. 5G-Ensure D3.1 further teaches that ABE encryption schemes provide an alternative to overcome the limitations of traditional public encryption schemes where a UE may only be able to connect to its home network by expanding capabilities to include lawful intercept scenarios. *Id.*, 32. Additional advantages of ABE encryption include the ability to encrypt sensitive data such as a UE’s IMSI using a single public key and decryption using different secret private keys in accordance with desired access policies. *Id.* These private keys can then be distributed to Mobile Network Operators (MNO) and Legal Authorities to support lawful interception applications. *Id.*, 33. ABE schemes such as those based on elliptic curve pairings offer the additional benefits of practicality, message randomization, and personalized randomization. *Id.*

5G-Ensure D3.1 also teaches that the public key for ABE encryption schemes is stored on a UE’s Subscriber Identity Module (SIM), and the associated private

key is stored on the network element responsible for decryption using the private key. *Id.* 5G-Ensure D3.1 teaches that another advantage of ABE encryption is the ability to avoid exposing the long-term identifier (*e.g.*, IMSI) within the serving network. *Id.* Finally, 5G-Ensure D3.1 teaches that the Mobile Network Code (MNC) and Mobile Country Code (MCC) would need to be left unencrypted within the identifier to aid the serving network in locating the home network. *Id.*

IX. SPECIFIC GROUNDS FOR PETITION UNDER 37 C.F.R. § 42.104(B)

A. Ground 1: Claims 1-6 and 8-16 Are Rendered Obvious By Nair in Combination with Forsberg

1. Motivation to Combine Nair And Forsberg

A POSITA would have been motivated to combine the complementary teachings of Nair and Forsberg, as explained below and supported by the Declaration of Dr. Harry V. Bims. Ex. 1002, ¶ 45–54.

First, a POSITA would have been motivated to combine Nair and Forsberg because both relate to the same field of invention, providing privacy features and security in transmitting and processing user identifiers within a mobile communication system. Ex. 1004, ¶[0011]; Ex. 1008, 2:16-19; Ex. 1005, ¶[0012]; Ex. 1002, ¶ 46. “When the references are in the same field as that of the applicant’s invention, knowledge thereof is presumed.” *In re Dance*, 160 F.3d 1339 at 1343 (Fed. Cir. 1998). Both Nair and Forsberg recognize and are directed at solving the problem that mobile subscription information numbers (*e.g.*, IMSIs or MSINs) are

susceptible to interception when transmitted in clear-text thereby causing privacy concerns. *See* Ex. 1005, ¶[0011–15]; Ex. 1004, ¶[0027–33]; Ex. 1002, ¶ 46. And both references have the same solution, encrypting the mobile subscription information numbers using public key encryption, as discussed below. Ex. 1002, ¶ 46.

Nair relates to encryption and “privacy indicator[s]” for use in concealment of a UE’s “subscription identifier” during the authentication process. Ex. 1004, ¶[0010]; Ex. 1008, 3:18-20; Ex. 1002, ¶ 46. Similarly, Forsberg teaches a method of protecting the privacy of a UE’s subscription identity during the authentication process via encryption. Ex. 1005, ¶[0020] (“[T]here is provided a method comprising receiving an identifier containing at least one encrypted part at a first network entity, determining a second network entity based on the identifier, and requesting for assistance in decryption of the identifier from the second network entity.”); Ex. 1002, ¶ 46.

Second, a POSITA would have been motivated to reduce the complexities of managing multiple public and private key pairs to support the use of multiple Home Subscription Servers (HSS) within a communications network, as described in Nair, by using public key identifiers, as described in Forsberg. Ex. 1002, ¶ 47. Nair teaches the benefits of using multiple keys during the encryption process to facilitate key mapping to multiple HSSs. Ex. 1004, ¶¶[0035] (“Once the IMSI is identified,

HSS/AuC (where AuC is the Authentication Center part of the HSS) will create authentication vectors (AVs) based on *the distinct shared root key K between a user (subscriber) and the HSS/AuC.*”), [0036] (“An operator in his network may have *implementations of multiple HSSs* which allows him to manage distinct sets of users in different HSSs/UDMs. Because of the multiple HSSs, a Server Location Function (SLF) may be implemented in front of a set of HSSs.”), [0038] (“*the SLF would need to store and use the network private key.*”). A POSITA would have understood the complexities of managing multiple public and private key pairs within an SLF to support the use of multiple HSSs within a communications network. Ex. 1002, ¶ 46-47. A POSITA reading Nair would have been motivated to seek key management techniques such as the use of public key identifiers as taught by Forsberg to support this use of multiple keys and multiple private and public key pairs in the encryption process. Ex. 1002, ¶ 48. After reviewing Forsberg, a POSITA would have understood the benefits of applying public key identifiers as taught by Forsberg to manage the implementation of multiple keys as taught by Nair. Ex. 1002, ¶ 48.

Third, a POSITA would have found it obvious to combine Nair and Forsberg because Nair itself provides a teaching, suggestion, or motivation that would have led a POSITA to combine its teachings with Forsberg to arrive at the combined Nair-Forsberg system. Ex. 1002, ¶ 47. Nair teaches the benefits of using multiple keys during the encryption process to facilitate key mapping to multiple Home

Subscription Servers (HSS), which allows an operator to manage different groups of users in different HSSs/UDMs. Ex. 1004, ¶[0036]; Ex. 1008, 5:7-10. Thus, Nair's teaching of multiple keys to support the implementation of multiple HSSs would lead a POSITA to seek Forsberg for its teachings of an identifier to support this use of multiple keys in the encryption process. A POSITA would have been motivated to consult and apply Forsberg because Forsberg teaches key identifiers to manage multiple keys used in encryption. Ex. 1005 ("The public key and secret key pairs are identified so that the correct secret key can be used to decrypt the IMSI. In this option the user equipment provides public key identifier along with the encrypted IMSI"); Ex. 1002, ¶ 48. Accordingly, a POSITA would have recognized that the combination of Nair's UE authentication system, including the encrypted IMSI, with Forsberg's public key identifier could be accomplished by known methods and would yield predictable results, as discussed in more detail below. *Id.*

Fourth, a POSITA would be motivated to include the decrypted (clear-text) IMSI as part of Nair's authenticator vector as taught by Forsberg, which is discussed below with regard to claim element [1g]). *See infra* at p. 43; Ex. 1002, ¶¶ 52, 97.

Fifth, based on complimentary disclosures in Nair and Forsberg and for the reasons stated above, a POSITA would have recognized that Forsberg's public key identifier could be used to improve a similar system (the combined Nair-Forsberg system) in a similar way (improved public and private key pair management). Ex.

1002, ¶ 53. Likewise, a POSITA would view Nair to be ready for improvement with respect to particular implementations requiring distributed subscriber management across multiple HSSs, and that Forsberg’s public key identifiers would provide that improvement in predictable ways. *Id.* And, a POSITA would have been prompted to try variations of Forsberg in the same field of endeavor—such as by applying it to Nair—based on design incentives (improved subscriber authentication management during the registration process). Ex. 1002, ¶ 53.

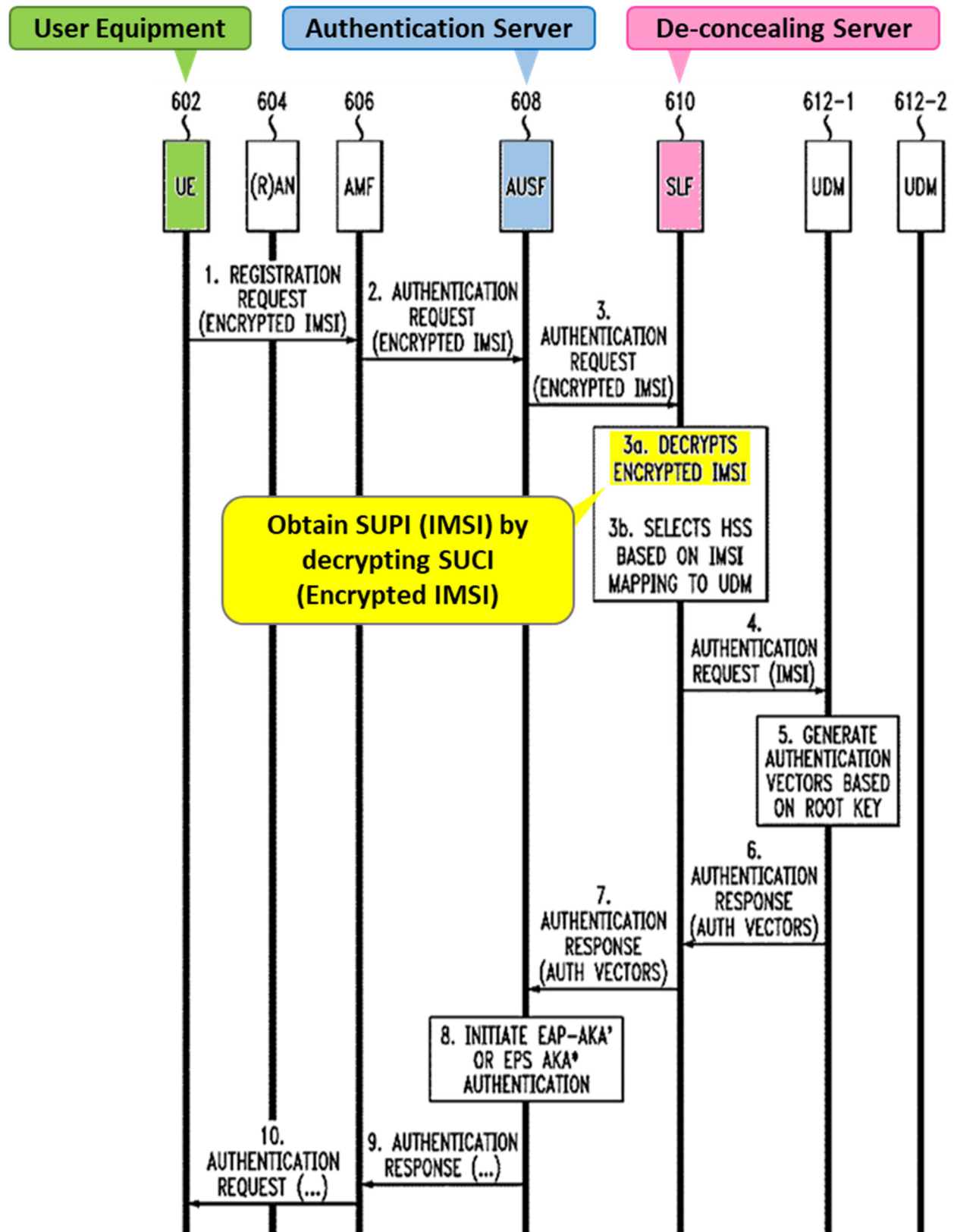
Sixth, a POSITA would have had a reasonable expectation of success in adding Forsberg’s public key identifier functionality to the encryption scheme identifier of the combined Nair-Forsberg system. For example, a POSITA would have understood to use Forsberg’s public key identifier technique in a similar manner as the existing privacy identifier technique of Nair, thus providing for the secure, distributed system taught by the combined Nair-Forsberg system. Ex. 1002, ¶ 53. In the proposed combination, each element merely performs the same function as it does separately. Ex. 1002, ¶ 53. Thus, implementing the known public key identifier technique taught in Forsberg in Nair would amount to applying a known key management technique to a known UE authentication process to yield predictable and improved results.

2. Independent Claim 1

- a. *[Preamble]: A method performed by an authentication server in a home network of a user equipment (UE) for obtaining a subscription permanent identifier (SUPI)*

To the extent that the preamble is limiting, Nair discloses a method performed by an Authentication and Security Function or “AUSF”—the claimed “authentication server”—in a home network of a user equipment (UE) for obtaining an IMSI—the claimed “SUPI.”² Ex. 1002, ¶¶ 55–61. Nair depicts an example of this method in its Figure 6 (annotated below). Ex. 1004, ¶¶[0024], [0077]; Ex. 1008, 13:17-18; Ex. 1002, ¶ 56.

² The ’817 patent confirms the claimed SUPI “may be IMSI-based,” and “may use the IMSI.” Ex. 1001, 8:20-24; Ex. 1004, ¶[0032] (“IMSI[] is a permanent subscription identifier (subscriber identity) of a UE.”).



Ex. 1004, Fig. 6 (annotated); *see also* Ex. 1008, Fig. 6; Ex. 1002, ¶ 56.

As shown above in Figure 6, when the UE wants to register itself on the wireless network, it “sends a registration request” to the home network’s Access and Mobility Management Function (AMF 606) in Step 1. Ex. 1004, ¶[0078]; Ex. 1008, Fig. 6. The UE 602 encrypts its subscriber’s IMSI (SUPI) and includes it in the registration request message sent to the AMF. Ex. 1004, ¶[0078]; Ex. 1008, 4:29-30. The “AMF 606 then sends an authentication request ([containing the] encrypted IMSI) to AUSF 608” in Step 2. Ex. 1004, ¶[0078]; Ex. 1008, 15:22-24, Fig 6. The AUSF is in the home network of the UE. Ex. 1004, ¶[0033]; Ex. 1008, 4:18-22.

The AUSF then in turn “sends the authentication request ([containing the] encrypted IMSI) to SLF 610 [*i.e.*, a de-concealing server as recited in element [1f]].” Ex. 1004, ¶[0078]; Ex. 1008. The claimed SUPI (non-encrypted IMSI) is obtained when the “SLF 610 decrypts the encrypted IMSI.” Ex. 1004, ¶[0078]; Ex. 1008, 5:23-30, Fig. 6. To the extent Patent Owner argues the preamble is limiting and requires that the authentication server obtains the SUPI directly, such a limitation is disclosed by Nair and taught by Nair in view of Forsberg, as discussed below for Element [1g].

Nair’s embodiments of Figures 4 and 5 also demonstrate the claimed method. There, the AMF (Fig. 4) or AMF/MME (Fig. 5) are each an “authentication server” and perform the claimed method for obtaining a SUPI. Ex. 1004, ¶¶[0072-0076]; Ex. 1008 Figs. 4-5. The AMF or AMF/MME receives the registration/attach request

containing an encrypted IMSI³ and sends the authentication request containing the encrypted IMSI to the SLF (de-concealing server), which decrypts the encrypted IMSI to obtain the unencrypted IMSI. Ex. 1004, ¶¶[0072-0076], Figs 4-5; Ex. 1008, Figs. 4-5.

- b. Element [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*

Nair discloses an International Mobile Subscriber Identity, or “IMSI,” that is the claimed SUPI and that meets the recited limitations. *See, e.g.*, Ex. 1004, ¶¶[0042] (“SUPI (Subscription Permanent Identifier of the UE)”), [0079–80]; Ex. 1008, 4:14–

³ Nair generally uses “attach request” to refer to requests to register and authenticate a UE with either of a 5G or mixed LTE/5G network. Ex. 1004, ¶¶[0010], [0014-0016], [0039-0040], [0044-0048]. In reference to Figures 4-6, however, Nair uses the term “registration request” to refer to requests to register with a 5G network and “attach request” to refer to requests to register with a mixed LTE/5G network but discloses that in both cases the requests comprise the UE’s encrypted IMSI and privacy indicators. *Id.* ¶¶[38-39], [0041-0049], [0073], [0076], [0078], Figs. 4-6. Because this difference in nomenclature is irrelevant, Petitioner uses the terms “registration request” and “attach request” interchangeably.

15; Ex. 1002, ¶¶ 62-65. Nair’s IMSI is a permanent subscription identifier . Ex. 1004, ¶[0032] (“[A]n ***International*** Mobile Subscriber Identity (IMSI) is a permanent subscription identifier (subscriber identity) of a UE.”); Ex. 1008, 4:14-15. Moreover, Nair teaches that the use of IMSI as a SUPI that is a globally unique identifier allocated to a subscriber was standard practice in the telecommunications industry. Ex. 1004, ¶¶[0038] (disclosing use of an IMSI as a permanent subscriber identity (*i.e.*, SUPI) in prior art 5G networks), [0042]; Ex. 1008, 4:14-17, 5:24-29; Ex. 1013, §5.9.2 at 63; *see also* Ex. 1002, ¶ 63.

A POSITA would have understood that Nair’s IMSI is a SUPI that also is a globally unique identifier allocated to a subscriber. Ex. 1002, ¶ 63. The ’817 patent confirms the IMSI is a globally unique identifier allocated to a subscriber. Ex. 1001, 1:22-36 (UE’s “long-term subscription identifier (e.g., an IMSI (International Mobile Subscriber Identity)”). As explained in the 3GPP TS 23.501 (V0.4.0), which is expressly incorporated by reference into Nair, (Ex. 1004 ¶[0006]; Ex. 1008, 1:26-30),⁴ “a globally unique 5G Subscription Permanent Identifier (SUPI) shall be allocated to each subscriber in the system,” and identifies “IMSI” “as [a] valid SUPI type[] for this Release [of the 5G standard].” Ex. 1013, §5.9.2 at 63.

⁴ *See Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000).

Further, Nair’s IMSI (SUPI) includes a home network identifier identifying a home network of the subscriber. Specifically, Nair teaches that the IMSI comprises a Mobile Country Code (MCC) and a Mobile Network Code (MNC), collectively a home network identifier. Ex. 1004, ¶¶[0032]; (“IMSI ... consists of a 3-digit Mobile Country Code (MCC) [and] a 3-digit Mobile Network Code (MNC)”), [0035]; Ex. 1008, 4:15-17, 4:29-31; *see also* Ex. 1013, §5.9.2 at 63. Nair’s home network identifier (*i.e.*, the MCC + MNC) is identical to the home network identifier disclosed in the ’817 patent. Ex. 1001, Fig 3 (below), 2:24–29, Cl. 6.

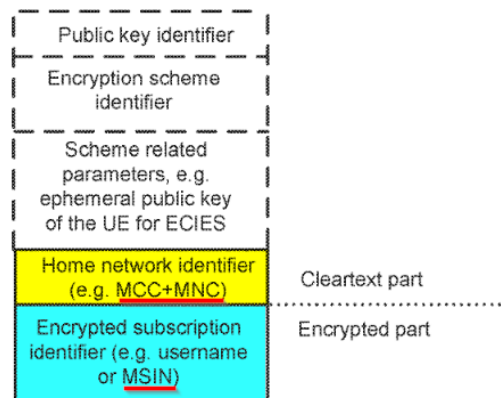


Fig. 3

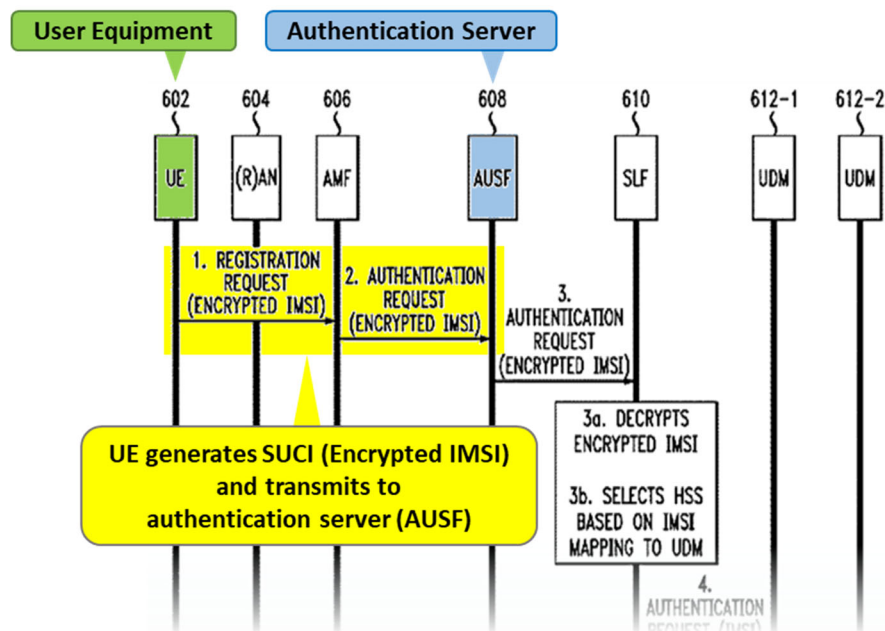
Id.

Further, Nair’s IMSI (*i.e.*, a SUPI) includes a subscription identifier identifying a subscription within the home network. Nair discloses the IMSI includes a 9-digit Mobile Station Identification Number (subscription identifier). Ex. 1004, ¶¶[0032]; (“IMSI ... consists of ... a 9-digit Mobile Station Identification Number (MSIN).”); Ex. 1008, 4:14-17. Again, Nair’s subscription identifier (MSIN) is the

same as that disclosed in the '817 Patent. Ex. 1001, Fig 3 (annotated above), 8:62-66 (“an encrypted subscription identifier, such as an MSIN”), Cl. 6.

c. Element [1c]: the method comprising: the authentication server receiving a subscription concealed identifier (SUCI) generated by the UE

Nair discloses that the authentication server (AUSF) receives a “SUCI” (Nair’s “Encrypted IMSI” and “privacy indicator”) that is generated by the UE. Ex. 1004, Fig. 6, ¶¶[0024], [0077]-[0078]; Ex. 1008, Fig. 6, 4:28-5:1, 13:17-20; Ex. 1002, ¶¶ 66-68.



Ex. 1004, Fig. 6; Ex. 1008, Fig. 6. Figure 6 of Nair is substantially similar to Figure 6 of the '817 Patent. Compare Ex. 1001, Fig. 6, with Ex. 1004, Fig. 6. Both show the UE sending a SUCI (or encrypted IMSI and privacy indicator) to the AUSF via the AMF.

Nair discloses that the UE generates a registration request message and “sends [the] registration request” to the AMF 606 in Step 1. Ex. 1004, ¶[0078]; Ex. 1008, Fig. 6. The registration request generated and sent by the UE 602 includes the “encrypted IMSI” generated by the UE. Ex. 1004, ¶[0078]; Ex. 1008, 4:28-5:1. The AUSF 608 (authentication server) then receives the SUCI generated by the UE (*i.e.*, Encrypted IMSI) in step 2, in which “AMF 606 then sends an authentication request ([containing the] encrypted IMSI [from the UE]) to AUSF 608.” Ex. 1004, ¶[0078]; Ex. 1008, Fig. 6.

Similarly, in the alternate embodiments of Figures 4 and 5, when the UE seeks to register on the wireless network, the UE generates an encrypted IMSI (*i.e.*, SUCI), and “sends a [registration/attach] request ([containing the] encrypted IMSI) ... to AMF 406” or “AMF/MME 506.” Ex. 1004, ¶¶ [0073], [0076], Figs. 4-5; Ex. 1008, Figs. 4-5.

d. Element [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;

Nair in combination with Forsberg discloses this element and renders it obvious. Ex. 1002, ¶¶ 69–88. Nair discloses that an authentication message generated by and sent from the UE (discussed in element 1[c]) includes the “encrypted IMSI” and privacy indicator (together, comprising the SUCI), which comprise both an encrypted part and a non-encrypted (*i.e.*, clear-text) part.⁵ See Ex. 1004, ¶¶[0035] (“**Only** the MSIN **part** [of the IMSI] needs to be **encrypted**, because MNC+MCC is **needed** by the serving network [and is thus in clear-text]”), [0038]

⁵ Nair expressly notes that its use of the term “encrypted IMSI” refers to all of the IMSI and not just the encrypted MSIN portion. Ex. 1004, ¶[0073].

(“decryption of the *MSIN part* of the IMSI.”); [0043] (“*decrypt the MSIN part*”); [0073] (“Note that by referring to encrypted IMSI, this can refer to the portion of the IMSI that is typically encrypted, *e.g., MSIN*, or all or other parts of IMSI.”); Ex. 1008, 4:29-5:1. Nair’s SUCI (including Encrypted IMSI) is generated from a SUPI (IMSI), which comprises an MCC, MNC, and MSIN (discussed in element 1[b]).

a) Encrypted part comprises the subscription identifier: Nair discloses that the encrypted part of the “encrypted IMSI” and privacy indicator information (*i.e.*, SUCI) included in an authentication request comprises the MSIN (*i.e.*, subscription identifier identifying the subscription within the home network, *see* Section IX.A.2.b). *See* Ex. 1004, ¶¶[0035] (“encrypt the subscriber identity, which is, by way of example, the MSIN part of IMSI”), [0038], [0041] (“MSIN is provided in encrypted form”), [0043]; Ex. 1008, 4:29-30, 5:24-26, 6:26-27; Ex. 1002, ¶¶ 71–72.

Encrypted part does not include the home network identifier: Nair also discloses that the encrypted part of the “encrypted IMSI” and privacy indicator information (collectively, the SUCI) included in the authentication request does not include the home network identifier (MNC+MCC). Ex. 1004, ¶[0035] (“Only the MSIN part needs to be encrypted, because MNC+MCC *is needed* by the serving network to route to the correct home network.”), [0038], [0043], [0073]; Ex. 1008, 4:28-5:1. A POSITA would have understood at the time of the alleged invention that

the “home network identifier” must not be encrypted because its purpose is to identify the home network to the serving network. Ex. 1002, ¶¶ 71-72. Encrypting the “home network identifier” would thus defeat the purpose of including it in the SUCI. *Id.* Indeed, Nair discloses this explicitly by stating “MNC+MCC is ***needed*** by the serving network to route to the correct home network.” Ex. 1004, ¶[0035].

b) i) Clear-text part comprises the home network identifier: As discussed above, *see* Section IX.A.2.b, Nair discloses that the clear-text part of the “encrypted IMSI” and privacy indicator information (*i.e.*, SUCI) included in the authentication request generated by the UE comprises the home network identifier (MCC+MCC) in its teaching that the UE encrypts ***only*** the MSIN part of the IMSI, and sends the MNC and MCC portions (*i.e.*, home network identifier) in clear-text rather than in the encrypted part to allow the serving network to identify the UE’s home network. Ex. 1004, ¶¶ [0035], [0038] [0043], [0073]; Ex. 1008, 4:29-5:1; Ex. 1002, ¶¶ 82-87.

b) ii) Clear-text part comprises an encryption scheme identifier: Nair further discloses that the clear-text part of the “encrypted IMSI” and privacy indicator information (*i.e.*, SUCI) included in the authentication request generated by the UE comprises an encryption scheme identifier because Nair teaches inclusion of an “identity privacy flag” (also termed “privacy indicator”) within the UE’s identification message to indicate to the core network whether the MSIN is encrypted, thus serving as an encryption scheme identifier. Ex. 1004, ¶¶[0035],

[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”); [0042] (discussing that the privacy indicator can be explicit or implicit but, in either case, informs the element receiving the SUCI of the “particular encryption algorithm” used to encrypt the MSIN); Ex. 1008, 6:17-18; Ex. 1002, ¶¶ 73–81. Nair discloses both an “‘explicit’ privacy indicator,” such as “a flag or field” and also an “‘implicit’ privacy indicator” in which the network element that receives the SUCI from the UE is informed of the encryption scheme “by the fact that the message is encrypted with a particular encryption algorithm.” Ex. 1004, ¶[0042]. Both the explicit and implicit privacy indicators are an encryption scheme identifier. Ex. 1002, ¶ 74. Nair discloses the privacy indicator is contained in the clear-text of the SUCI by disclosing that the indicator “informs” “the network element/function receiving the message from the UE” that a “particular encryption algorithm” has been used before the SLF even attempts to decrypt the message. Ex. 1004, ¶¶ [0042-0043]; Ex. 1002, ¶ 74

A POSITA would have understood at the time of the alleged invention that Nair’s explicit privacy indicator “identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI,” as required by claim 1. For example, Nair teaches that “[i]f 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.” Ex. 1004, ¶[43] Ex. 1002, ¶ 75..⁶ Nair’s privacy indicator/flag 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. Ex. 1002, ¶ 76. Otherwise, the SLF would be unable to decrypt since decryption requires knowledge of the particular encryption scheme used to encrypt the IMSI. *Id.* The ’817 patent’s example of the scheme identifier relies on both the UE and SLF understanding that “1” means ECIES encryption. Ex. 1001, 9:62-10:20. Likewise, the Nair system necessarily requires that the privacy indicator means the same encryption scheme to both the UE and SLF. Ex. 1002, ¶ 76.

To the extent Patent Owner argues this limitation is not met, a POSITA would have found it obvious for Nair’s privacy indicator to indicate the particular encryption scheme used to encrypt the IMSI for the same reasons expressly identified in Nair, namely, so that the SLF could select the correct decryption scheme on its first attempt to decrypt and thereby reduce processing time and resource consumption. Ex. 1002, ¶¶ 77.

⁶ Nair’s claim 4 discloses the same, reciting “responsive to the flag indicating that the subscription identifier is privacy-protected, removing the privacy protection from the subscription identifier in the attach request.”

Additionally, Nair teaches that an encryption scheme identified by the privacy indicator is the “null-encryption scheme” where the “input equals the output.” Ex. 1004, ¶[0042]; Ex. 1002, ¶ 78. Nair’s privacy indicator is an encryption scheme identifier as it indicates whether either the null-encryption scheme or the other scheme is used. Ex. 1004, ¶[0054] (“SLF 107 [*i.e.*, de-concealing server]... respond[s] to one or more privacy indicators that are set in messages it receives.”); Ex. 1008, 9:23-24; Ex. 1002, ¶ 78. As Dr. Bims’s explains, the ’817 patent expressly discloses that the null-encryption scheme is one encryption scheme that may be identified by the encryption scheme identifier. *See* Ex. 1001, 3:27-28 (“[T]he encryption scheme may be a null-encryption scheme”), 9:11-13, 15:7-9. The ’817 patent also expressly discloses that a field with a value of “0” to indicate null-encryption scheme and “1” to indicate a non-null-encryption scheme is an “encryption scheme identifier.” *See id.*, 10:17-20 & Figs. 4, 5, and 15. Nair’s privacy indicator is therefore the claimed encryption scheme identifier. Ex. 1002, ¶ 78.

Alternatively, Nair’s implicit privacy indicator embodiment also “identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI,” as required by claim 1. ; Ex. 1002, ¶ 79. Nair discloses that its “implicit” privacy indicator will “implicitly reside in the algorithm scheme used (e.g., null-encryption or *an algorithm that actually encrypts a message*),” and will indicate to

the network element receiving the SUCI that “the message is encrypted with a **particular** encryption algorithm.” Ex. 1004, ¶[0042]; Ex. 1008, 6:17-30.

To the extent that Patent Owner argues that an encryption scheme identifier must explicitly identify a particular **non-null** encryption scheme and that Nair’s explicit privacy indicator does not identify a non-null encryption scheme,⁷ it would be obvious to include explicit identification of a **non-null** encryption scheme in light of Nair alone.⁸ Ex. 1002, ¶ 79. As discussed above, the purpose of Nair’s privacy indicator is to give the SLF the information needed to decrypt the IMSI and to save the time and resources that would be wasted if the SLF attempted to use an incorrect encryption scheme. Ex. 1004, ¶¶[0042-43]; Ex. 1002, ¶ 79. A POSITA would thus have been motivated to use a privacy indicator that indicates the scheme used to encrypt the IMSI. Ex. 1002, ¶ 79.

As noted, Nair discloses that the “‘explicit’ privacy indicator” may be “a flag or **field**.” Ex. 1004, ¶¶[0042], [0044] (“identify privacy flag or other privacy indicator”); Ex. 1008, 6:18; Ex. 1002, ¶ 80. Nair uses the term “flag” to refer to a

⁷ As explained above, Nair’s explicit privacy indicator does disclose a particular **non-null** encryption scheme. *See supra* at p. 34-35.

⁸ As discussed in connection with Ground 2, *infra*, this would also be obvious over Nair in light of Togawa.

binary, yes-or-no value. Ex. 1004, ¶¶[0010] (“a flag indicating *whether* [*i.e.*, yes or no] the subscription identifier ... is privacy-protected”), [0043] (referring to the privacy indicator flag as being “set” or “not set,” and making a binary decision based on this value); Ex. 1008, 6:22-23, 6:29-30. Conversely, Nair uses the term “field” to refer to a value that can contain multiple bits, and thus can represent more values than “0” or “1.” *See* Ex. 1004, ¶¶[0046], [0081] (“[P]rivacy indicators can be controlled (e.g., set) by using one *or more* bits.”); Ex. 1008, 8:1-3. Nair also discloses (and it was well known to a POSITA), that multiple non-null-encryption schemes existed. Ex. 1004, ¶[0042]; Ex. 1008, 2:4-8; Ex. 1007 (incorporated by reference into Nair), §5.7.4.10.1 at 360 (disclosing encryption schemes including “Diffie-Hellman Integrated Encryption Scheme” and “Elliptic Curve Integrated Encryption Scheme”), 374 (“Attribute-Based Encryption scheme”); Ex. 1002, ¶ 81. As discussed above, a POSITA would have known that the de-concealing server would need to know the type of encryption used to decrypt of the IMSI. Ex. 1002, ¶ 81. Accordingly, in light of Nair’s disclosure that the explicit privacy indicator may be a multi-valued “field,” in addition to a binary “flag,” it would have been obvious that the explicit privacy indicator would indicate which of the numerous well-known encryption algorithms was used to encrypt the MSIN. Ex. 1002, ¶¶ 80-81.

b) iii) Clear-text part comprises public key identifier: This element is taught by the combination of Nair and Forsberg. Ex. 1002, ¶¶ 82–87. Like Nair,

Forsberg teaches encrypting the MSIN portion of the IMSI, Ex. 1005, ¶[0049], and further discloses that, in the case of a roaming UE, the MME (*i.e.*, authentication server) may analyze the MCC and MNC portions of the IMSI to determine the correct home MME to decrypt the IMSI (*i.e.*, de-concealing server), *id.* ¶[0051]. [0053-0054], implying that, like Nair, the MCC and MNC are not encrypted. Ex. 1002, ¶¶ 83-84. Forsberg also expressly discloses that its UE identification message includes a public key identifier to allow identification of the correct public key needed to decrypt the encrypted IMSI when multiple public keys are associated with a home network. Ex. 1005, ¶¶[0049], [0055] (“In this option ***the user equipment provides public key identifier*** along with the encrypted IMSI (e.g. similar to the key set identifier, KSI).”), [0056] (“[T]he public key and secret key pairs are provided with an identifier [and] [t]he user equipment may then send the identifier with the encrypted IMSI to the visited mobile management entity, and the decryption can be accomplished on these basis [*sic*].”), [0058] (“***key identifier***”); *see also* Figs. 4 & 5 (depicting the transmission of a user identity response comprising encrypted IMSI and a public key identifier (PK-Id)). Thus, Forsberg discloses a SUCI comprising an encrypted subscription identifier (*i.e.*, encrypted MSIN) and a clear-text home identifier (*i.e.*, MCC+MNC) and public-key identifier. Ex. 1002, ¶¶ 85-86.

It would have been obvious to a POSITA, in light of Forsberg, to augment Nair’s SUCI to include in the clear-text part a public key identifier to identify which

specific public key of the home network was used by the UE to encrypt the MSIN, so that the home network could use the appropriate corresponding private key for decryption in networks that used multiple public keys.⁹ Ex. 1002, ¶ 87.

As Dr. Bims explains, home networks that use multiple public/private key pairs enhance security because, even if one private key is compromised, messages encrypted using other keys will remain protected. Ex. 1002, ¶ 49. A POSITA would have found it obvious to use the secure process disclosed in Nair to authenticate UE's with home networks utilizing multiple public/private key pairs, such as those disclosed in Forsberg, to further enhance the privacy of a UE's subscription identifier. *Id.*, ¶¶ 49-50. Further, it would have been obvious to apply Forsberg's public key identifier to Nair because a POSITA applying Nair to home networks using multiple public/private key pairs would have been motivated to seek methods of managing multiple public keys as taught by Forsberg. *Id.*, ¶ 47. As Dr. Bims further explains, upon consultation with Forsberg, the benefits of applying public

⁹ Nair expressly notes that its use of "encrypted IMSI" refers to all of the ISMI and not just the encrypted portion. Ex. 1004, ¶ [0073]. Accordingly, a POSITA would understand the "encrypted IMSI" includes a clear-text portion, as discussed above. Ex. 1002, ¶ 70.

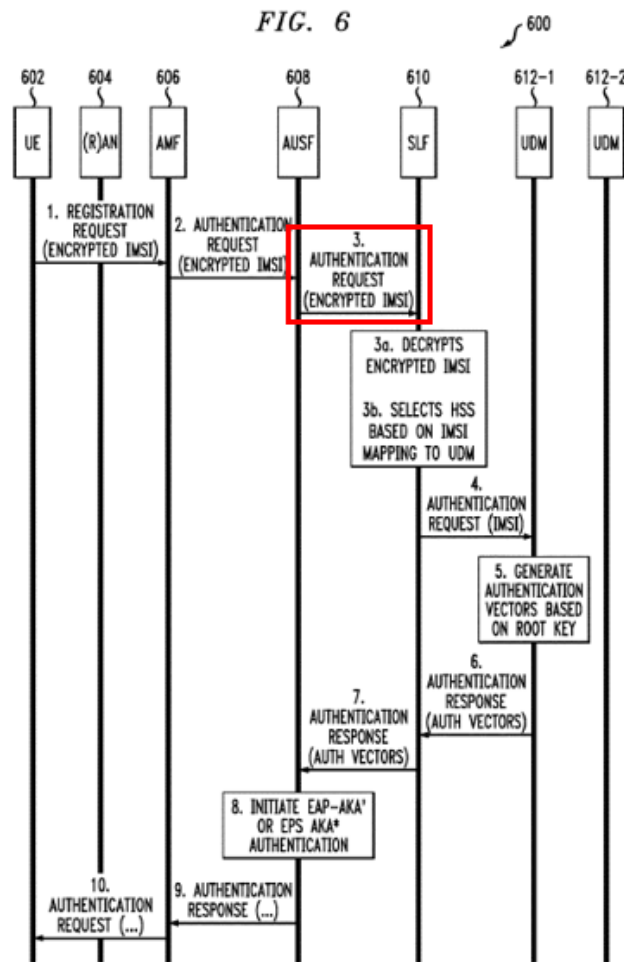
key identifiers to Nair would have been an obvious solution to track and manage multiple keys as taught by Forsberg. *Id.*, ¶ 47; *see also* Section IX.A.1, *supra*.

Clear-text part does not comprise subscriber identifier: Nair teaches that the clear-text part of the SUCI (Encrypted IMSI) generated by the UE does not comprise the MSIN (*i.e.*, subscriber identifier). Ex. 1004 ¶¶[0035] (“MSIN part *needs* to be encrypted”), [0073], [0076], [0078]; Ex. 1008, 4:30, 6:25-28; Ex. 1002 ¶ 88.

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

Nair discloses this element. Nair teaches that the authentication server (AUSF) may determine a de-concealing server (*i.e.*, SLF) to decrypt the encrypted part of the SUCI and send the SUCI to the SLF, which decrypts the encrypted part of the SUCI in accordance with Figure 6. Ex. 1004 ¶ [0078] (“In step 3, AUSF 608 sends the authentication request (encrypted IMSI) to SLF 610. In step 3a, SLF 610 decrypts the encrypted IMSI.”), Fig. 6; Ex. 1008, 5:9-10, 5:24-26, Fig. 6. Nair teaches that its cellular network can have multiple SLF’s. Ex. 1004, ¶¶[0057], [0067], [0085]; Ex. 1008, 10:14–20. A POSITA would, therefore, have understood that the AUSF would necessarily determine which SLF to use for decryption in a multi-SLF system to make the authentication request. Ex. 1002, ¶ 89. Moreover, to the extent Patent Owner argues that Nair does not inherently disclose this feature, it

would have been obvious to a POSITA for the AUSF to make that determination for the same reason. Ex. 1002, ¶ 90.



Ex. 1004, Fig. 6 (annotated); *see also* Ex. 1008, Fig. 6.

Nair's other embodiments, depicted in Nair's Figures 4 and 5, similarly disclose or render obvious this element for the same reasons. Ex. 1004, ¶¶[0072-76], Figs. 4 & 5; Ex. 1008, Figs. 4 & 5; Ex. 1002, ¶ 91.

f. Element [1f]: the authentication server sending the SUCI to the de-concealing server;

Nair discloses this element. Ex. 1002, ¶ 92-93. Nair teaches that the AUSF (authentication server) sends the encrypted IMSI (SUCI) to the SLF (de-concealing server), which decrypts the encrypted IMSI. Ex. 1004 ¶¶[0078], Fig. 6, *see also* ¶ [0038]; Ex. 1008, 13:18-20, Figs. 4-6; Ex. 1002, ¶ 92. Nair's other embodiments, depicted in Nair's Figure 4 and 5, also disclose this limitation. Ex. 1004, ¶¶[0072-76]; Ex. 1008, Figs. 4 & 5. Ex. 1002, ¶ 93.

g. Element [1g]: and after the authentication server sends the SUCI to the de-concealing server, the authentication server receiving the SUPI in response.

Nair in view of Forsberg teaches this element. Ex. 1002, ¶¶ 94-97. Nair discloses that an SLF (*i.e.*, de-concealing server) provides authentication vectors to an AUSF (*i.e.*, authentication server) after decryption of the IMSI as depicted in Fig. 6. Ex. 1004, ¶¶[0078], Fig. 6; Ex. 1008, 5:8-9, 9:17-20, Fig. 6. Ex. 1002, ¶ 95. Nair's other embodiments, depicted in Nair's Figures 4 and 5, similarly disclose an SLF providing authentication vectors to an AMF (Fig. 4) or AMF/MME (Fig. 5) after decryption. Ex. 1004, ¶¶[0072-76].

Forsberg teaches that upon receiving the UE's encrypted IMSI, the visited MME (authentication server) sends an decryption request to the UE's home network via message 3, which contains the encrypted IMSI (SUCI). Ex. 1005, ¶[0051] ("In accordance with an embodiment the visited mobile management entity *asks the*

home mobile management entity to decrypt the IMSI on its behalf.”), Fig. 4. “The *decrypted identifier* is then sent in clear format” back to the authentication server. *Id.*, ¶¶[0047], [0054] (“*send the IMSI in a clear text format* back”), Figs. 3 & 4.

In view of the teachings of Forsberg, a POSITA would have been motivated to include the decrypted IMSI in (or along with) the authentication vectors sent by Nair’s SLF (Figs. 4-6) to the AUSF (Fig. 6), AMF (Fig. 4), or AMF/MME (Fig. 5) (authentication servers) to aid in decryption. Ex. 1002, ¶ 97. As Forsberg explains, the decrypted identifier is sent back to aid in the “authentication of a visiting user equipment.” Ex. 1005, ¶[0047]; Ex. 1002, ¶ 97. The decrypted SUPI is used to route the authentication vectors to the requesting UE associated with the SUPI more accurately and expeditiously. Ex. 1002, ¶ 97. A POSITA would be motivated to apply that benefit to Nair’s system. *Id.* The combination represents combining prior art elements (Nair’s authentication method and system with Forsberg’s method of transferring the decrypted identifier back to the authentication server) according to known methods to yield predictable results (authenticating a visiting UE). *Id.*

3. Dependent Claim 2

- a. *The method of claim 1, wherein the de-concealing server is one of a plurality of de-concealing servers, and the determining of the de-concealing server is based on information received from the UE.*

See Section IX.A.2 for disclosure of claim 1. Nair and Forsberg each disclose this claim element. Ex. 1002, ¶¶ 98-102. Nair discloses multiple SLFs (*i.e.*, a

plurality of de-concealing servers) because Nair teaches that there may be larger numbers of SLF elements. Ex. 1004, ¶[0057] (“[A]lthough only single [] **SLF**[] element[] [is] shown in the FIG. 1 embodiment, this is for simplicity and clarity of description only. A given alternative embodiment ***may of course include larger numbers of such system elements.***”); Ex. 1008, 10:14-20.

Nair also teaches that information received from the UE is used to determine the SLF. Specifically, Nair discloses that the unencrypted MNC and MCC provided in the UE’s authentication request is used to route to request to the correct home network. Ex. 1004, ¶¶[0035] (“MNC+MCC is needed by the serving network to ***route to the correct home network.***”), [0037]; Ex. 1008, 4:29-5:2, 5:9-10. A POSITA would have understood that when a system includes multiple SLFs and multiple home networks, as Nair expressly contemplates, Ex. 1004, ¶[0057], routing an authentication request to the correct home network using the UE’s MCC and MNC would require first determining the SLF configured to provide the UE information to that home network. Ex. 1002, ¶ 99.

This limitation is additionally rendered obvious by Nair in view of Forsberg. Ex. 1002, ¶ 100-102. Forsberg teaches that a mobile management entity may determine the UE’s home mobile management entity by analyzing network information received from the UE, including the UE’s mobile country code (MCC)

and mobile network code (MNC). Ex. 1005, ¶¶[0053]; [0051]; *see also* Section VIII.E *supra*.

Specifically, Forsberg discloses a UE that receives a user-identity request from the Visited-MME in Forsberg's Figure 4 (*i.e.*, the authentication server) as part of the process of registering with a communications network. *Id.*, ¶[0048]. The UE responds by sending its identity (including its encrypted IMSI and a public key identifier) to the Visited-MME. *Id.*, ¶[0049]. If the Visited-MME is part of the UE's home network, it decrypts the encrypted portions of the IMSI. *Id.*, ¶[0050]. If the Visited-MME is not part of the UE's home network, it uses the information in the UE's response (including the UE's associated mobile country code (MCC) or the mobile network code (MNC)) to determine and contact the UE's home network (Home-MME in Figure 3) for decryption of the UE's identity. *Id.*, ¶¶[0051], [0053]. In response, the Home-MME (*i.e.*, de-concealing server) decrypts the UE's IMSI and transmits the unencrypted IMSI back to the Visited-MME for use in completing the UE authentication process. *Id.*, ¶[0054]; *see also* Figs. 2-4.

A POSITA would have found it obvious to incorporate the functionality taught by Forsberg into Nair. As Dr. Bims explains, using information from the UE to determine one of a plurality of de-concealing servers to decrypt a UE's IMSI would beneficially allow the authentication server to identify the proper de-concealing server when the UE is not on a home network. Ex. 1002, ¶ 100-102. The

combination thus represents combining prior art elements according to known methods to yield predictable results. *Id.*

4. Dependent Claim 3

- a. The method of claim 1, further comprising receiving the SUCI from the UE as part of a registration procedure for registering the UE with a wireless communication network.*

See Section IX.A.2 for disclosure of claim 1. Nair discloses this element. Ex. 1002, ¶ 103. Nair discloses a technique for transmitting a SUCI (Encrypted IMSI) as part of an attach request for registering a UE with a communications network, *see* Section IX.A.2.a, including 5G wireless networks. Ex. 1004, ¶¶ [0004-0005], [0006], [0026], [0057], [0076], [0078], Figs. 1 & 6; Ex. 1008, 1:12-2:4, 2:22-23, 10:14-15, 13:17-20, Figs. 1 & 6.

5. Dependent Claim 4

- a. The method of claim 1, further comprising receiving the SUCI from the UE via an authentication request from a Security Anchor Function.*

See Section IX.A.2 for disclosure of claim 1. Nair discloses this claim element. Ex. 1002, ¶¶ 104-105. Nair's Figure 6 discloses an AUSF (*i.e.*, authentication server) receiving an authentication request comprising encrypted IMSI (*i.e.*, SUCI) from an AMF, which Nair discloses implements a Security Anchor Function (SEAF). Ex. 1004, ¶¶ [0077-0078], Fig. 6; *see also* Figs. 4 & Fig. 5; Ex. 1008, Figs. 4-6.

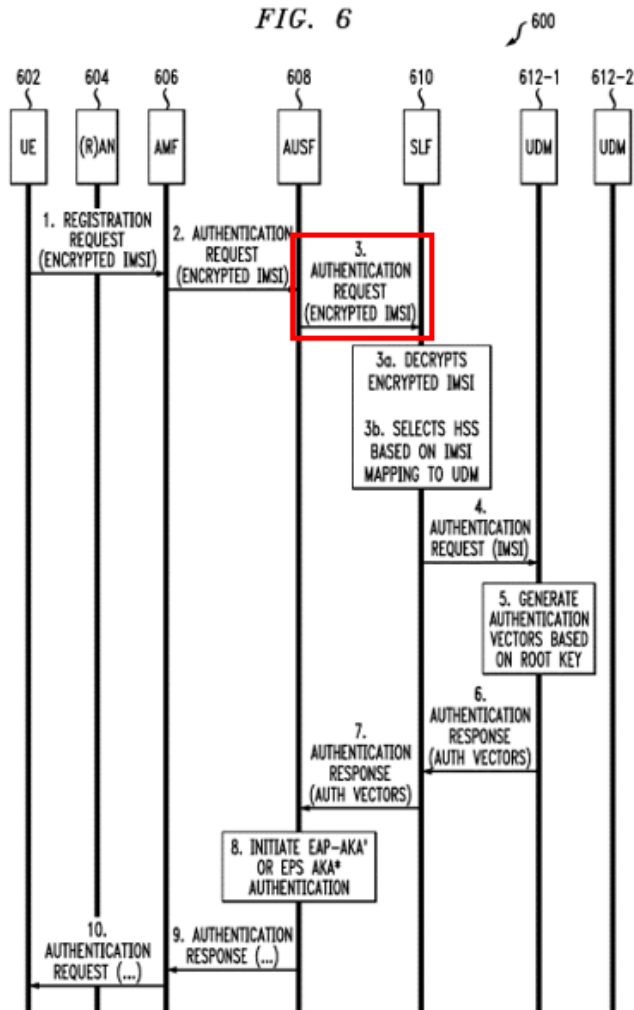
Nair further teaches that in embodiments wherein the UE authentication request includes privacy indicators (*i.e.*, enhanced attach requests), an “MME/SEAF” (Security Anchor Function) “handle[s] the enhanced initial attach message from the UE.” Ex. 1004, ¶[0046]; Ex. 1008, 7:29-8:1. Nair further teaches that the SEAF may be implemented with the Access and Mobility Management Function (AMF), which handles authentication operations with the UE in a 5G network. Ex. 1004, ¶[0053]; Ex. 1008, 9:14-21; *see also* Ex. 1013, §6.2.1 at 75 (“Access and Mobility Management function (AMF) includes ... Security Anchor Function (SEA),” which “interacts with the AUSF and the UE.”). As shown in Nair’s Figure 6, the AMF then sends the encrypted IMSI (*i.e.*, SUCI) to the AUSF (*i.e.*, authentication server) as part of an authentication request. Accordingly, Nair discloses that when the AUSF (*i.e.*, authentication server) receives the SUCI from the UE via an authentication request, that request is specifically from the Security Anchor Function of the AMF, which is responsible for handling such interaction. Ex. 1002, ¶ 105.

6. Dependent Claim 5

- a. The method of claim 1, further comprising sending the SUCI and a request for an authentication vector for authenticating the UE to the determined de-concealing server in the same message.*

See Section IX.A.2 for disclosure of claim 1. Nair discloses this element. Ex. 1002, ¶¶ 106-108. Nair teaches a UE authentication procedure for a 5G network in

which the encrypted IMSI (*i.e.*, SUCI) and a request for authentication vectors for authenticating the UE are sent together within message 3 to the SLF (*i.e.*, de-concealing server) as depicted in Fig. 6. Ex. 1004, Fig. 6; Ex. 1008, Fig. 6.



Nair teaches that the home operator may “split” subscribers among a multitude of HSSs. Ex. 1004, ¶[0038]; Ex. 1008, 5:23. Nair further teaches that in this embodiment, the SLF receives the authentication request and the encrypted IMSI (*i.e.*, SUCI) in message 3 depicted in Fig. 6, decrypts the MSIN part of the

IMSI, and forwards the authentication request to the UE's HSS (the UDM in Fig. 6), which responds to the authentication request by generating and returning authentication vectors. Ex. 1004, ¶¶[0038], [0078]; Ex. 1008, 5:24-29, Fig. 6. Accordingly, Nair discloses sending the SUCI and a request for an authentication vector (*i.e.*, the authentication request) for authenticating the UE to the determined de-concealing server in the same message. Ex. 1002, ¶¶ 107-108.

7. Dependent Claim 6

- a. *The method of claim 1, wherein the home network identifier consists of a Mobile Country Code, and a Mobile Network Code, and*

See Section IX.A.2 for disclosure of claim 1. As discussed in connection with element 1[b], Nair discloses that the SUPI (*e.g.*, the 15-digit IMSI) comprises a home network identifier that includes the user's Mobile Country Code and Mobile Network Code. *See* Ex. 1004, ¶¶[0032], [0035] (“[T]he IMSI is a fixed 15-digit length and consists of a 3-digit **Mobile Country Code (MCC)**, a 3-digit **Mobile Network Code (MNC)**.”); Ex. 1008, 4:14-17, 4:30-5:1; *see also* Ex. 1007, §5.7.3.9.1 at 341.

- b. *the subscription identifier is a Mobile Subscription Identification Number (MSIN).*

As discussed in connection with element 1[b], each of Nair and Forsberg disclose that the SUPI (*e.g.*, the 15-digit IMSI) comprises a subscriber identifier. The subscriber identifier of the UE is a 9-digit MSIN. *See* Ex. 1004, ¶[0032] (“[T]he

IMSI is a fixed 15-digit length and consists of . . . a 9-digit ***Mobile Station Identification (MSIN)***.”); Ex. 1008, 4:14-17; *see also* Ex. 1007, §5.7.3.9.1 at 341 (“IMSI is composed of three parts ... [3] Mobile Subscriber Identification Number (MSIN) identifying the mobile subscriber within a PLMN.”).

9. Dependent Claim 8

c. The method of claim 1, wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme (ECIES).

See Section IX.A.2 for disclosure of claim 1. Nair discloses this element because Nair incorporates by reference in its entirety 3GPP TR 33.899 V1.1.0 (Release 14) (Ex. 1004, ¶[0007]; Ex. 1008, 2:4-9), which teaches concealment of the MSIN portion of a UE’s IMSI using an Elliptic Curve Integrated Encryption Scheme (ECIES) to address the same problem addressed by Nair, Ex. 1004, ¶[0007], namely securing permanent subscriber identifiers using public key encryption. Ex. 1007, §§5.7.4.15 at 376-77, 5.7.4.3.2.2 at 344; Ex. 1002, ¶ 111. TR 33.899 further teaches that ECIES is a public key encryption scheme that uses Elliptic Curve Cryptography (ECC) and a symmetric encryption function whereby public and private key pairs are used to generate the encryption key in accordance with the process depicted in its Figures 5.7.4.15.2-1 and 5.7.4.15.2-2. *Id.*, 285, Fig. 5.7.4.15.2-1, Fig. 5.7.4.15.2-2.

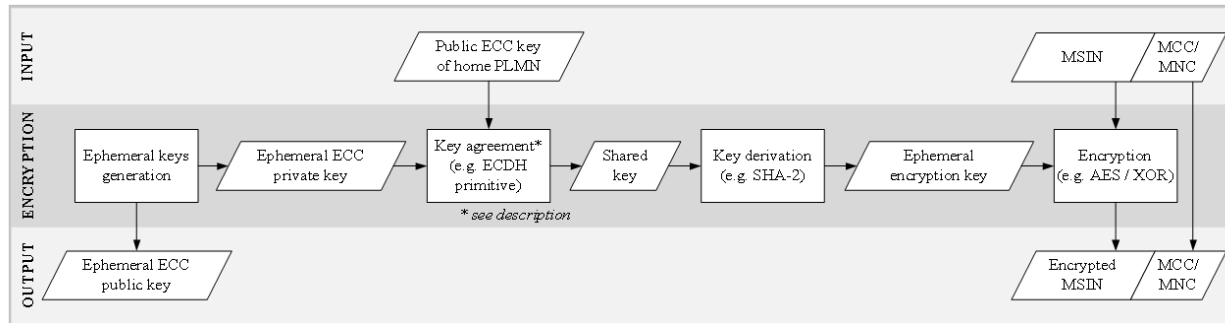


Figure 5.7.4.15.2-1: Encryption at the UE side (based on ECIES)

Id., Figure 5.7.4.15.2-1.

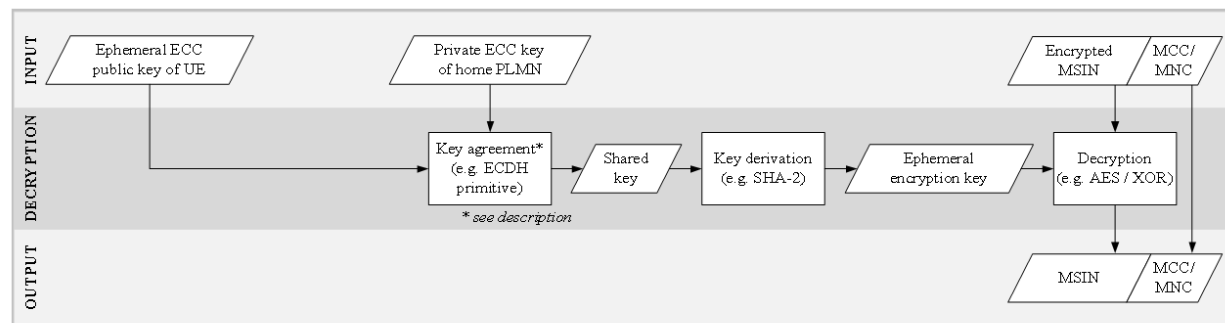


Figure 5.7.4.15.2-2: Decryption at the network side (based on ECIES)

Id., Figure 5.7.4.15.2-1.

10. Independent Claim 9

- a. *Preamble: A method, performed by a de-concealing server, for providing a subscription permanent identifier (SUPI) to an authentication server*

Nair in combination with Forsberg discloses the preamble for the reasons discussed above with regard to Elements [1a] and [1g].

- b. Element 9[b]: 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*

See element 1[b].

- c. Element 9[c]: the method comprising: the de-concealing server receiving, from the authentication server, a subscription concealed identifier (SUCI) generated by the UE*

See element 1[c] (discussing the UE sending the SUCI to the authentication server) and element 1[f] (discussing the authentication server sending the SUCI that it received from the UE to the de-concealing server).

- d. Element 9[d]: wherein the SUCI comprises an encrypted part and a clear-text part ...*

See element 1[d].

- e. Element 9[e]: the de-concealing server decrypting the encrypted part of the SUCI, using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI*

Nair discloses a de-concealing server that decrypts the encrypted part of the SUCI (see element 1[e]) using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI (see element 1[d][b][ii]).

- f. Element 9[f]: and the de-concealing server sending the SUPI to the authentication server.*

See element 1[g].

11. Independent Claim 10

- a. *[Preamble]: A method performed by a user equipment (UE) for concealing a subscription permanent identifier (SUPI)*

Nair discloses this element because Nair teaches a method whereby a UE sends the UE's IMSI (*i.e.*, SUPI) in concealed/encrypted form (*i.e.*, Nair's encrypted IMSI, which is the claimed SUCI) to an AMF (*i.e.*, authentication server) as depicted in Fig. 6. *See* claim 10 and elements 1[a]-[d]; Ex. 1002, Claim 10.

- b. *Element [10b]: 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*

See element 1[b].

- c. *Element 10[c]: the UE generating a subscription concealed identifier (SUCI)*

See element 1[c].

- d. *Element 10[d]: [a subscription concealed identifier (SUCI)] which comprises an encrypted part and a clear-text part...*

See element 1[d].

- e. *Element 10[e]: 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.*

See elements 1[c] (discussing the transmission of the SUCI generated by the UE to an authentication server) and 1[f] (discussing the forwarding of the SUCI by the authentication server to the de-concealing server).

12. Dependent Claim 11

- a. The method of claim 10, wherein the SUCI is transmitted in a request to register with a wireless communication network (30).*

See claim 3.

13. Dependent Claim 12

- a. The method of claim 10, wherein generating the SUCI comprises using a tamper resistant secure hardware component of the UE to generate the SUCI.*

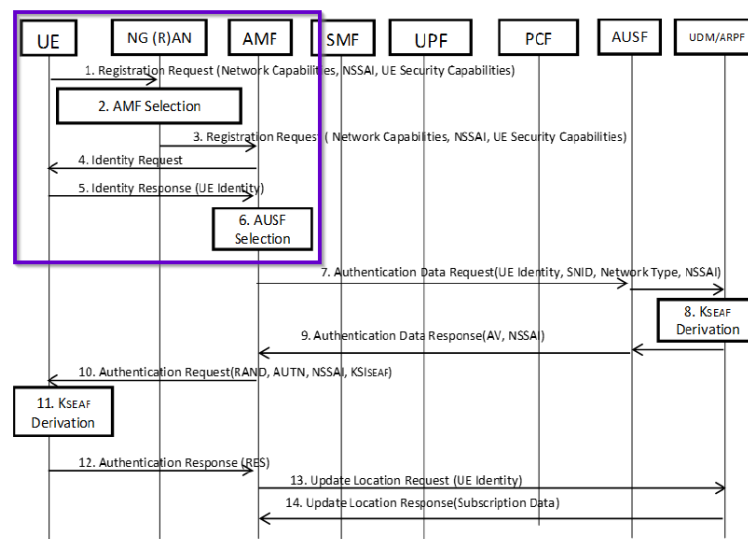
See Section IX.A.9 for disclosure of claim 10. Nair discloses this limitation because Nair discloses that the UE is comprised of a hardware component called a “Universal Integrated Circuit Card (UICC),” which itself “contains at least one Universal Subscriber Identity Module (USIM) and appropriate application software.” Ex. 1004, ¶[0051]; Ex. 1008, 9:2-4; Ex. 1002, ¶ 121. “The USIM securely [*i.e.*, in a tamper-resistant manner] stores the International Mobile Subscriber Identity (IMSI) number and its related key, which are used to identify and authenticate subscribers to access networks.” Ex. 1004, ¶[0051]; Ex. 1008, 9:4-6. Security features of the USIM are well known in the art and required for compliance with technical standard 3GPP TR 33.899. Ex. 1002, ¶ 121; Ex. 1007, §5.5.4.1.2 at 323 (“[S]ubscription credentials . . . *shall always be stored and processed in a tamper resistant secure hardware solution.*”). A POSITA would understand that storing and “process[ing]” the subscription credentials, *i.e.*, the IMSI, using a USIM includes generating an encrypted version of the IMSI (*i.e.*, a SUCI), therefore

generating the SUCI comprising using a tamper resistant secure hardware component to generate the SUC. Ex. 1002, ¶ 121.

14. Dependent Claim 13

- a. *The method of claim 10, wherein transmitting the SUCI to the authentication server comprises transmitting the SUCI to the authentication server in response to an identifier request message received from an Authentication and Mobility management Function, AMF, as part of a procedure for registering the UE with a wireless communication network.*

See Section IX.A.9 for disclosure of claim 10. Nair discloses this limitation. Nair teaches an AMF performs a mobility management function for a communications system in a 5G network. Ex. 1004, ¶[0053]; Ex. 1008, 9:14-17; Ex. 1002, ¶¶ 122-26. Nair discloses this limitation through its incorporation of TR 33.899, which describes how to register a UE with a wireless communication network using the AMF. For example, TR 33.899’s Figure 5.1.4.30.2-1 shows the “call flow for registration procedure of non-roaming scenario.”



Ex. 1007, § 5.1.4.30.2 at 119, Fig. 5.1.4.30.2-1. The figure shows that UE sends a registration request to the AMF, which then “sends the Identity Request to the UE.” *Id.* In response, the “UE sends the Identity Response (UE Identity) to the AMF.” *Id.* at 120. A POSITA would have understood TR 33.899’s registration request as the “registration request” (or “attach request”) in Nair. Ex. 1004, ¶[0078], Fig. 6. Ex. 1002, ¶ 123. As discussed above for claim elements 1[c] and 1[d], Nair discloses transmitting the SUCI to the authentication server as part of the registration request.

Forsberg also teaches that the MME requests the UE to send the UE’s identity as part of a procedure for registering the UE with the communications network. Ex. 1005, ¶[0048], Figs. 4 & 5. In response, the UE sends the UE’s associated IMEI and IMSI to the MME. *Id.*, ¶[0049], Figs. 4 & 5. Forsberg further teaches that this UE identity response may also include additional information such as public key identifiers, and that the UE conceals its subscription identifier by encrypting at least its mobile subscription identification number (MSIN). *Id.*, ¶[0049]. As explained in Nair, in a 5G system, the MME functionality is performed in the AMF. Ex. 1004, ¶[0053]; Ex. 1008, 9:14-17.

As explained above in reference to element 1[d][b][iii], a POSITA would have been motivated in light of Forsberg to use Nair’s authentication process with home networks that utilize more than one public-private key pair for enhanced security. Ex. 1002, ¶¶ 49, 52, 87, 97, 126. In the context of such a network, a POSITA would

have been motivated in light of Forsberg to include as part of Nair's authentication process Forsberg's identifier request so that Nair's UE would include in its response to the AMF public key identifier information along with the encrypted IMSI and privacy flag indicator (*i.e.*, SUCI). Ex. 1002, ¶¶ 45–54, 126. *See also* element 4[a]; Section IX.A.1.

15. Dependent Claim 14

- a. The method of claim 10, wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme.*

See Sections IX.A.9 and IX.A.9 claim 8.

16. Independent Claim 15

- a. [Preamble]: A user equipment (UE) for concealing a subscription permanent identifier (SUPI),*

Nair discloses a user equipment (UE) for encrypting (*i.e.*, concealing) the UE's IMSI (*i.e.*, SUPI). *See* element 1[a]-1[c].

- b. Element 15[b]: wherein the SUPI is a globally unique identifier allocated to a subscriber and the SUPI comprises a home network identifier identifying the home network of the subscriber and a subscription identifier identifying a subscription within the home network,*

See element 1[b].

- c. Element 15[c]: [the UE comprising] processing circuitry and memory circuitry, the memory circuitry containing instructions executable by the processing circuitry,*

Nair discloses the recited “processing circuitry and memory circuitry.” *See* Ex. 1004, ¶¶ [0050], [0084-0085]; Ex. 1008, 2:24-27, 14:10-22.

- d. Element 15[d]: wherein the UE is operative to generate a subscription concealed identifier (SUCI)...*

See elements 1[c]-1[d].

- e. Element 15[e]: [and wherein the UE is operative to] transmit the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the SUCI*

See elements 1[c], 1[e], and 1[f].

17. Dependent Claim 16

- a. The UE of claim 15, wherein the SUPI comprises a Mobile Subscription Identification Number.*

See Section IX.A.15 for disclosure of claim 15. See element 1[b] for disclosure of the SUPI comprising a Mobile Subscription Identification Number. See also element 6[a].

B. Ground 2: Claims 1-6 and 8-16 Are Rendered Obvious By Nair in Combination with Forsberg and Togawa

1. Motivation to Combine Nair, Forsberg, and Togawa

See Section IX.A.1 for motivation to combine Nair and Forsberg. A POSITA would have been further motivated to combine the complementary teachings of Nair, Forsberg, and Togawa, as explained below and supported by the Declaration of Dr. Harry V. Bims. Ex. 1002, ¶¶ 133–140.

First, a POSITA would have been motivated to use Togawa’s encryption scheme identifier in place of Nair’s privacy indicator for several reasons, as Dr. Bims explains. *Id.* ¶ 134. The combination of Nair, Forsberg, and Togawa represents the

use of known techniques to improve similar devices in the same way. Nair and Togawa relate to the same field of privacy-protection scheme identification. *Compare* Ex. 1004, ¶[0010], *with* Ex. 1006, 10:31-39.

Second, as Dr. Bims explains, Nair, Forsberg, and Togawa address the same problem: securing messages within a communication system by identifying encryption and/or an encryption scheme identifier within the transmitted message. *Compare* Ex. 1004, ¶[0007] (describing the importance of security and subscription privacy in communication systems), *with* Ex. 1006, 1:20-23 (describing the information security problem that an encryption information method must be shared between the encrypting device and the decrypting device for decryption to occur in a communication system); Ex. 1002, ¶ 135. Based on the similar components and structures of the references and the common nature of the problem to be solved, a POSITA would have naturally turned to Togawa to use as the secondary encryption identification technique in the Nair-Forsberg-Togawa combination design. For similar reasons, this combination would have yielded predictable results. *Id.*

Third, a POSITA would have been motivated to improve Nair's privacy indicator with Togawa, as Dr. Bims explains. Ex. 1002, ¶ 136. Togawa represents a known improvement to an encryption identifier by its ability to identify more than one type of encryption scheme, which may easily be integrated with the

authentication method of Nair with a reasonable expectation of success. *Id.* In other words, the Nair-Forsberg-Togawa combination represents the simple substitution of one known element of Nair’s privacy indicator for another (Togawa’s encryption scheme identifier) to achieve a predictable result with a reasonable expectation of success. *Id.*

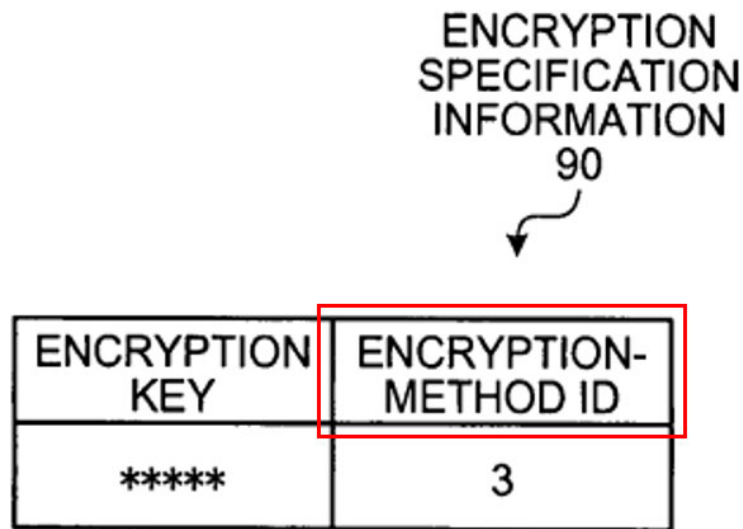
Fourth, Nair teaches the benefits (*e.g.*, saving time and reducing required resources) of using privacy indicators to assist the de-concealing server in determining information about the encryption process used within the data transmission, as Dr. Bims explains. Ex. 1004, ¶[0043] (“[O]ne key reason 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.***”). Ex. 1008, 6:21-23; Ex. 1002, ¶ 137. The inclusion of a privacy indicator (*e.g.*, encryption scheme identifier) allows a de-concealing server to begin the decryption process immediately using the decryption method indicated by the identifier. Ex. 1002, ¶ 137. This technique frees the de-concealing server from first having to figure out which decryption scheme was used to encrypt the message and which decryption technique to apply to decrypt the message. *Id.*

A POSITA reading Nair would have understood the time and resource-saving benefits of providing encryption technique identification to a de-concealing server

rather than wasting server resources deciphering the encryption technique manually.

Ex. 1002, ¶ 138. A POSITA would have been motivated to consult and apply Togawa for its teachings of an encryption scheme identifier to take advantage of the faster processing time and resource-reducing benefits that Togawa provides and that Nair extols the benefits of. *Id.*

A POSITA reading Nair would have been motivated to seek and apply additional techniques for flagging encryption schemes to a de-concealing server, such as the use of an encryption method ID (*i.e.*, encryption scheme identifier) as taught by Togawa and depicted in Fig. 13, to leverage the benefits taught by Nair. Ex. 1002, ¶ 139. Upon consultation with Togawa, a POSITA would have understood the benefits of applying an encryption method ID as taught by Togawa to manage the implementation of multiple non-null encryption methods and capitalize on the encryption indicator benefits as taught by Nair. Ex. 1002, ¶ 139.



Id., Fig. 13 (annotated); *see also id.*, 23:17-25.

Additionally, the use of an encryption scheme identifier and its benefits of providing faster processing times and reducing required resources were well-known in the art at the time of the alleged invention, and as such, a POSITA would have found it obvious to use this known technique to improve upon Nair's teaching, as Dr. Bims explains. Ex. 1002, ¶ 140.

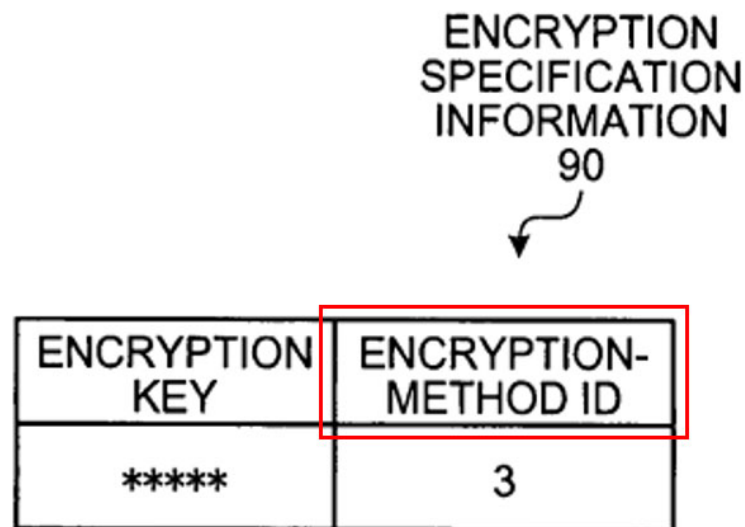
2. Independent Claim 1

As discussed in connection with Ground 1, Petitioner has shown that claim 1 is obvious over Nair in light of Forsberg. Element [1d] contains the sub-element (b)(ii), which recites that "the clear-text part of the SUCI generated by the UE comprises ... an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI." As discussed above, Nair's "privacy indicator," which is contained in the clear-text part of Nair's SUCI, is an "encryption scheme identifier" because it identifies which encryption scheme is used by the UE (*i.e.*, the null-scheme encryption or a non-null-scheme) to encrypt the MSIN. *See* Ground 1, element [1d].

However, to the extent that Patent Owner argues that an "encryption scheme identifier" must disclose which of a plurality of *non*-null-scheme encryption schemes are used, it would have been obvious to a POSITA to supply such an

encryption scheme identifier to the combination of Nair and Forsberg, in light of Togawa. Ex. 1002, ¶ 141.

Togawa discloses a data decryption apparatus and a data encryption apparatus to allow secure communication between the apparatuses. Ex. 1006, 1:7-11. Togawa teaches inclusion of an encryption key and an encryption-method ID (i.e., an encryption scheme identifier) within the transmitted message, which identify the encryption key and encryption scheme/method, respectively, used to encrypt the communicated message. *Id.*, Fig. 13; 23:19-25. Upon receipt of the transmitted message containing the encryption key identifier, the data receiving apparatus extracts the identifier and stores the corresponding encryption key to be used in the decryption process. *Id.*, 10:41-46, 23:26-33.



Id., Fig. 13 (annotated). Togawa’s “encryption specification information 90” specifies which of a plurality of encryption methods was used. *Id.*, 23:1-4 (noting

the encryption method changes over time), 23:17-39. As discussed above in Section IX.B.1, a POSITA would have been motivated to use Togawa's encryption scheme identifier in place of Nair's privacy indicator for several reasons. Ex. 1002, ¶¶ 133–140.

3. Independent Claims 9, 10, and 15

As discussed for Ground 1, Petitioner has shown that independent claims 9, 10, and 15 are obvious over Nair in light of Forsberg. Just as with claim 1, however, each of these claims contain the limitation that “the clear-text part of the SUCI generated by the UE comprises ... an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI.” Should Patent Owner argue that Nair's “privacy indicator” does not disclose this sub-element, it would have been obvious to supply this element to the SUCI of the combination of Nair and Forsberg in light of the Encryption-Method ID disclosed in Togawa, for the same reasons as discussed for Ground 2, claim 1, *supra*.

4. Dependent Claims 2-6, 8, 11-14, and 16-17

As discussed for Ground 1, Petitioner has shown that each of these dependent claims are disclosed or rendered obvious by Nair in light of Forsberg. Dependent claims 2-6 and 8 depend on independent claim 1. Dependent claims 11-14 depend on independent claim 10. Dependents claim 16 and 17 depend on independent claim 15. As noted above, Patent Owner may argue that the combination of Nair and

Forsberg does not disclose the “encryption scheme identifier” recited in independent claims 1, 10, and 15, but if so, this element of those claims would be obvious to supply in light of Togawa. Accordingly, their dependent claims would likewise be obvious over the combination of Nair, Forsberg, and Togawa for the reasons stated in Ground 1, *supra*.

C. Grounds 3 and 4: Claims 8 and 14 are Rendered Obvious By The References of Grounds 1 and 2, in Further Combination with 5G-Ensure D3.1

Claims 8 and 14 each add the limitation that the encryption scheme is an Elliptic Curve Integrated Encryption Scheme. These limitations would have also been obvious in light of the combinations of Grounds 1 and 2, in further combination with 5G-Ensure D3.1. 5G-Ensure D3.1 was publicly available as of March 2016, which is more than a year prior to the earliest effective filing date of the '817 patent (July 25, 2017).

1. Claims 8 and 14

Nair in combination with Forsberg and 5G-Ensure D3.1 (and optionally in combination with Togawa) render claims 8 and 14 obvious. 5G-Ensure D3.1 teaches the benefits of practicality and inherent message randomization provided by attribute based encryption schemes such as those based on elliptic curve pairings. Ex. 1010, §3.1.5.1 at 33 (“The ABE [attribute based encryption] schemes based on elliptic curve pairings are practical and inherently include message randomization for

semantic security and personalized randomization for collusion resistance.”). A POSITA would have understood that 5G-Ensure D3.1 is referring to ECIES because “[t]he best known encryption scheme based on ECC [elliptic curve cryptography] is the Elliptic Curve Integrated Encryption Scheme (ECIES).” Ex. 1011, 7; Ex. 1002, ¶ 144. As Dr. Bims further explains, a POSITA would have been familiar with ECIES, especially since ECIES had already been included in many industry standards, such as the “ANSI X9.63, ISO/IEC 18033-2, IEEE 1363a, and SECG SEC 1 standards.” Ex. 1011, 7; Ex. 1002, ¶ 145-46. Furthermore, a POSITA would have understood the benefits of using ECIES, including its offering of greater security level using a smaller key length size. Ex. 1011, 7-8; Ex. 1002, ¶ 146. As Dr. Bims explains, a smaller key length size translates to “easier data management, lower hardware requirements (in terms of buffers, memory, data storage, etc.), less bandwidth when transmitting the keys over a network, and longer battery life in devices where it is important, such as mobile phones. Ex. 1011, 7; Ex. 1002, ¶ 146. Given that these well-known qualities of ECIES are particularly useful for mobile phones, where bandwidth and power consumption are crucial design considerations, a POSITA would have not only known about ECIES, but would have been particularly motivated to implement ECIES encryption after consulting and applying the teachings of 5G-Ensure D3.1. Ex. 1002, ¶ 146.

Because Nair also teaches techniques and applications for the 4G-LTE and 5G Next Generation standards, and is expressly addressed to the problem of ensuring privacy and security in communication systems, Ex. 1004, ¶¶ [0002], [0004], a POSITA would have been motivated to consult 5G-Ensure D3.1 to supplement and complement Nair's system with predictable results. Ex. 1002, ¶ 147.

Additionally, a POSITA would have been motivated to improve the Nair's privacy indicator with 5G-Ensure D3.1. For example, 5G-Ensure D3.1 represents a known additional encryption scheme, which may easily be integrated with the authentication method of Nair with a reasonable expectation of success. Ex. 1002, ¶ 147. In other words, the Nair-5G-Ensure D3.1 combination represents the simple substitution of one known element, Nair's encryption scheme, for another (5G-Ensure D3.1's ECIES encryption scheme) to achieve a predictable result with a reasonable expectation of success. *Id.* For the same reasons, the Nair-5G-Ensure D3.1 combination represents combining prior art elements (Nair's authentication method and system with 5G-Ensure D3.1's ECIES encryption scheme) according to known methods to yield predictable results. Ex. 1002, ¶ 147.

X. SECONDARY CONSIDERATIONS

Petitioner is unaware of any evidence of secondary considerations that would support a finding of non-obviousness. *See Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1311–12 (Fed. Cir. 2006). The asserted prior art cited herein

demonstrates there is no evidence of failure by others and that the features recited in the Challenged Claims were readily available in the prior art. Even if secondary considerations did exist, they could not overcome the strong *prima facie* case of obviousness shown in this Petition. *See Wyers v. Master Lock Co.*, 616 F.3d 1231, 1246 (Fed. Cir. 2010). Should Patent Owner attempt to meet its burden to show secondary considerations, Petitioner reserves the right to respond.

XI. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. The *Advanced Bionics* Test Favors Institution—§ 325(d)

This Petition also does not present the same or substantially the same arguments that were previously considered by the Office. Nair was not considered by the examiner during the original prosecution. *See* Ex. 1009, 94-96.

Although Forsberg was cited during prosecution (*see* Ex. 1009 at 94, 191, 199), it was not relied upon by the Examiner as a primary reference for any of the Challenged Claims. Likewise, TR 33.899, which is incorporated by reference into Nair, was cited in an IDS and in the International Search Report generated for the '817 patent's associated PCT application PCT/EP2018/69432, but it was not discussed by the Examiner or the Patent Owner during prosecution. *See generally* Ex. 1009.

With regard to Forsberg, there is no record evidence that the Examiner appreciated the import of Forsberg's teachings (discussed above) about public key

identifiers. *See, e.g.,* Ex. 1005 ¶¶49, 54; *Advanced Bionics, LLC v. Med-El Elektromedizinische Gerate GMBH*, IPR2019-01469, Paper 6, at 10 (P.T.A.B. Feb. 13, 2020) (precedential). Instead, the Examiner relied upon Lee (Ex. 1012) as a primary reference, which does not mention a public key identifier. *See* Ex. 1012. This petition thus presents a new primary reference and focuses on a different aspect that was either not previously considered or was overlooked.

B. The *Fintiv* Factors Favor Institution—§ 314(a)

The Board should not apply *Fintiv* to discretionarily deny institution under §314(a) in view of the International Trade Commission (“ITC”) or the Eastern District of North Carolina (“EDNC”) proceedings for at least the following reasons. First, *Fintiv* does not apply to parallel ITC proceedings. Vidal Memo at 3. Second, the EDNC litigation is stayed—with regard to the ‘817 patent—in view of the ITC investigation. Third, this petition presents compelling evidence of unpatentability, as shown below in Section IX.

Factor 1: On February 19, 2024, the EDNC was stayed until the determination of the ITC becomes final.

Factors 2 and 3: The Board will very likely issue its Final Written Decision before a trial occurs in the EDNC. The case is stayed, no discovery with regard to the ‘817 patent has taken place, no claim construction proceedings have occurred,

and no scheduling order or trial date have been set in the EDNC. All major case milestones in the EDNC litigation are yet to occur.

Factor 4: If the EDNC is unstayed (unlikely) and if IPR is instituted, Petitioners will file a stipulation that it will not pursue in the EDNC litigation the actual grounds raised in this IPR. The Board has recognized that this *Sand Revolution* type stipulation effectively addresses the risk of duplicative efforts. *Apple Inc. v. Aire Technology Ltd.*, No. IPR2022-01136, Paper 11 (P.T.A.B. Jan. 4, 2023).

Factor 5: Petitioners and defendants in the EDNC litigation are the same entities. However, in view of the other *Fintiv* factors—which heavily weigh against the Board’s exercise of §314(a) discretion—the similarity of the parties is of limited weight. *See, e.g., NanoCollect Biomedical, Inc. v. Cytonome/ST, LLC*, IPR2020-00551, Paper 19 at 24-25 (P.T.A.B. Aug. 27, 2020) (Petitioner and Patent Owner parties to district court case, but declining to exercise discretion); *NVIDIA Corp. v. Invesas Corp.*, IPR2020-00602, Paper 11 at 28, 33 (P.T.A.B. Sept. 3, 2020) (same). Further, institution would permit the Board to resolve questions of patentability regarding claims that Patent Owner might otherwise assert against others later. *See Apple Inc. v. Seven Networks, LLC*, IPR2020-00235, Paper 10 at 16 n.7 (P.T.A.B. July 28, 2020).

Factor 6: This Petition’s merits are strong, which weighs against the Board exercising its discretion under §314(a). *Sand Revolution II, LLC, v. Continental Intermodal Grp. Trucking LLC*, IPR2019-01393, Paper 24 at 13 (P.T.A.B June 16, 2020) (informative). Further, the petition presents compelling evidence of unpatentability such that “the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” Vidal Memo at 4.

In view of the foregoing, “[c]onsidering the *Fintiv* factors as part of a holistic analysis,” it would run counter to “the interests of the efficiency and integrity of the system” if the Board were “to deny institution of a potentially meritorious Petition.” *Sand Revolution II, LLC*, IPR2019-01393, Paper 24 at 14. Thus, the Board should decline to exercise its discretion under § 314(a).

XII. CONCLUSION

Petitioner requests institution of IPR and cancellation of the challenged claims.

DATED: March 15, 2024

Respectfully submitted,

/s/ Robert A. Appleby

**Robert A. Appleby
Counsel For Petitioner
Reg. No. 40,897**

CERTIFICATE OF COMPLIANCE

This Petition complies with the type-volume limitations as mandated in 37 C.F.R. § 42.24, totaling 13,946 words. Counsel has relied upon the word count feature provided by Microsoft Word.

/s/ Robert A. Appleby
Robert A. Appleby

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I certify that I caused to be served on March 15, 2024, a true and correct copy of the foregoing **PETITION FOR *INTER PARTES* REVIEW UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104** by overnight carrier to the Patent Owner at the correspondence address of record for the Patent Owner's Attorneys as follows:

6449 - ROTHWELL, FIGG, ERNST & MANBECK, P.C.
901 New York Avenue, N.W.
SUITE 900 East
WASHINGTON, DC 20001
UNITED STATES

A courtesy copy was also served via electronic mail on Patent Owner's counsel of record in the investigation before the International Trade Commission, Inv. No. 337-TA-1375.

Adam D. Swain
Alston & Bird LLP
950 F Street NW
Washington, D.C. 20004
Telephone: 202-239-3622
Facsimile: 202-239-3333

John D. Haynes
Shri Abhyankar
David S. Frist
Katherine M. Donald
Shawn Gannon
Sloane Kyrazis
Alston & Bird LLP
1201 West Peachtree Street, Suite 4900
Atlanta, GA 30309
Telephone: (404) 881-7000
Facsimile: (404) 881-7777

Theodore Stevenson
Alston & Bird LLP
Chase Tower
2200 Ross Avenue
Suite 2300
Dallas, TX 75201
Telephone: 214-922-3400
Facsimile: 214-922-3899

Karlee N. Wroblewski
Alston & Bird LLP
Vantage South End
1120 South Tryon Street, Suite 300
Charlotte, NC 28203-6818
Telephone: 704-444-1000
Facsimile: 704-444-1111
Email: EricssonLenovo@alston.com.

/s/ Robert A. Appleby
Robert A. Appleby