

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

**DECLARATION OF HARRY BIMS, Ph.D.
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,425,817**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND AND QUALIFICATIONS	2
III.	MATERIALS REVIEWED	6
IV.	PERSON OF ORDINARY SKILL IN THE ART AND THE TIME OF THE ALLEGED INVENTION	9
V.	THE '817 PATENT	10
VI.	CLAIM CONSTRUCTION	18
VII.	OVERVIEW OF THE PRIOR ART	19
	A. Nair (Ex. 1004).....	19
	B. 3GPP TR 33.899 V1.1.0 (Release 14)	21
	C. 3GPP TS 23.501 V0.4.0 (Release 15).....	23
	D. Forsberg.....	24
	E. Togawa	25
	F. 5G -Ensure Deliverable D3.1, “5G-PPP security enablers technical roadmap” (early version)	27
VIII.	THE PRIOR ART DISCLOSES AND/OR SUGGESTS THE RECITED FEATURES OF CLAIMS 1-6 and 8-16 OF THE '817 PATENT	28
	A. Ground 1: Claims 1-6 and 8-16 Are Rendered Obvious By Nair in Combination with Forsberg.....	28
	1. Obviousness of Nair And Forsberg	28
	2. Independent Claim 1	34
	3. Dependent Claim 2.....	59
	4. Dependent Claim 3.....	62

5.	Dependent Claim 4.....	63
6.	Dependent Claim 5.....	64
7.	Dependent Claim 6.....	66
8.	Dependent Claim 8.....	68
9.	Independent Claim 9	69
10.	Independent Claim 10	71
11.	Dependent Claim 11	72
12.	Dependent Claim 12	72
13.	Dependent Claim 13	74
14.	Dependent Claim 14	77
15.	Independent Claim 15.....	77
16.	Dependent Claim 16	79
B.	Ground 2: Claims 1-6 and 8-16 Are Rendered Obvious By Nair in Combination with Forsberg and Togawa.....	79
1.	Motivation to Combine Nair, Forsberg, and Togawa.....	79
2.	Independent Claim 1	83
3.	Claims 2-17	85
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	85
1.	Claims 8 and 14.....	85
IX.	CONCLUSION.....	87

I, Harry Bims, Ph.D., declare as follows:

I. INTRODUCTION

1. I have been retained by Lenovo (United States) Inc. (“Lenovo” or “Petitioner”) as an independent expert consultant in this proceeding before the United States Patent and Trademark Office (“PTO”) against Telefonaktiebolaget LM Ericsson, (“Patent Owner”) regarding U.S. Patent No. 10,425,817 (“the ’817 patent”) (Ex. 1001).¹ I have been asked to consider whether certain references disclose or suggest the features recited in claims 1-6 and 8-16 (“the challenged claims”) of the ’817 patent. My opinions are set forth below.

2. I am being compensated at a rate of \$750/hour for my work in this proceeding. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding.

¹ Where appropriate, I refer to exhibits that I understand are to be attached to the petition for *inter partes* review of the ’817 patent.

II. BACKGROUND AND QUALIFICATIONS

3. My educational background, career history, publications, and other relevant qualifications provided here are only a summary. My full curriculum vitae is attached to this declaration as Exhibit 1003.

4. Based on my education, research, and work experience, I am knowledgeable about the subject matter of the '817 patent and the related prior art.

5. I have worked extensively in the field of digital communications. I have studied telecommunications and systems engineering since approximately 1981. Further, I have over 20 years of industry experience in computer network design, including the design of hardware and software for computer communications in a wireless context. During this period, I have designed and implemented various products involving cellular communication technology.

6. I received a B.S. in Computer and Systems Engineering from Rensselaer Polytechnic Institute in 1985. In 1988, I received a M.S. in Electrical Engineering from Stanford University. In 1993, I received a Ph.D. in Electrical Engineering, also from Stanford University. As a graduate student at Stanford University, I studied the principles of digital communications theory, including data modulation and demodulation, error checking and correction algorithms, and the architecture and design of semiconductor circuits used for digital communications. My Ph.D. thesis at Stanford addressed the application of trellis coding and precoding

Declaration of Harry Bims, Ph.D.

U.S. Patent No. 10,425,817

to a digital modulation system, and was titled “Trellis Coding for Multi-Level, Partial Response Continuous Phase Modulation with Precoding.”

7. After receiving my Ph.D. in 1993, I worked for Glenayre Technologies - Wireless Access Group, where I focused on hardware and software architecture and design, including inventing, designing, and building a patented computer system for real-time testing of two-way pagers and co-developing a wireless application protocol that included a CRC error checking algorithm. From 1999 to 2001, I was the Director of Engineering for Symmetry Communications, where I was responsible for managing the software development for 2.5G network equipment (the precursor to 4G network equipment) that handles communications to and from personal cellular telephones. The equipment products we developed (a “Serving GPRS Support Node” (or “SGSN”) and “Gateway GPRS Support Node” or (“GGSN”)) routed and managed cellular phone communications by relaying packets of voice, data, and video between the base station tower and the Internet, regulating the network bandwidth allocated to different classes of cellular phone applications, and transferring control of cellular phone communications from one base station to the next as cellular phones move throughout a geographic area. I also held management responsibility for the Firmware, Hardware, Performance, and Systems Engineering Groups.

8. In January of 1999, I launched a technology consulting company, Protocomm Systems Inc., which focuses on the development of advanced wireless communications protocols and related software implementations for wireless product companies.

9. From 1999 to 2001, I was also the Director of Software Architecture for Symmetry Communications System. In this position, I was responsible for the software architecture for core SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node) products for the GPRS (Generic Packet Radio Services) market. I also held management responsibility for the Firmware, Hardware, Performance, and Systems Engineering Groups.

10. In 2001, I developed a business plan for building network infrastructure for 802.11 enterprise networks, and then later that year founded AirFlow Networks, Inc., where I invented and received over eleven patents on its core technology, which was based on the 802.11 wireless local area network specification.

11. I have been a member of the Institute of Electrical and Electronics Engineers ("IEEE") for more than 28 years. The IEEE is an international organization of more than 400,000 engineers, and is the world's largest technical professional society, with locations in more than 160 countries. I am currently a Senior Member of the IEEE, and serve in a variety of leadership roles, including as a reviewer and voter on draft amendments to technical standards such as 802.11 (Wi-

Fi), and 802.3 (Ethernet) prior to publication by their 802 Committee. The IEEE 802 Committee is the standards development organization responsible for publishing protocol standards for Ethernet, Wi-Fi, and a variety of other wired and wireless protocols that are in commercial use globally.

12. I am currently an expert consultant for Protocomm Systems, LLC and Bims Laboratories, LLC, both of which I founded. I perform technical research in wireless technology standards, such as UMTS, LTE/4G, 5G, Wi-Fi, Bluetooth, and other network communication protocols. I am named as an inventor of twenty-three telecommunications related patents. The services I provide include consulting in telecommunication standards setting, protocol simulation and implementation, technology assessments, engineering lab testing, and product analysis. Through Bims Laboratories, I have participated in technical discussions for several years in the IEEE 802 Committee to develop new technology that allows LTE and 5G networks to coordinate their network activities with Wi-Fi networks.

13. I have also served in several leadership capacities with the IEEE 802.16 Working Group (2009-present) and the IEEE 802.15 Working Group where I currently serve as technical editor for a wide-area cellular standard that is a competitor to LTE and 5G, and I am currently a voting member in the IEEE 802.11 Working Group. Within the IEEE 802.15 Working Group, I am the technical editor for IEEE 802.16t, an amendment to the WiMAX standard that supports long-range

Declaration of Harry Bims, Ph.D.

U.S. Patent No. 10,425,817

wireless networks for the railroad industry. Furthermore, since 2003, I have served as a wireless technology expert in patent infringement cases. I am actively involved in liaison conversations regarding the interoperation of IEEE 802.11-based wireless networks and 3GPP networks, including 3G, LTE, and 5G networks.

14. I am an author of 9 technical publications and a named inventor of 23 telecommunication-related patents, including U.S. Patent No. 8,995,996, which describes how wireless devices that interfere with each other can coordinate their communications in an optimal manner. The entire list of those patents and publications can be found in my full CV.

15. I have been active in professional engineering associations and research bodies. From 1985 to 1991, I was the AT&T Bell Labs Cooperative Research Fellow. In 2000, I served as a Chair of IEEE Engineering Management Society, Silicon Valley Chapter. From 2007 to 2010, I served as a vice chair and secretary of IEEE 802.16h License-Exempt Task Group and have been a senior member of IEEE since 2012.

III. MATERIALS REVIEWED

16. The opinions contained in this declaration are based on the documents I reviewed, my professional judgment, as well as my education, experience, and knowledge regarding signal processing, communications, and coding.

17. In forming my opinions expressed in this declaration, I reviewed the following materials and information:

Exhibit No.	Description
1001	U.S. Patent No. 10,425,817 to Torvinen, <i>et al.</i> (“the ’817 patent”)
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)
1016	Declaration of Friedhelm Rodermund
1017	Declaration of Nathaniel E Frank-White

18. I also reviewed any other materials I refer to in this declaration in support of my opinions.

19. My opinions contained in this declaration are based on the documents I reviewed and my knowledge and professional judgment. My opinions have also been guided by my understanding of how a person of ordinary skill in the art would have understood the state of the art, the prior art, and the claims and the specification of the '817 patent at the time of the alleged invention.

20. I have been asked to consider that the time of the alleged invention of the '817 patent is around July 25, 2017, which I understand is the filing date of Provisional Application No. 62/536,632, to which the '817 patent claims priority. Ex. 1001, 1 (Related U.S. Application Data section). My opinions reflect how one of ordinary skill in the art (which I describe below) would have understood the '817 patent, the prior art to the patent, and the state of the art at the time of the alleged invention as I was asked to consider, noted above.

21. Based on my experience and expertise, it is my opinion that the prior art discloses and/or suggests all the features recited in challenged claims 1-6 and 8-16 of the '817 patent, as I discuss in detail below.

IV. PERSON OF ORDINARY SKILL IN THE ART AND THE TIME OF THE ALLEGED INVENTION

22. Based on my knowledge and experience, I understand what a person of ordinary skill in the art would have known at the time of the alleged invention, which I discussed above as being around July 25, 2017. My opinions herein are, where appropriate, based on my understandings as to a person of ordinary skill in the art at that time. In my opinion, based on the materials and information I have reviewed, and based on my experience in the technical areas relevant to the '817 patent, a person of ordinary skill in the art at the time of the alleged invention 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. Additional education would compensate for less experience, and vice versa. I apply this understanding in my analysis herein.

23. All of my opinions in this declaration are from the perspective of one of ordinary skill in the art, during the relevant timeframe (*e.g.*, the time of the alleged invention), which I discussed above as being around July 25, 2017. During this timeframe, I possessed at least the qualifications of a person of ordinary skill in the art, as defined above.

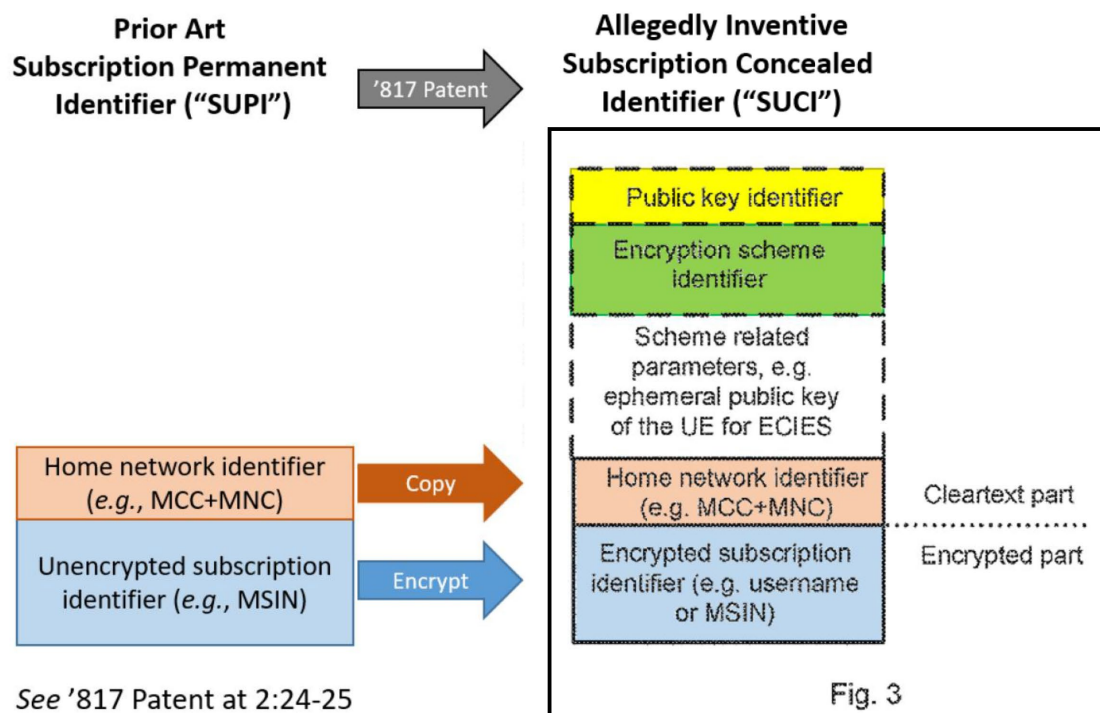
V. THE '817 PATENT

24. The '817 patent relates to encrypting a subscription identifier. Ex. 1001 at Abstract. 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. *Id.*, 1:22-36. A POSITA would have understood that in the context of the '817 patent "long-term subscription identifier" means information permanently allocated to a UE that uniquely identifies the UE within a network. The '817 patent discloses that the information permanently allocated to and used to uniquely identify a UE connected to 5G communication networks (i.e., the long-term subscription identifier) is known as a Subscription Permanent Identifier ("SUPI") and cites a user's IMSI as an exemplary SUPI. *Id.*, 1:22-36, 1:37-43, 2:24-31, 8:19-24. When UE, such as a mobile phone, authenticated to the mobile network in certain prior-art systems (such as LTE), the UE sent the user's IMSI through the air in clear text (that is, unencrypted). *Id.*, 1:31-33. Devices called "IMSI catchers" could monitor the airwaves for transmissions of IMSIs, or even impersonate a base station to request the UE to send the IMSI, to retrieve the IMSI and thereby allow a bad actor to impersonate the user associated with the IMSI. *Id.*, 1:33-36. The '817 patent admits that before the alleged invention members of the standards-setting organization 3rd Generation Partnership Project ("3GPP") had noted that one solution to the problem of IMSI catchers was to encrypt the user's SUPI, including

Declaration of Harry Bims, Ph.D.
U.S. Patent No. 10,425,817

using public key encryption. Id., 1:22-43 (citing 3GPP TS 33.501 V0.2.0 (Release 15) (Ex. 1014), published May 2017).

25. The '817 patent also acknowledges that it was known in the prior art to use an IMSI as a long-term subscription identifier. Ex. 1001, 1:22-43. As explained above, a POSITA would have understood that the long-term subscription identifier used in prior art 5G networks was known as a SUPI. In the scheme of the '817 patent, 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 ("The SUPI may comprise a Mobile Subscription Identification Number."), 8:62-66 ("When the encrypted part is included in the SUCI, the SUCI is a protected version of SUPI. The encrypted part includes an encrypted subscription identifier, such as an MSIN (Mobile Subscription Identification Number) or username."), Fig. 3.



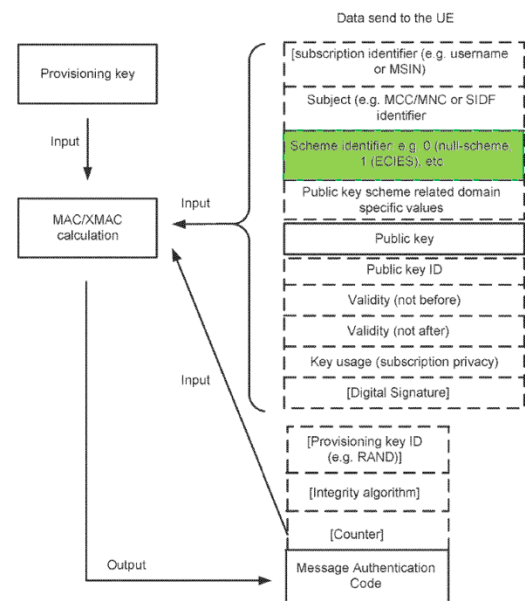
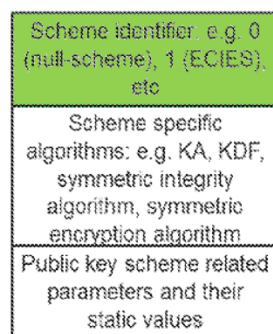
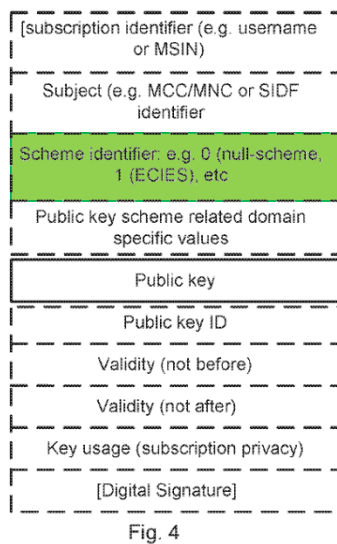
26. As shown in Figure 3, which I annotated above, the SUCI has both an “encrypted part” and a “cleartext part.” Id., 1:52-56, 8:39-40. The encrypted part of the SUCI contains the MSIN portion of the IMSI (the pink “Encrypted subscription identifier” in annotated Figure 3 above). Id., 2:26-28, 8:62-66. The clear-text part of the SUCI contains the MCC and MNC portions of the IMSI (collectively, the blue “home network identifier” in annotated Figure 3 above). Id., 2:24-29, 7:28-29, 8:41-43. It is necessary for the home network identifier to be in clear-text because a base station, which may not be operated by the user’s carrier (such as when the user is roaming), needs to know what the user’s home network is to route the authentication request to that home network during a registration. Id., 7:34-35, 8:28-33.

27. The '817 patent's SUCI also contains several other fields in the clear-text part including a field called the "encryption scheme identifier," (green in annotated Figure 3 above), which indicates the particular encryption method (or "scheme") used to encrypt the MSIN. *Id.*, 2:38-44, 8:44-50. As one example of an encryption scheme, the '817 patent identifies the well-known Elliptic Curve Integrated Encryption Scheme ("ECIES"). *Id.*, 3:29-34, 8:44-50. "ECIES is an example of a public key encryption scheme," which means that it encrypts data according to a "public key" that can be shared with the world, but that such encrypted data can only be decrypted by someone that has the corresponding "private key," which is kept secret. *Id.*, 9:8-13; Ex. 1011, 7. Any arbitrary number of ECIES public key / private key pairs can be generated. Ex. 1001, 9:22-39; Ex. 1011, 9.

28. The '817 patent describes a second example of an encryption scheme being the "null-scheme," which actually performs no encryption. See Ex. 1001, 3:27-28 ("[T]he encryption scheme may be a null-encryption scheme"), 9:11-12 ("[T]he encrypted part of the SUCI may use a null encryption scheme...."), 15:9-11 ("The null-scheme is implemented such that it returns the same output as the input...."). Though it may seem counterintuitive that a scheme that performs no encryption could be an "encryption scheme," the '817 Patent expressly states that the "encrypted part" of the SUCI may be generated using the null-encryption scheme. See *id.*, 9:11-13 ("[T]he encrypted part of the SUCI may use a null

encryption scheme, e.g., if the UE 1 has not been provisioned with the public key of the home network.”), 15:7-9 (“Because the UE initially has no privacy key in this scenario, the UE uses a null-scheme or null-encryption method to create the SUCI.”).

29. The ’817 patent states that the “encryption scheme identifier” contained in the SUCI can be as simple as a single bit, using “0” to indicate that the MSIN is “encrypted” using the null-scheme, and “1” to indicate that the MSIN is encrypted using ECIES. See *id.*, 10:17-20 (“Each scheme adopted as standard may be assigned a specific identifier. For example, the null-scheme may be assigned a 0, ECIES may be assigned a 1, and so on.”). Figures 4, 5 and 15 (annotated below) likewise depict a SUCI with an encryption scheme identifier bit field, wherein a “0” indicates the null-scheme was used to encrypt the SUPI and a “1” indicates the ECIES scheme was used.



Id., Figs 4, 5, and 15 (annotated).

30. The clear-text portion of the '817 patent's SUCI also contains a "public key identifier." *Id.*, 1:62-63, 2, 1-3, 2:45-50, Fig. 3. A given network may include multiple decryption servers (called "Subscription Identifier De-concealing Functions," or "SIDFs"), each with their own public key and corresponding private key. *Id.*, 6:50-62. The public key identifier indicates which public key was used to encrypt the SUCI, and accordingly, indicates to the authentication server which SIDF (containing the corresponding private key) to send the SUCI to for decryption. *Id.*, 8:54-57 ("[T]he public key identifier is an identifier that may be used within the home network to identify the correct SIDF in a home network that includes a plurality of SIDFs."), 10:50-53 ("[T]he AUSF may use the public key identifier carried in the SUCI ... to identify the correct SIDF 6.").

31. The authentication process (or "registration procedure") is shown in the '817 patent's Figure 6, reproduced below. *Id.*, 5:47, 10:25-37. During the authentication process in which a UE seeks to register with a communications network, the UE generates a SUCI of the aforementioned format and first transmits it to a server known as the "Authentication and Management Function" ("AMF"). See *id.*, Fig. 6 (step 3), 10:43-45. The AMF (or specifically, the component of the AMF known as the "Security Anchor Function," or "SEAF"), then forwards the SUCI to the Authentication Server Function ("AUSF"). See *id.*, Fig. 6 (step 4),

10:45-48. The AUSF uses the unencrypted home network identifier to identify the UE's home network to be used for authenticating the UE. Id., Fig. 6 (step 5), 1:64-67, 10:48-50. The AUSF also may use the unencrypted public key identifier within the clear-text part of the SUCI to identify the UE's home network to be used for authenticating the UE. Id., 10:50-53. Upon identification of the home network, the authentication server sends an authentication request, along with the SUCI, to the de-concealing server within the UE's home network. Id., Fig. 6 (step 6), 2:16-19, 11:11-12. Thereafter, the de-concealing server decrypts the SUCI using the scheme indicated by the encryption scheme identifier, and (if appropriate) the key identified by the public key identifier, thereby revealing the UE's SUPI. Id., 2:32-44, 11:17-18. The de-concealing server then returns the SUPI to the AUSF, which forwards this to the AMF/SEAF. Id., Fig. 6 (steps 7 and 9), 11:16-20, 11:32-34. Upon successful receipt of the SUPI and registration of the UE, the AMF/SEAF transmits a registration acceptance message to the UE, completing the registration process. Id., Fig. 6 (step 10), 11:34-36.

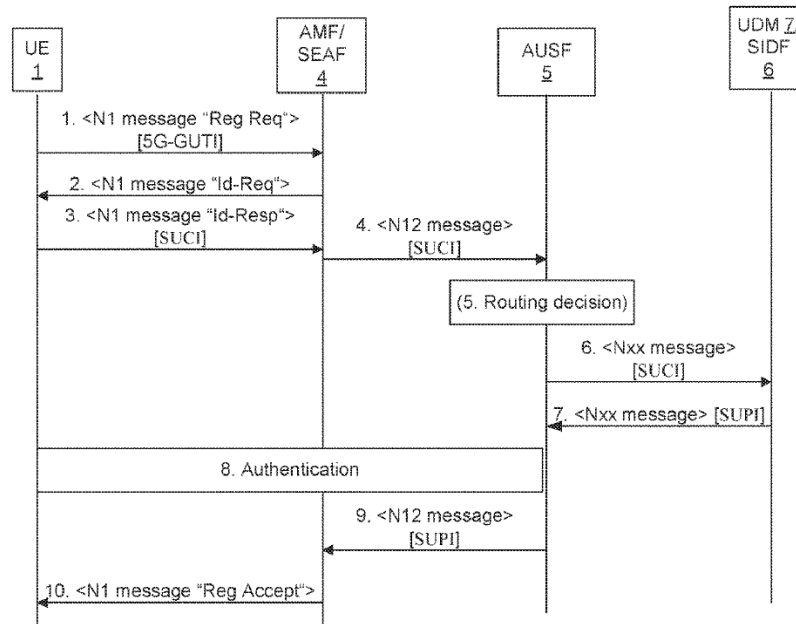


Fig. 6

Id., Fig. 6.

VI. CLAIM CONSTRUCTION

33. I understand that claim terms are typically given their ordinary and customary meanings, as would have been understood by a person of ordinary skill in the art at the time of the alleged invention, which as I explained above I have been asked to assume is around July 25, 2017. In considering the meaning of the claims, however, I understand that one must consider the language of the claims, the specification, and the prosecution history of record. I have been asked to consider the claim terms under their plain meanings and thus I have considered the claims, specification and prosecution history for the '817 patent in doing so in support of my opinions concerning the '817 patent and the prior art discussed herein. (Ex. 1001; Ex. 1004.)

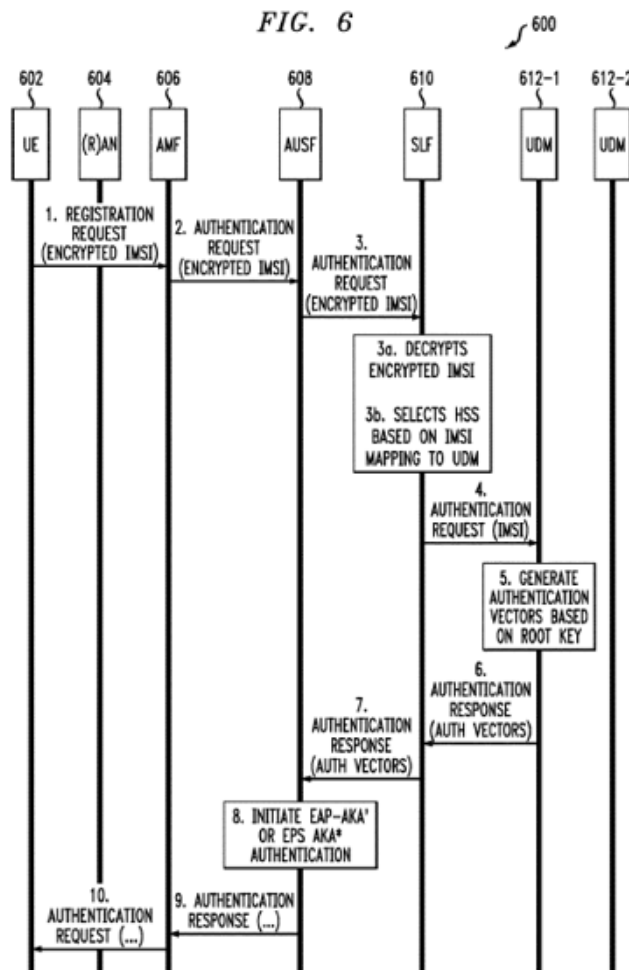
VII. OVERVIEW OF THE PRIOR ART

A. Nair (Ex. 1004)

34. Nair describes a process for maintaining the confidentiality of a UE's permanent subscription identifier (SUPI) during a UE authentication process by encrypting the user-specific information of a UE's IMSI (i.e., the MSIN), while keeping the remaining information of the IMSI (i.e., the MNC+MCC) in clear-text so that the transmission can be routed to the correct home network. Ex. 1004, ¶[0035].

35. Nair's Figure 6 (reproduced below), depicts such a process for authenticating a UE with a 5G network. As shown in Figure 6, a registration/authentication 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]. 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]. The User

Data Management (UDM), which acts as the home subscriber server in a 5G network, is then contacted to provide UE authentication vectors used to complete the UE registration process. *Id.*, ¶¶[0046], [0078], Fig. 6 (steps 5-7); Ex. 1008, Fig. 6 (steps 5-7); see also *id.* ¶¶[0072-73], Fig. 4 (disclosing a similar process for registration with a 5G network wherein the AUSF is co-located with the UDM); Ex. 1008, Fig. 4.



Ex. 1004, Fig. 6; *see also* Ex. 1008, Fig. 6.

36. Nair discloses similar a process for authenticating a UE with a mixed LTE/5G system. *See* Ex. 1004, ¶¶[0074-76], Fig. 5; Ex. 1008, Fig. 5. An attach/authentication request comprising the UE's partially-encrypted IMSI along with privacy indicators is transmitted to a Mobility Management Entity/Access and Mobility Management Function (MME/AMF) and then forwarded to a SLF. *Id.*, ¶[0076]. The SLF uses the indicators to determine applicable privacy features and decrypts the message to obtain the UE's IMSI, which is then forwarded as part of an authentication request to a Home Subscriber Server (HSS). *Id.* The HSS then provides UE authentication vectors based on the IMSI to complete the UE registration process. *Id.*

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

37. 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 ("This solution addresses the key issue #7.3 'Concealing permanent or long-term subscription identifier' by providing a way to conceal the IMSI using public key encryption based on Elliptic Curve Integrated Encryption Scheme (ECIES)."). ECIES, a public key encryption scheme, 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 ("The ECIES is a public key encryption

scheme that uses Elliptic Curve Cryptography (ECC) and constitutes of various functions like key agreement, key derivation, hash, encryption, and MAC. The encryption function in the ECIES is symmetric; however, the key used in the encryption is generated using the ECC public/private key pairs of the communicating parties.”); *see also* Ex. 1011, Abstract (“Elliptic curve cryptographic schemes are public-key mechanisms that provide encryption The best known encryption scheme based on ECC is the Elliptic Curve Integrated Encryption Scheme (ECIES).”). 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.

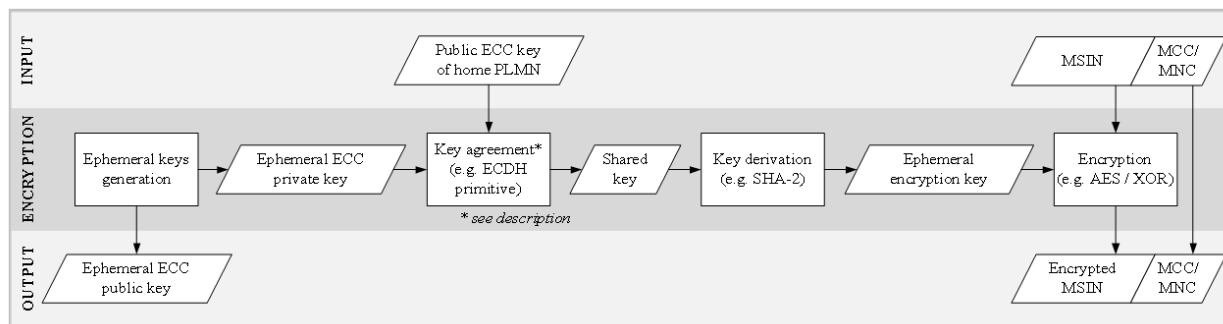


Figure 5.7.4.15.2-1: Encryption at the UE side (based on ECIES)

Id., Figure 5.7.4.15.2-1.

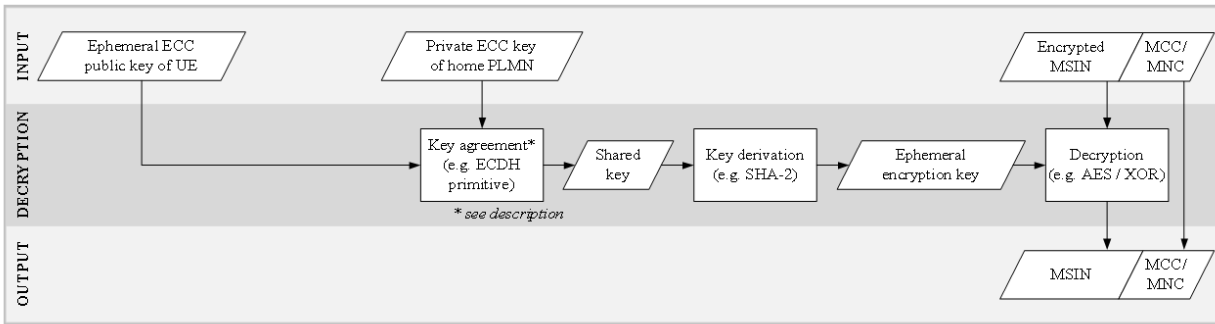


Figure 5.7.4.15.2-2: Decryption at the network side (based on ECIES)

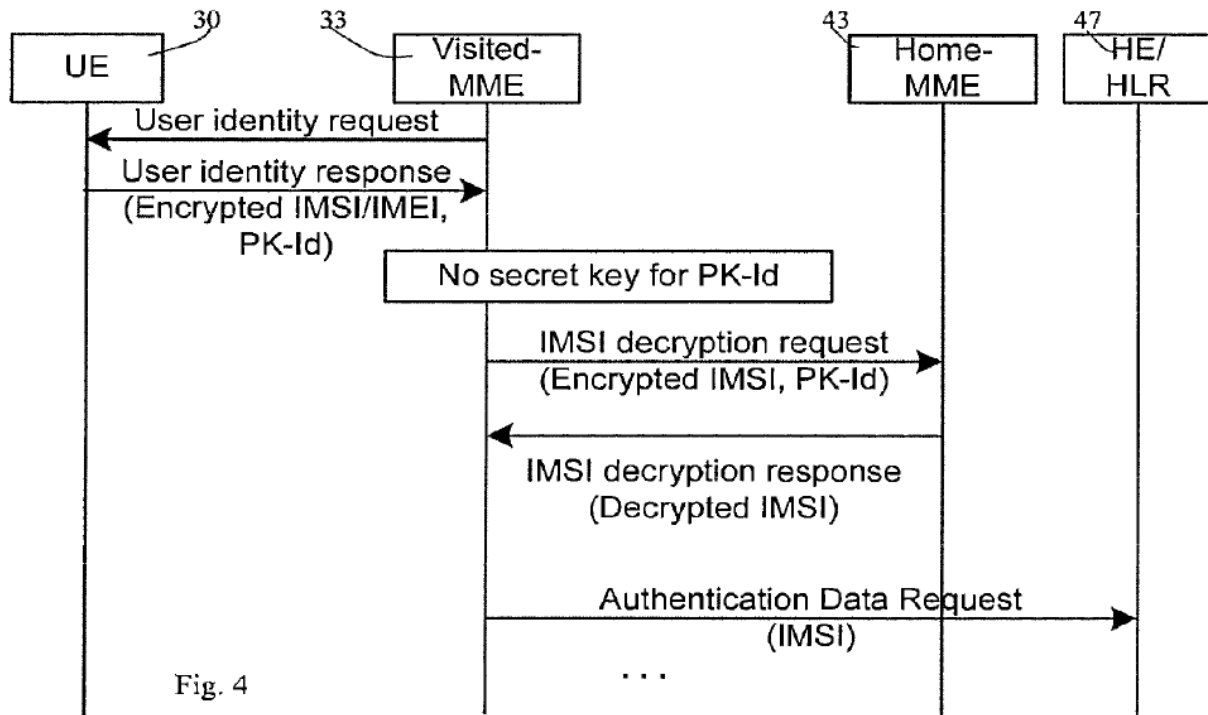
Id., Figure 5.7.4.15.2-1.

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

38. 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 further 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

39. 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.



Id., Fig. 4.

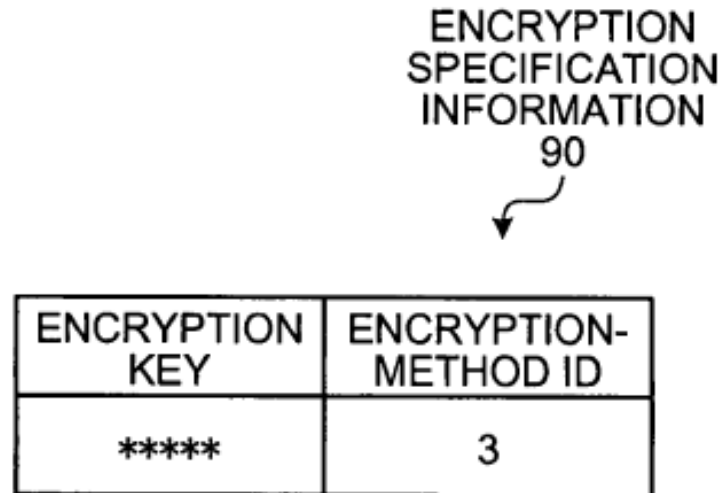
40. Forsberg discloses a UE that receives a user-identity request from an authentication server (Visited-MME 33 in Figure 4) as part of the process of registering with a communications network. *Id.*, ¶[0048]. The UE responds by sending its identity (including its encrypted IMSI and a public key identifier) 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]; *see also* Figs. 2-4.

E. Togawa

41. 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 ("The data

transmitting apparatus 10 and the data receiving apparatus 20, which have a voice call function, convert a voice of a user into a voice signal and exchange the voice signal bi-directionally, thereby carrying out a voice call between users.”).



Id., Fig. 13.

42. 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 (“[T]he encryption specification information 90 includes information on an encryption key and an encryption-method ID. The encryption key is an encryption key for use in encryption of user data.”). 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 (“The encryption-method ID is the identity that identifies an encryption method for use in encryption of the user data.”), 23:28-33 (“[T]he data receiving apparatus 20, 60

selects an encryption key and an encryption method that decrypt user data encrypted by the data transmitting apparatus 10, 50 based on the information on the call duration times or times, and decrypts the encrypted user data using the selected encryption key and the encryption method.”); 26:31-39 (“According to the present invention, the information on the encryption specification includes ... information on an encryption method... and information obtained by converting the encryption method by a predetermined method.”).

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

43. 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.*

44. 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.*

VIII. THE PRIOR ART DISCLOSES AND/OR SUGGESTS THE RECITED FEATURES OF CLAIMS 1-6 AND 8-16 OF THE '817 PATENT

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

1. Obviousness of Nair And Forsberg

45. In my opinion, a POSITA would have been motivated to combine the teachings of Nair and Forsberg to arrive at the claimed invention of claims 1-6 and 8-16.

46. Nair and Forsberg because both relate to the same field of invention. Nair and Forsberg both discuss security and privacy features for transmitting user identifiers within a wireless communication system. Ex. 1004, ¶[0011]; Ex. 1008, 2:16-19; Ex. 1005, ¶[0012]. Both Nair and Forsberg recognize and are directed at solving the problem that unencrypted mobile subscription information numbers

(e.g., IMSIs or MSINs) can be captured by third parties when sent in clear-text. *See* Ex. 1005, ¶[0011–15]; Ex. 1004, ¶[0027–33]. Both references teach encrypting the mobile subscription information numbers using public key encryption, which was well known at the time of the alleged invention. For example, Nair teaches using encryption and privacy indicators for use in concealment of a UE's subscription identifier during the authentication process for joining new UEs to a network. Ex. 1004, ¶[0010] (“The message may comprise an attach request comprising a subscription identifier for a subscriber of the communication network associated with the user equipment, the one or more privacy indicators comprising a flag indicating whether the subscription identifier in the attach request is privacy-protected.”); Ex. 1008, 3:18-20. Likewise, Forsberg teaches encrypting a UE's subscription identity during the authentication process to protect the privacy of the user. 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.”). Accordingly, in my opinion a POSITA would have been motivated to combine Nair and Forsberg because both relate to the same field of invention.

47. Additionally, a POSITA would have been motivated to use Forsberg's public key identifiers to reduce the complexities of managing multiple public and

private key pairs to allow the use of multiple Home Subscription Servers within a communications network, as described in Nair. Indeed, Nair teaches the benefits of using multiple encryption keys to allow 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], [0038] (“the SLF would need to store and use the network private key.”). Nair also teaches the benefits of using multiple keys to map to multiple HSS allows an operator to manage different groups of users in different HSSs/UDMs. Ex. 1004, ¶[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. ... The SLF analyzes the authentication request for a user received from the MME/AMF and routes it to the correct HSS.”); Ex. 1008, 5:7-10. In my opinion, Nair’s teachings would lead a POSITA to seek Forsberg for its teachings of an identifier to support this use of multiple keys in the encryption process.

48. Accordingly, 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, ¶¶[0055] (“[A] valid public key and secret key pair along with a key identifier may be sent in message 4 to the requesting mobile

management entity. 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 (e.g. similar to the key set identifier, KSI).”), [0049] (“Other information, such as information about public key identifiers may also be included in the response.”), [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] (“A validly authenticated network can then update the user equipment with a valid new public key, *key identifier* and other information with a validity period.”); *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. Due to the express teachings of Forsberg, a POSITA would have understood the benefits of applying public key identifiers to manage the implementation of multiple keys as taught by Nair.

49. A POSITA would have understood that 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. 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.

50. Thus, in my opinion, a POSITA would have been motivated to implement 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, as taught by Nair.

51. For the same reasons discussed in the preceding paragraphs, Nair provides teaching, suggestion, and motivation that would have led a POSITA to combine its teachings with Forsberg to arrive at the combined Nair-Forsberg system.

52. A POSITA would also be motivated to include the decrypted (or clear-text) IMSI as part of Nair's authenticator vector as taught by Forsberg. In view of the teachings of Forsberg, a POSITA would have been motivated to include the decrypted IMSI (*i.e.*, SUPI) in (or along with) the authentication vectors sent by Nair's SLF (Figs. 4-6) (de-concealing server) to the AUSF (Fig. 6), AMF (Fig. 4), or AMF/MME (Fig. 5_ (authentication servers). As Forsberg explains, the decrypted identifier is sent back to aid in the "authentication of a visiting user equipment." Ex. 1005, ¶[0047]. This is because the decrypted IMSI (*i.e.*, SUPI) contains the permanent subscriber identity for the UE, which allows the authentication server to

identify the UE and determine whether the UE should be granted access. A POSITA would be motivated to apply that benefit to Nair's system. The combination represents combining prior art elements (Nair's authentication method and system with Forsberg's method of transfer the decrypted identifier back to the authentication server) according to known methods to yield predictable results (authenticating a visiting UE).

53. Additionally, a POSITA would have understood 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) based on complimentary and overlapping disclosures in Nair and Forsberg and for the reasons stated above. 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).

54. Finally, 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. In the proposed combination, each element merely performs the same function as it does separately. Thus, incorporating 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.

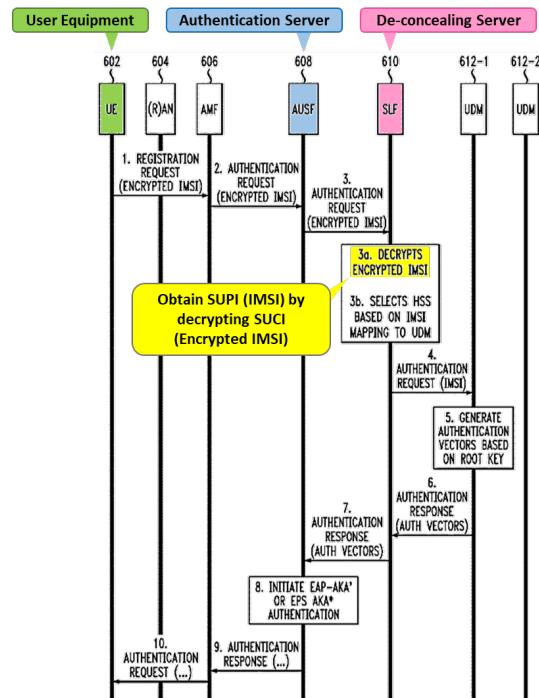
2. Independent Claim 1

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

55. In my opinion, Nair discloses this limitation. Nair discloses a method performed by an authentication server (Nair's "Authentication and Security Function" or "AUSF") in a home network of a user equipment (UE) for obtaining a SUPI" (Nair's "IMSI"). There can be no doubt that Nair's IMSI is an example of a claimed SUPI because the 817 patent explains that the claimed SUPI "may be IMSI-based," and [e]mbodiments that include an IMSI-based SUPI may use the IMSI" described by the 3GPP standards. Ex. 1001, 8:20-24; Ex. 1004, ¶[0032].

56. As shown in Figure 6, Nair "shows a message flow for a user equipment authentication procedure for a 5G network." Ex. 1004, ¶¶[0024], [0077] ("Fig. 6

illustrates a high-level UE authentication procedure ... in 5G using encrypted IMSI...”); Ex. 1008, 13:17-18.



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

57. Figure 6 illustrates that the UE “sends a registration request” to the home network’s AMF 606 in Step 1 to register itself with the network. Ex. 1004, ¶[0078]; Ex. 1008, Fig. 6. The UE 602 encrypts the IMSI (or SUPI) as part of the registration request message sent to the AMF. Ex. 1004, ¶[0078]; Ex. 1008, 4:29-30. The “AMF 606 then sends an authentication request (encrypted IMSI) to AUSF 608 in Step 2.” Ex. 1004, ¶[0078]; Ex. 1008, 15:22-24, Fig 6. The AUSF is the “Authentication and Security Function (AUSF).” Ex. 1004, ¶[0033]. In the context

of the '817 patent the AUSF is an example of the claimed "authentication server."
Ex. 1001 at 6:45-49, Fig. 6.

58. Nair's AUSF is in the home network of the UE. Ex. 1004, ¶[0033] ("[T]he home subscriber server/function ... in a 5G network ... is called User Data Management (UDM) which may also comprise an Authentication and Security Function (AUSF)"); Ex. 1008, 4:18-22.

59. The AUSF (or authentication server) "sends the authentication request (encrypted IMSI) to SLF 610." Ex. 1004, ¶[0078]; Ex. 1008. Nair's SLF 610 is a de-concealing server, as I explain below for element 1[f]. The non-encrypted IMSI (or SUPI) is found when the "SLF 610 decrypts the encrypted IMSI." Ex. 1004, ¶[0078]; Ex. 1008, 5:23-30, Fig. 6.

60. In my opinion, Nair's other embodiments also disclose this limitation for the same reasons discussed above. In the embodiments of Figure 4 the AMF, and in Figure 5 the AMF/MME, are an "authentication server." Ex. 1004, ¶¶[0072-0076]; Ex. 1008 Figs. 4-5. Like the embodiment of Figure 6, the AMF or AMF/MME receive the registration/attach request containing encrypted IMSI. And like in Figure 6, the AMF or AMF/MME in Figures 4 and 5 sends the authentication request containing the encrypted IMSI to the SLF to decrypt the encrypted IMSI to obtain the unencrypted IMSI. Ex. 1004, ¶¶[0072-0076], Figs 4-5; Ex. 1008, Figs. 4-5.

61. 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. *See, e.g.*, Ex. 1004, ¶¶[0010], [0014], [0016], [0039-0040], [0044], [0046], [0048]. When discussing 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. *See* Ex. 1004 ¶¶[38-39], [0041-0049], [0073], [0076], [0078], Figs. 4-6.

2. 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

62. In my opinion, Nair discloses this limitation. As I discussed above for the preamble, Nair discloses an “IMSI” that is a SUPI. Nair’s IMSI is a “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, e.g.*, Ex. 1004, ¶¶[0042] (“SUPI (Subscription Permanent Identifier of the UE)”), [0079–80]; Ex. 1008, 4:14-15.

63. Nair explains it’s IMSI is “a permanent subscription identifier (subscriber identity) of a UE.” Ex. 1004, ¶[0032]; Ex. 1008, 4:14-15. Moreover,

Nair's IMSI is a globally unique identifier allocated to a subscriber, as was standard practice in the telecommunications industry at the time. Ex. 1004, ¶¶[0038], [0042]; Ex. 1008, 4:14-17, 5:24-29; Ex. 1013, §5.9.2 at 63. As explained in the 3GPP standards document TS 23.501 (V0.4.0), which is incorporated by reference into Nair, (Ex. 1004 ¶[0006), "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. Moreover, TS 23.501 makes clear that the IMSI, identifies the subscriber specifically. *See id.* ("The 5G system supports identification of subscriptions independently of identification of the user equipment," which are instead identified by "a Permanent Equipment Identifier"). For these reasons, a POSITA would have understood that Nair's IMSI is a globally unique identifier allocated to a subscriber.

64. Further, Nair's IMSI includes a home network identifier identifying a home network of the subscriber. Specifically, Nair teaches that the IMSI comprises a 3-digit Mobile Country Code (MCC) and a 3-digit Mobile Network Code (MNC), which collectively are a home network identifier identifying the home network of the subscriber. Ex. 1004, ¶¶[0032]; ("IMSI ... consists of a 3-digit Mobile Country Code (MCC) [and] a 3-digit Mobile Network Code (MNC)"), [0035] ("MNC+MCC is needed by the serving network to route to the correct home network"); Ex. 1008, 4:15-17, 4:29-31; *see also* Ex. 1013, §5.9.2 at 63 ("In order to enable roaming

scenarios, the SUPI shall contains [*sic*] the address of the home network (e.g. the MCC and MNC in the case of an IMSI based SUPI.”). Indeed, Nair’s home network identifier as that disclosed in the ’817 patent. Ex. 1001, Fig 3 (below annotated), 2:24–29 (“the MCC and the MNC are the home network identifier”), Cl. 6.

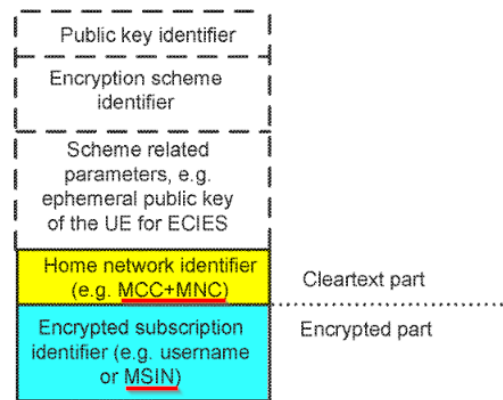


Fig. 3

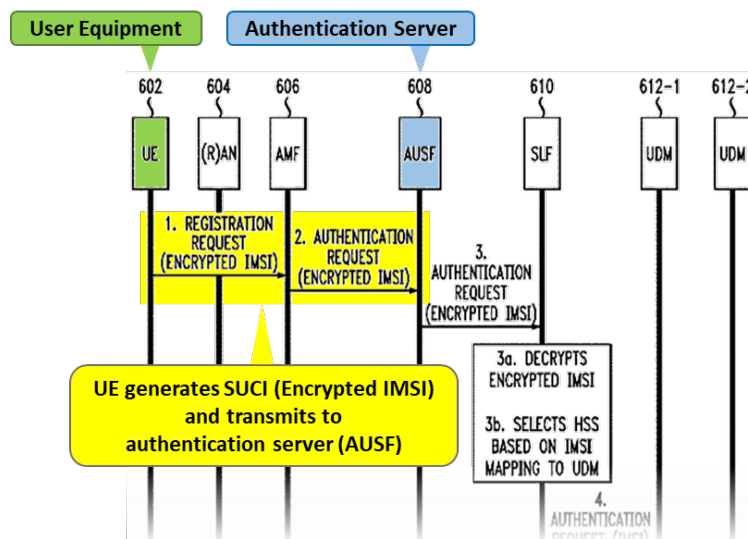
Id.

65. Additionally, Nair’s IMSI includes a subscription identifier identifying a subscription within the home network. For example, Nair teaches that the IMSI also comprises a 9-digit Mobile Station Identification Number that is allocated to the subscriber and identifies the subscriber’s subscription within the home network. Ex. 1004, ¶[0032]; (“IMSI ... consists of ... a 9-digit Mobile Station Identification Number (MSIN).”); Ex. 1008, 4:14-17. Nair’s MSIN is the same subscription identifier disclosed in the ’817 Patent. Ex. 1001, Fig 3, 8:62-66 (“an encrypted subscription identifier, such as an MSIN”), Cl. 6.

3. Element [1c]: the method comprising: the

**authentication server receiving a subscription
concealed identifier (SUCI) generated by the UE**

66. In my opinion, Nair discloses this limitation. Nair discloses that the AUSF receives a SUCI, which corresponds to 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. 1004, Fig. 6 (annotated); Ex. 1008, Fig. 6. As shown in Figure 6. Nair teaches 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 contains an encrypted IMSI, which is generated by the UE by encrypting the IMSI. Ex. 1004, ¶[0078]; Ex. 1008, 4:28-5:1.

67. Next, the AUSF 608 receives the authentication request with the encrypted IMSI generated by the UE in step 2. Ex. 1004, ¶[0078] (“AMF 606 then sends an authentication request (encrypted IMSI) to AUSF 608.”; Ex. 1008, Fig. 6.

68. In my opinion, Nair’s alternative embodiments also disclose this limitation. For example, in Figure 4, the UE generates an encrypted IMSI and “sends a registration request (encrypted IMSI) ... to AMF 406 [*i.e.*, the authentication server].” Ex. 1004, ¶[0073], Fig. 4; Ex. 1008, Fig. 4. And in Figure 5, the UE generates an encrypted IMSI and “sends an attach request (encrypted IMSI) ... to AMF/MME 506 [*i.e.*, the authentication server].” Ex. 1004, ¶[0076], Fig. 5; Ex. 1008, Fig. 5.

4. 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;

69. In my opinion, Nair in combination with Forsberg renders this element obvious. Nair expressly teaches each sub-element of this element except Nair does not provide explicit disclosure of “a public key identifier.” In my opinion, it would have been obvious to use a public key identifier with Nair’s encrypted IMSI as discussed above. As I discussed above for limitation 1[c], Nair discloses an authentication message generated by UE that includes the “encrypted IMSI” and privacy indicator (collectively, the claimed SUCI).

70. Nair teaches its authentication message has an encrypted part and a non-encrypted (*i.e.*, clear-text) part. *See* Ex. 1004, ¶¶[0035] (“Only the MSIN part [of the IMSI] needs to be encrypted, because MNC+MCC is needed by the serving network”), [0038] (“Thus, in a 5G network with permanent subscriber identity (e.g., IMSI) encrypted by one of the methods, an SLF would need to take over the decryption of the MSIN part of the IMSI.”); [0043] (“[T]he 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.”); [0073]); Ex. 1008, 4:29-5:1. Nair’s Encrypted IMSI is generated from a IMSI, which comprises a 3-digit MCC, 3-digit MNC, and 9-digit MSIN, as I showed for limitation 1[b]. I note that Nair uses the term “encrypted IMSI” to refer to the entire IMSI even though only the MSIN

portion is typically encrypted. Ex. 1004, ¶[0073]. Thus, a POSITA would understand the “encrypted IMSI” includes a clear-text portion.

- a) **Encrypted part comprises the subscription identifier but the encrypted part of the SUCI generated by the UE does not include the home network identifier and**
- b) **Clear-text part comprises the home network identifier:**

71. Nair discloses encrypting the subscription identifier (i.e., the MSIN), but the home network identifier (i.e., MNC+MCC). *See* Ex. 1004, ¶¶[0035] (“encrypt the subscriber identity, which is, by way of example, the MSIN part of IMSI”), [0038] (“[I]n a 5G network with permanent subscriber identity (e.g., IMSI) encrypted by one of the methods [of Nair], an SLF would need to take over the *decryption of the MSIN part* of the IMSI.”), [0041] (“MSIN is provided in encrypted form”), [0043] (“decrypt the MSIN part to form the real unencrypted IMSI”); Ex. 1008, 4:29-30, 5:24-26, 6:26-27.

72. Nair discloses that the encrypted part of the authentication request does not include the MNC+MCC (collectively, the home network identifier). 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. Thus, in my opinion, Nair discloses limitation

explicitly. Moreover, A POSITA would have understood that disclosure to mean the unencrypted MNC+MCC is needed. Nair does not teach an embodiment in which the MNC or MCC are encrypted. 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. The AUSF needs to know the home network of the subscriber so that it can find the correct decryption server. For that reason, encrypting the “home network identifier” would defeat the purpose of including it in the SUCI.

b) ii) Clear-text part comprises an encryption scheme identifier:

73. In my opinion, Nair teaches this limitation. Nair discloses that the clear-text part of the authentication request comprises an encryption scheme identifier. For example, Nair teaches inclusion of an “identity privacy flag” (which is also called a “privacy indicator” by Nair) to indicate to the core network whether the MSIN is encrypted. 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. Nair discloses both an “‘explicit’ privacy indicator,” such as “a flag or field” and

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].

74. In my opinion, a POSITA would have understood that both the explicit and implicit privacy indicators are an encryption scheme identifier because both methods “identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI,” which is how the ‘817 patent describes the encryption scheme identifier. Ex. 1001 at Abstract, 4:20-25. Nair discloses the privacy indicator is contained in the clear-text of the SUCI by teaching 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]. Nair also teaches that including a privacy indicator indicating the null-encryption scheme has been used to encrypt a message “saves processing time” and requires “fewer resources” by informing the SLF it need not attempt decryption when a null-encryption scheme has been used. *Id.*

75. 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], Cl. 4 (“[R]esponsive to the flag indicating that the subscription identifier is privacy-protected, removing the privacy protection from the subscription identifier in the attach request.”).

76. 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. Otherwise, the SLF would be unable to decrypt since decryption requires knowledge of the particular encryption scheme used to encrypt the IMSI. For example, 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 requires that the privacy indicator means the same encryption scheme to both the UE and SLF. Accordingly, a POSITA would have understood that Nair teaches that the privacy indicator indicates the encryption scheme used by the UE to encrypt the subscription identifier.

77. To the extent Patent Owner argues that Nair does not require that the UE and SLF understand which encryption is used when the privacy indicator is

flagged,² 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. A POSITA would be motivated to do 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. 1004, ¶¶ [0042-0043].

78. Furthermore, Nair also discloses that one encryption scheme identified by the privacy indicator is the "null-encryption scheme," in which the "input equals the output." Ex. 1004, ¶[0042]. In my opinion, Nair's privacy indicator is an encryption scheme identifier for the additional reason that it indicates whether the null-encryption scheme is used, or the other encryption scheme is used, to aid the de-concealing server in processing received messages. 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. As discussed in Section VI.A, the '817 patent expressly discloses that the null-encryption scheme is one encryption

² For the reasons discussed above, I disagree. If the UE and SLF did not both understand what encryption scheme is indicated by the privacy indicator then the SLF would not be able to decrypt the SUCI. Such a network scheme would be non-functional and illogical.

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 (“[T]he encrypted part of the SUCI may use a null encryption scheme....”), 15:7-9 (“[T]he UE uses a null-scheme or null-encryption method to create the SUCI.”). Moreover, the ’817 patent 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 (“Each scheme adopted as standard may be assigned a specific *identifier*. For example, the null-scheme may be assigned a 0, ECIES may be assigned a 1, and so on.”) & Figs. 4, 5, and 15. Nair’s privacy indicator is therefore the claimed encryption scheme identifier in my opinion.

79. As I explained above, 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. Nair discloses:

It is to be appreciated that the privacy indicator, in addition to being an “explicit” privacy indicator such as a flag or field, can *alternatively be an “implicit” privacy indicator*. By implicit privacy indicator, it is meant that the *privacy feature is conveyed by the UE* to a network element/function via the algorithm used to encrypt the message. Thus, the network element/function receiving the message from the UE is informed of the privacy feature by the fact that *the message is encrypted with a*

particular encryption algorithm. This also applies to a null-encryption scheme. In a null-encryption scheme, the input equals the output, and the SUPI (Subscription Permanent Identifier of the UE) is unencrypted, i.e., a format-preserved scheme. One could interpret this as the SUPI (or IMSI) is always encrypted, but if no privacy is “switched on,” then the null-encryption is used. Thus, the privacy indicator would implicitly reside in the algorithm scheme used (e.g., null-encryption or an algorithm that actually encrypts a message).

x. 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, it would have been obvious to include explicit identification of a *non-null* encryption scheme in view of Nair’s teachings, especially when starting with a system that has only one non-null encryption scheme available. Nair’s privacy indicator is designed to give the decryption severer (e.g., the SLF) the requisite information to decrypt the IMSI. Ex. 1004, ¶¶[0042-43]. Nair also recognizes the benefit of saving time and resources that would be wasted if the SLF attempted to use an incorrect encryption scheme. Ex. 1004, ¶¶[0042-43]. A POSITA would thus have been motivated to use a privacy indicator that explicitly indicates which scheme used to encrypt the IMSI.

80. For example, Nair teaching of a “field” that indicates which encryption scheme is used renders obvious an explicit privacy indicator that would indicate

which of the numerous well-known encryption algorithms was used for encryption. Nair teaches that an “explicit’ privacy indicator” may be “a flag or *field*.” Ex. 1004, ¶¶[0042], [0044] (“identify privacy flag or other privacy indicator”); Ex. 1008, 6:18. In the context of Nair, the term “flag” is a binary, yes-or-no value. Ex. 1004, ¶¶[0010] (“a flag indicating *whether* 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. In contrast, “field” is a value that can contain multiple bits, and thus can represent more values than “0” or “1.” *See* Ex. 1004, ¶¶[0046]; Ex. 1008, 8:1-3. A POSITA would have understood that a field with multiple values would be beneficially used to indicate which of a plurality of non-null schemes is used.

81. Nair also recognizes that multiple non-null-encryption schemes existed. Ex. 1004, ¶[0042]; Ex. 1008, 2:4-8; Ex. 1007 at §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”). A POSITA would have been well aware that multiple encryption schemes were known. As I explained above, a POSITA would have known that the SLF would need to know the type of encryption used to encrypt the IMSI. Accordingly, 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 IMSI,

particularly in view of the teachings of Nair—i.e., that explicit privacy indicator may be a “field,” in addition to a binary “flag.”

b) iii) Clear-text part comprises public key identifier:

82. In my opinion, Nair in combination of Forsberg renders obvious this limitation. As I discuss below, Forsberg discloses a clear-text public key identifier.

83. Nair teaches that it’s MSIN is encrypted by the “UE using the public key of the home network.” Ex. 1004, ¶¶[0030], [0034], [0035] (“In the home network public key based solution, the home operator provides its public key to all home network subscribers. They will use it to encrypt the [MSIN]”), claim 6 (“the privacy-protected identifier that is encrypted utilizing a public key of a home network”); Ex. 1008, 4:10-13, 4:28-5:6.

84. Similarly, Forsberg discloses an UE identification message comprising encrypted IMSI for registering and authenticating a UE with a network. Ex. 1005, ¶¶[0039], [0049]. Like Nair, Forsberg teaches that the MSIN portion of the IMSI is encrypted. *Id.* ¶[0049]. Forsberg also teaches that the MCC and MNC portions of the IMSI are not encrypted. *Id.* ¶[0051]. [0053-0054],

85. Additionally, Forsberg that the 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] (“Other information, such as information about public

key identifiers may also be included in the response.”), [0055] (“[A] valid public key and secret key pair along with a key identifier may be sent in message 4 to the requesting mobile management entity. 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 (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] (“A validly authenticated network can then update the user equipment with a valid new public key, key identifier and other information with a validity period.”); *see also* Figs. 4 & 5 (depicting the transmission of a user identity response comprising encrypted IMSI and a public key identifier (PK-Id)).

86. For these reasons, it is my opinion that Forsberg discloses a SUCI with an encrypted subscription identifier (*i.e.*, encrypted MSIN) and a clear-text home identifier (*i.e.*, MCC+MNC) and public-key identifier.

87. As I explained above, it would have been obvious to a POSITA to add Forsberg’s clear-text public key indicator to Nair’s SUCI (*i.e.*, the “encrypted IMSI” and privacy indicator information) to identify which specific public key of the home network was used by the UE to encrypt the MSIN. *See* Section []. Doing so would

allow the home network to use the appropriate corresponding private key for decryption in networks that used multiple public keys. *Id.*

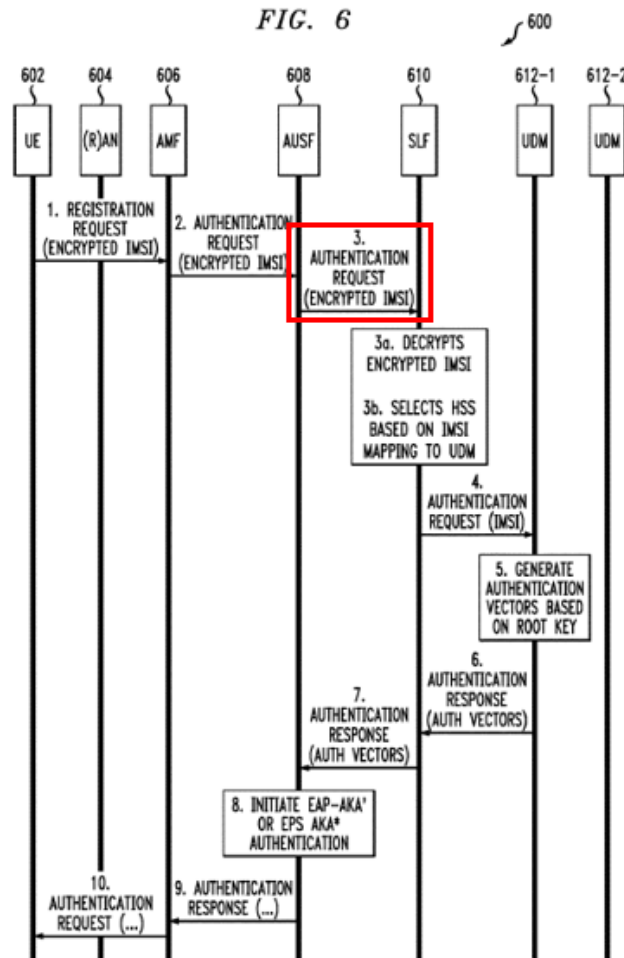
**Clear-text part does not comprise subscriber
identifier:**

88. In my opinion, Nair discloses 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] (“encrypted IMSI ... can refer to *the portion of the IMSI that is typically encrypted, e.g., MSIN*, or all or other parts of IMSI”), [0076], [0078]; Ex. 1008, 4:30, 6:25-28 (“[T]he 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.”).

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

89. In my opinion, Nair discloses this element. Nair teaches that the AUSF determines which SLF is used to decrypt the encrypted part of the SUCI. 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 discloses that the network may have multiple SLF’s. Ex. 1004, ¶¶[0057] (“[A]lthough only a single ... SLF ... [is] shown in the Fig. 1 embodiment, this is for simplicity and clarity only. A given alternative embodiment

may of course include larger numbers of such system elements, as well as additional or alternative elements of a type commonly associated with conventional system implementations.”), [0067], [0085]; Ex. 1008, 10:14–20. A POSITA would therefore have understood that the AUSF would necessarily determine which SLF is used for decryption in a multi-SLF system in order to make the authentication request. The AUSF cannot “send[] the authentication request” (Ex. 1004 ¶ [0078]) without first determining where to send the request.



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

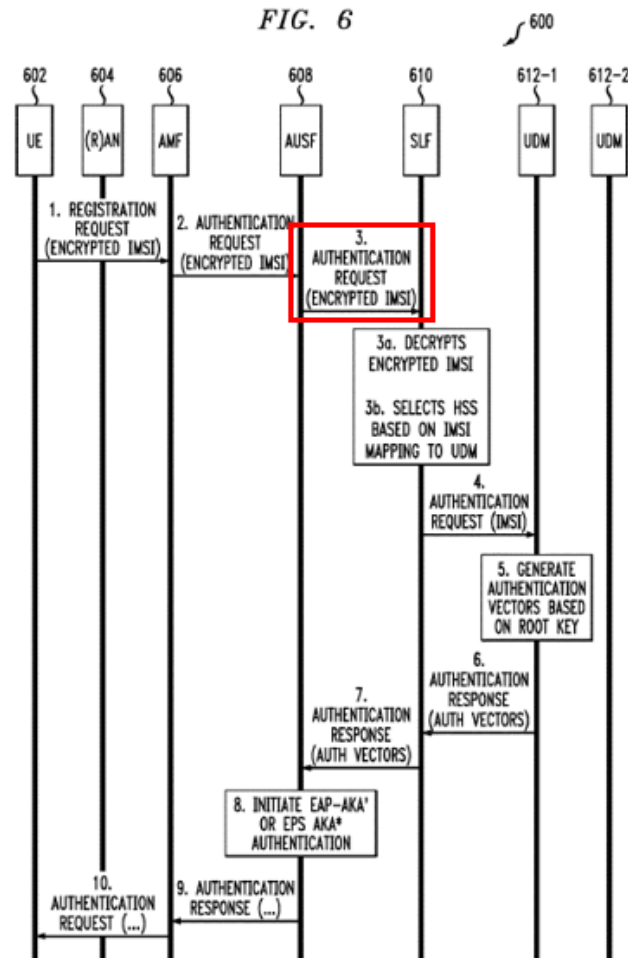
90. To the extent Patent Owner argues that Nair does not inherently disclose this feature, it would have been obvious to a POSITA for the AUSF to make that determination for the same reason. As shown in Figure 6, there is no other server between the AUSF and the SLF to make such a determination. Accordingly, the AUSF is the logical and obvious choice.

91. Nair's embodiments of Figures 4 and 5 disclose and render obvious this limitation for the same reasons. In the embodiments depicted in Figures 4 and, an AMF (Fig. 4) or AMF/MME (Fig. 5) (*i.e.*, the authentication server) receives encrypted IMSI (*i.e.*, SUCI) as part of an authentication request. Nair discloses that the AMF or AMF/MME then forwards the request to a SLF (*i.e.*, de-concealing server) for decryption. Ex. 1004, ¶¶[0072-76]; Ex. 1008, Figs. 4 & 5. Nair further discloses that the network may have multiple SLF's (Ex. 1004, ¶[0057]; Ex. 1008, 10:14–20) and thus a POSITA would have understood that the AUSF would necessarily determine which SLF to use for decryption in a multi-SLF system in order to make the authentication request. To the extent 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 reasons discussed above for Figure 6.

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

92. In my opinion, Nair discloses that the authentication server sending the SUCI to the de-concealing server. For example, Nair teaches that the AUSF sends

the encrypted IMSI to the SLF. Ex. 1004 ¶[0078], Fig. 6, *see also* ¶ [0038] (“[I]n a 5G network with permanent subscriber identity (e.g., IMSI) encrypted by one of the methods, an SLF would need to take over the decryption of the MSIN part of the IMSI.”); Ex. 1008, 13:18-20, Fig. 6.



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

93. Nair’s embodiments of Figures 4 and 5 disclose and render obvious this limitation for the same reasons. In the embodiments depicted in Figures 4 and, an AMF (Fig. 4) or AMF/MME (Fig. 5) (*i.e.*, the authentication server) receives

encrypted IMSI (*i.e.*, SUCI) as part of an authentication request. Nair discloses that the AMF or AMF/MME then forwards the request to a SLF (*i.e.*, de-concealing server) for decryption. Ex. 1004, ¶¶[0072-76]; Ex. 1008, Figs. 4 & 5.

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

94. In my opinion, Nair in view of Forsberg renders obvious this element.

95. Nair discloses that an SLF (*i.e.*, de-concealing server) provides authentication vectors to an AUSF after decryption of the IMSI. 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. ... [I]n step 7, SLF 610 sends the authentication response (AVs) to AUSF 608.”), Fig. 6; Ex. 1008, 5:8-9, 9:17-20, Fig. 6. In Nair’s Figures 4 and 5, the SLF provides authentication vectors to an AMF (Fig. 4) or AMF/MME (Fig. 5) (*i.e.*, the authentication server) after decryption of the IMSI. Ex. 1004, ¶¶[0072-76].

96. Forsberg discloses that “after the authentication server sends the SUCI to the de-concealing server, the authentication server recei[ceives] the SUPI in response.” Like Nair, Forsberg discloses that upon receiving the UE’s encrypted IMSI, the visited MME (*i.e.*, authentication server) sends an authentication request to the UE’s “home operator mobile management entity” (*i.e.*, a de-concealing server) via message 3, which contains the encrypted IMSI (*i.e.*, SUCI). Ex. 1005, ¶[0051]

(“The mobile management entity can nevertheless determine the home network of the user equipment sending message 2 based on information available to it and request for assistance in the decryption by contacting the home operator mobile management entity by means of message 3. 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 UE’s home network decrypts the IMSI and sends the decrypted IMSI back to the authentication server. *Id.*, ¶¶[0047] (“The decrypted identifier is then sent in clear format to the requestor at 204 for use e.g. in authentication of a visiting user equipment.”), [0054] (“In response to message 3 the home mobile management entity can then decrypt the MSIN part and send the IMSI in a clear text format back in message 4 to the visited mobile management entity.”), Figs. 3 & 4.

97. As I explained above in Section [], a POSITA would have been motivated to include the decrypted IMSI (*i.e.*, SUPI) in (or along with) the authentication vectors sent by Nair’s SLF (Figs. 4-6) (de-concealing server) to the AUSF (Fig. 6), AMF (Fig. 4), or AMF/MME (Fig. 5_ (authentication servers) in view of the teachings of Forsberg. As Forsberg explains, the decrypted identifier is sent back to aid in the “authentication of a visiting user equipment.” Ex. 1005, ¶[0047]. For example, the decrypted SUPI may be used to route the authentication vectors to the requesting UE associated with the SUPI more accurately and

expeditiously. A POSITA would be motivated to apply that benefit to Nair's system. The combination represents combining prior art elements (Nair's authentication method and system with Forsberg's method of transfer the decrypted identifier back to the authentication server) according to known methods to yield predictable results (authenticating a visiting UE).

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.**

98. In my opinion, both Nair and Forsberg individually discloses this claim limitation and also render it obvious individually and collectively. Nair explicitly discloses multiple SLFs (which are "a plurality of de-concealing servers) because Nair explains that there "may of course" of each system elements, which includes SLF elements. Ex. 1004, ¶[0057] ("[A]lthough only single UE, eNB/gNB, MME/AMF, **SLF**, SGW/SMF and PGW elements are 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, as well as additional or alternative elements of a type commonly associated with conventional system implementations."); Ex. 1008, 10:14-20.

99. Further, Nair discloses that information received from the UE is used to determine the SLF (the claimed de-concealing server). For example, Nair

discloses that the MNC and MCC sent in the UE's authentication request is used to route to request to the correct home network. 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."), [0037] ("[I]n a 5G network with permanent subscriber identity (e.g., IMSI) encrypted by one of the methods, an SLF would need to take over the decryption of the MSIN part of the IMSI. Further, the SLF would need to keep a database of all subscribers' profiles with the routing information, i.e., a profile should map a subscribers' permanent identity (e.g., IMSI) to one of the HSSs in the network to forward the Authentication Request after decrypting the received (encrypted) IMSI."); Ex. 1008, 4:29-5:2, 5:9-10. A POSITA would have understood that in a system includes multiple SLFs and multiple home networks routing an authentication request to the correct home network using the UE's MCC and MNC would therefore require first determining the SLF configured to provide the UE information to that home network. Ex. 1004, ¶[0057]

100. Additionally, Forsberg discloses this element, in my opinion, through its teaching that a mobile management entity may determine the UE's home mobile management entity by analy[zing] the mobile country code (MCC) and/or mobile network code (MNC)" from the UE.. Ex. 1005, ¶¶[0053] ("The visited mobile management entity may resolve the necessary details of the home mobile management entity by analysing a network specific information part of message 2.

For example, the visited mobile management entity may analyse the mobile country code (MCC) and/or mobile network code (MNC) of the IMSI to see if it is acting as a visited mobile management entity or the home mobile management entity for the user equipment, and if not, which network it should contact for help.”); [0051] (“The mobile management entity may realise that the user equipment is a roaming using equipment, and/or that it does not possess enough information to decrypt the encrypted portions of the IMSI identifier. The mobile management entity can nevertheless determine the home network of the user equipment sending message 2 based on information available to it and request for assistance in the decryption by contacting the home operator mobile management entity by means of message 3.”).

101. Forsberg teaches that a UE that receives a user-identity request from the Visited-MME (*i.e.*, an authentication server) as part of the process of registering with a communications network. Ex. 1005, ¶[0048]. The UE responds by sending its identity, which includes the encrypted IMSI and a public key identifier, to the Visited-MME. *Id.*, ¶[0049]. If the Visited-MME is not part of the UE’s home network, it uses 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 to decrypt the UE’s identity. *Id.*, ¶¶[0051], [0053]. The Home-MME (*i.e.*, a de-concealing server) decrypts the UE’s IMSI and sends the

unencrypted IMSI back to the Visited-MME (*i.e.*, authentication server) for use in completing the UE authentication process. *Id.*, ¶[0054]; *see also* Figs. 2-4.

102. For these reasons, in my opinion, a POSITA would have found it obvious to incorporate the functionality taught by Forsberg into Nair. 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, as Forsberg explains. In my opinion, the combination thus represents combining prior art elements according to known methods to yield predictable results.

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.**

103. In my opinion, Nair discloses receiving the SUCI from the UE as part of a registration procedure for registering the UE with a wireless communication network. For example, Nair discloses transmitting a SUCI (Encrypted IMSI and associated indicators/flags) as part of an attach request for registering a UE with a wireless communications network. Ex. 1004, ¶¶[0004-0005], [0006] (“In an example communication system, user equipment (5G UE in a 5G network or, more broadly, a UE) such as a mobile terminal (subscriber) communicates over an air interface with a base station or access point referred to as a gNB in a 5G network.”),

[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.

104. In my opinion, Nair discloses receiving the SUCI from the UE via an authentication request from a Security Anchor Function. Ex. 1004, ¶¶[0077-0078], Fig. 6. Nair's Figure 6 discloses an authentication server (AUSF) receiving an authentication request comprising encrypted IMSI (a claimed SUCI) from an AMF, which Nair discloses implements a Security Anchor Function (SEAF). Ex. 1004, ¶¶[0077-0078], Fig. 6; *see also* Figs. 4 (depicting an authentication request comprising encrypted IMSI from an AMF) & Fig. 5 (depicting an authentication request comprising encrypted IMSI from an AMF/MME); Ex. 1008, Figs. 4-6.

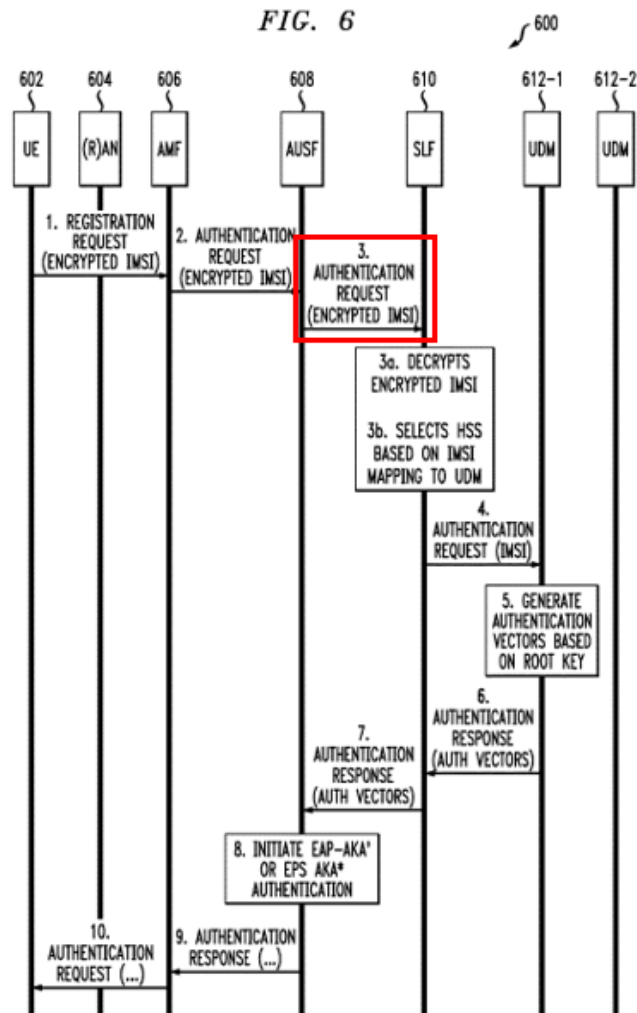
105. Nair further teaches that in embodiments wherein the UE authentication request includes privacy indicators, an MME/SEAF (Security Anchor Function) "handle[s] the enhanced initial attach message from the UE." Ex. 1004, ¶[0046] ("The MME/SEAF (SEAF is a Security Anchor Function) has to handle the enhanced initial attach message from the UE, form the UE Authentication Request message, and route it to the home network for requesting the AV."); Ex. 1008, 7:29-8:1. Nair also explains that the SEAF may be alternatively implemented with the Access and Mobility Management Function (AMF). Ex. 1004, ¶[0053] ("SEAF can

be implemented with the AMF connecting a UE with the mobility management. A mobility management function ... manages, among other network operations, access and *authentication operations with the UE* (through the access point 104).”); Ex. 1008, 9:14-21; *see also* Ex. 1013, §6.2.1 at 75 (stating that “Access and Mobility Management function (AMF) includes ... Security Anchor Function (SEA),” which “interacts with the AUSF and the UE.”). Nair’s Figure 6 shows that the AMF then sends the encrypted IMSI (a claimed SUCI) to the AUSF (a claimed authentication server) as part of an authentication request. Therefore, in my opinion, Nair discloses that when the AUSF (authentication server) receives the SUCI from the UE via an authentication request, that request is specifically from the Security Anchor Function of the AMF.

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.**

106. In my opinion, Nair discloses this limitation. As shown in Figure 6 below, Nair discloses sending the encrypted IMSI (*i.e.*, SUCI) and a request for authentication vectors for authenticating the UE together within message 3 as depicted in Fig. 6. Ex. 1004, Fig. 6; Ex. 1008, Fig. 6.



Ex. 1004, Fig. 6.

107. The Server Locating Function (SLF) (the de-concealing server) receives the authentication request and the encrypted IMSI in message 3 depicted in Fig. 6, performs the decryption (*i.e.*, de-concealing) function by decrypting 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] (“[I]n a 5G network with

permanent subscriber identity (e.g., IMSI) encrypted by one of the methods, an SLF would need to take over the decryption of the MSIN part of the IMSI. Further, the SLF would need to keep a database of all subscribers' profiles with the routing information, i.e., profile should map a subscriber's permanent identity (e.g., IMSI) to one of the HSSs in the network to forward the Authentication Request after decrypting the received (encrypted) IMSI.”), [0078] (“In step 3, AUSF 609 sends the authentication request (encrypted IMSI) to SLF 610. In step 3a, SLF 610 decrypts the encrypted IMSI In Step 3b, SLF 610 selects an HSS based on IMSI mapped to UDM. In Step 4, SLF 610 sends the authentication request (IMSI) to the selected UDM [and] [i]n Step 5, UDM 612-1 generates authentication vectors (Avs) based on a root key. In Step 6, UDM 612-1 sends an authentication response to SLF 610.”); Ex. 1008, 5:24-29, Fig. 6.

108. For these reasons, 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.

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 the subscription identifier is a Mobile Subscription Identification Number (MSIN)

109. In my opinion, Nair discloses this limitation. As I explained above with regard to limitation 1[b], Nair discloses that the Nair’s IMSI (*i.e.*, the SUPI)

comprises a home network identifier at includes an MCC and MNC. Ex. 1004, ¶[0032] (“[A]n International Mobile Subscriber Identity (IMSI) is a permanent subscription identifier (subscriber identity) of a UE.... [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), and a 9-digit Mobile Station Identification....”); Ex. 1008, 4:14-17; *see also* Ex. 1007, §5.7.3.9.1 at 341 (“IMSI is composed of three parts: [1] Mobile Country Code (MCC) consisting of three digits. The MCC identifies uniquely the country of domicile of the mobile subscriber; [and] [2] Mobile Network Code consisting of two or three digits for GSM/UMTS applications.”). The 3-digit MCC and the 3-digit MNC collectively are a 6-digit home network identifier because they are used to route to the user’s correct home network. 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.”); Ex. 1008, 4:30-5:1; *see also* Ex. 1007, §5.7.3.9.1 at 341.

110. Further, the 15-digit IMSI (SUPI) includes a subscriber identifier—an 9-digit MSIN. Ex. 1004, ¶[0032] (“[A]n International Mobile Subscriber Identity (IMSI) is a permanent subscription identifier (subscriber identity) of a UE. [T]he IMSI is a fixed 15-digit length and consists of a . . . 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.”).

8. Dependent Claim 8

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

111. In my opinion, Nair discloses this element because Nair incorporates through its incorporation by reference in its entirety of 3GPP TR 33.899 V1.1.0 (Release 14) (Ex. 1004, ¶[0007]; Ex. 1008, 2:4-9). TR 33.899 teaches encrypting the MSIN of a UE's IMSI using the Elliptic Curve Integrated Encryption Scheme (ECIES). TR 33.899 address the same problem addressed by Nair of protecting the privacy of 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. 1004, ¶[0007]. TR 33.899 discloses 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.

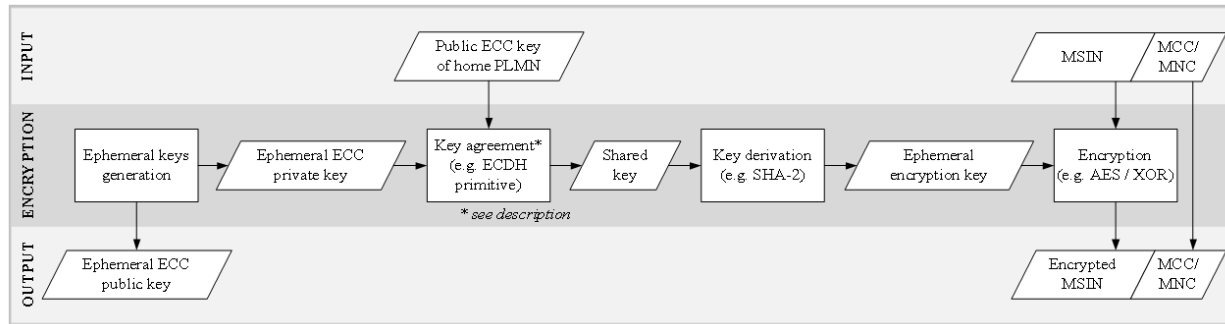


Figure 5.7.4.15.2-1: Encryption at the UE side (based on ECIES)

Id., Figure 5.7.4.15.2-1.

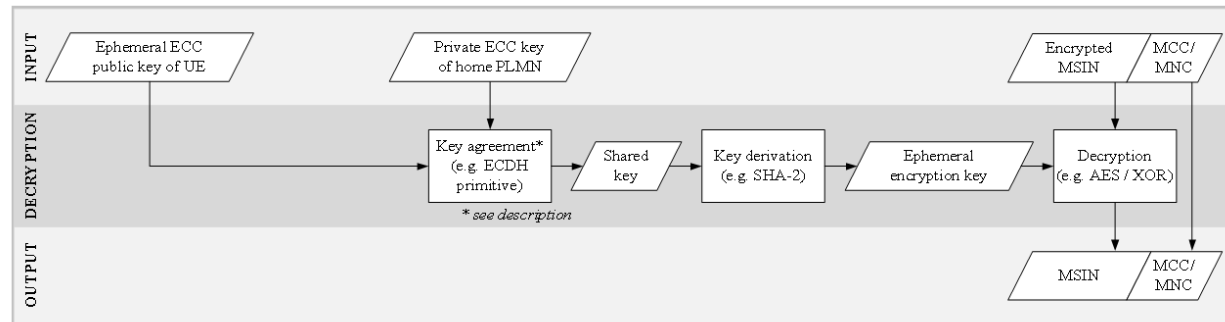


Figure 5.7.4.15.2-2: Decryption at the network side (based on ECIES)

Id., Figure 5.7.4.15.2-1.

9. Independent Claim 9

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

112. In my opinion, Nair in combination with Forsberg renders obvious the preamble for the reasons I discussed above for Element [1g].

1. **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**

113. In my opinion, Nair in combination with Forsberg renders this limitation for the reasons I discussed above for Element 1[b].

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

113. In my opinion, Nair in combination with Forsberg renders obvious this limitation for the reasons I discussed above for Elements 1[c] and 1[f]. In my above discussion of Element 1[c], I explain how Nair discloses a UE sending the SUCI to the authentication server and for Element 1[f] Nair in combination with Forsberg discloses an authentication server sending the SUCI that it received from the UE to the de-concealing server.

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

114. In my opinion, Nair in combination with Forsberg renders obvious this limitation for the reasons I discussed above for Element 1[d].

4. 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

115. In my opinion, Nair in combination with Forsberg renders obvious this limitation for the reasons I discussed above for Elements 1[d] and 1[e]. As I explained above, Nair discloses a concealing server that decrypts the encrypted part

of the SUCI (element 1[e]) using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI(element 1[d]).

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

116. In my opinion, Nair in combination with Forsberg renders obvious this limitation for the reasons I discussed above for Element 1[g].

10. Independent Claim 10

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

In my opinion, Nair discloses the preamble for the reasons I've discussed above with respect to Elements 1[a]-[c]. For example, Nair discloses that an UE sends the IMSI (which is a claimed SUPI) in concealed/encrypted form (*i.e.*, Nair's encrypted IMSI, which, along with the associated indicators/flags is a claimed SUCI) to an AMF (which is an authentication server) as depicted in Figs. 4-6.

1. 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

116. In my opinion, Nair in combination with Forsberg renders obvious this limitation for the reasons I discussed above for Element 1[b].

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

117. In my opinion, Nair in combination with Forsberg renders obvious this limitation for the reasons I discussed above for Element 1[c].

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

118. In my opinion, Nair in combination with Forsberg renders obvious this limitation for the reasons I discussed above for Element 1[d].

4. 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.

119. In my opinion, Nair in combination with Forsberg renders obvious this limitation for the reasons I discussed above for Elements 1[c] and 1[[]]. As I explain for Element 1[c] Nair in view of Forsberg teaches the transmission of the SUCI generated by the UE to an authentication server. And I discussed above for Element 1[f] Nair in view of Forsberg teaches the forwarding of the SUCI by the authentication server to the de-concealing server.

11. 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).

120. In my opinion, Nair in combination with Forsberg renders obvious this limitation for the reasons I discussed above for claim 3.

12. 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.

121. In my opinion, Nair discloses this limitation. Nair teaches that the UE is comprised of a hardware “Universal Integrated Circuit Card (UICC)” that “contains at least one Universal Subscriber Identity Module (USIM) and appropriate application software.” Ex. 1004, ¶[0051]; Ex. 1008, 9:2-4. Nair teaches:

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. Before the time of the alleged invention, the security features of the USIM were known for compliance with technical standard 3GPP TR 33.899 and were none to be a “tamper resistant secure hardware solution.” Ex. 1007, §5.5.4.1.2 at 323 (“[S]ubscription credentials together with the USIM application (or its equivalent(s) in 5G) and the network access algorithm used to access the 5G network through a 3GPP or non-3GPP accesses shall always be stored and processed in a tamper resistant secure hardware solution defined by ETSI SCP.”). A POSITA would understand that Nair’s USIM thus securely stores the IMSI and its related key, which are used to identify and authenticate subscribers to access networks, and uses those values to “process” or generate the subscription credentials, such as the SUCI. A POSITA would understand that “tamper resistant

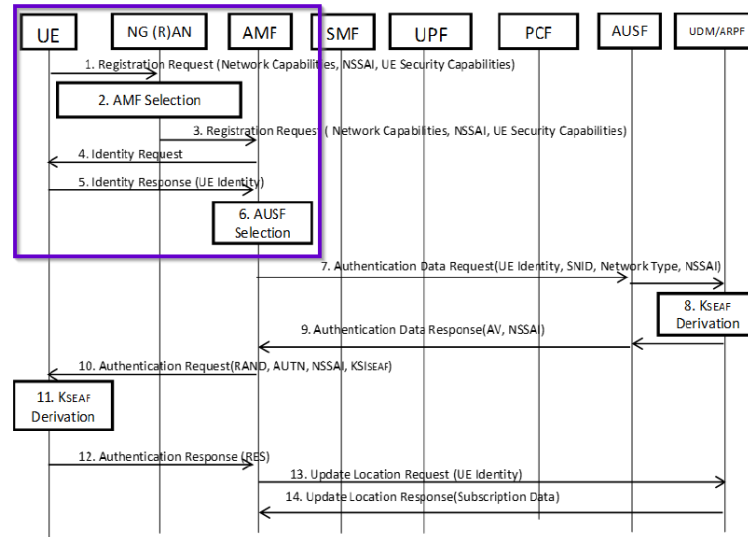
secure hardware component of the UE to generate the SUCI” because, as 3GPP TR 33.899 explains, the “subscription credentials” are “processed in a tamper resistant secure hardware solution.” Ex. 1007, §5.5.4.1.2 at 323.

13. 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.**

122. In my opinion, Nair discloses this limitation. Nair teaches an AMF performs a mobility management function for a communications system in a 5G network. Ex. 1004, ¶[0053] (“The access point 104 in this illustrative embodiment is operatively coupled to a mobility management function 106. In an LTE network, the function is typically implemented by a Mobility Management Element (MME), while in a 5G network, the function is implemented by an Access and Mobility Management Function (AMF).”); Ex. 1008, 9:14-17.

123. Nair also discloses this limitation through its incorporation by reference in its entirety of the TR 33.899 standard document. TR 33.899 teaches how to register a UE with the 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. As Figure 5.1.4.30.2-1 illustrates, the UE transmits a registration request to the AMF and the AMF “sends the Identity Request to the UE.” *Id.* Then “UE sends the Identity Response (UE Identity) to the AMF.” *Id.* at 120. In my opinion, a POSITA would have understood TR 33.899’s registration request is what Nair calls the “registration request” (or “attach request”). Ex. 1004, ¶[0078], Fig. 6. As I explained for claim elements 1[c] and 1[d], Nair teaches transmitting the SUCI to the authentication server as part of the registration request. It is therefore my opinion that Nair (including the incorporated TR 33.899) discloses “transmitting the SUCI to the authentication server in response to an identifier request message received from an [AMF].”

124. Additionally and alternatively, Forsberg discloses 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] (“[A] user equipment

indicates its willingness to use communication services provided by a network. The MME of the network then sends a message 1 to the user equipment to request for a user identity.”), Figs. 4 & 5. Then the UE sends the UE’s associated IMEI and IMSI to the MME. *Id.*, ¶[0049] (“The user equipment responds by returning a message 2 including an IMSI and IMEI associated with the user equipment.”), Figs. 4 & 5.

125. Forsberg further teaches that the 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] (“Other information, such as information about public key identifiers may also be included in the response. The user equipment sends at least a part of the identifiers encrypted. For example, at least the mobile subscriber identification number (MSIN) part of the IMSI may be transmitted as encrypted over the air interface.”). As explained in Nair, in a 5G system, the MME functionality is performed in the AMF. Ex. 1004, ¶[0053]; Ex. 1008, 9:14-17.

126. 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. A POSITA would have also 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 (which are a claimed SUCI) in such as combination.

14. Dependent Claim 14

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

127. I explained above for claim 8 that Nair discloses and renders obvious that the encryption scheme is an Elliptic Curve Integrated Encryption Scheme.

15. Independent Claim 15

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

128. As I explained above for elements 1[a] and [c], Nair discloses a UE for encrypting (concealing) the UE's IMSI (which is a 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,**

129. As I explained above for element 1[b], Nair discloses that 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.

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

130. In my opinion, Nair discloses this limitation. Ex. 1004, ¶¶[0050] (“The UE may 102 may be a mobile station, and such a mobile station may comprise, by way of example, a mobile telephone, or any other type of communication device.”), [0084-0085] (“The *processor, memory*, controller and other components of a user equipment ... of a communication system as disclosed herein may include well-known circuitry suitably modified to implement at least a portion of the identity request functionality [E]mbodiments may be implemented in the form of articles of manufacture each comprising one or more software programs that are executed *on processing circuitry of user equipment.*”); Ex. 1008, 2:24-27 (“[E]mbodiments are provided in the form of *non-transitory computer-readable storage medium* having embodied therein executable program code that when executed by a *processor causes the processor to perform the above steps.* Still further embodiments comprise apparatus with a *processor and a memory* configured to perform the above steps.”), 14:10-22.

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

131. In my opinion, Nair in view of Forsberg teaches this limitation, as I explained above with regard to elements 1[c]-1[d]. For example, I showed that Nair in view of Forsberg teaches that the SUCI is generated by the UE in the section above discussing element 1[c].

2. Element 15[e]: transmit the SUCI to an authentication

**server for forwarding of the SUCI to a de-concealing
server capable of decrypting the SUCI**

132. In my opinion, Nair in view of Forsberg teaches this limitation, as I explained above with regard to elements 1 [c], 1[e], and 1[f]. For example, I showed that Nair in view of Forsberg teaches that the authentication server receives a SUCI generated from the UE in the section above discussing element 1[c]. And I showed that it teaches that authentication server sending the SUCI to the de-concealing server in the in the section above discussing element 1[f] and that the de-concealing server is capable of decrypting the SUCI in in the section above discussing element 1[e].

16. Dependent Claim 16

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

As I explained above with regard to elements 1[b] and 6[a], Nair teaches that its SUPI (i.e., the IMSI or NAI) includes the MSIN.

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

133. In Section VIII.A.1, above, I explained why a POSITA would be motivated to combine Nair and Forsberg. In my opinion, a POSITA would have been further motivated to combine the complementary teachings of Nair, Forsberg, and Togawa for several reasons.

134. A POSITA would have been motivated to use Togawa's encryption scheme identifier in place of Nair's privacy indicator for several reasons. 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. Ex. 1004, ¶[0010] ("The message may comprise an attach request comprising a subscription identifier for a subscriber of the communication network associated with the user equipment, the one or more privacy indicators comprising a flag indicating whether the subscription identifier in the attach request is privacy-protected."), *with* Ex. 1006, 10:31-39 ("[T]he encryption-specification embedding unit 10f of the data transmitting apparatus 10 embeds an encryption key in a Voice signal. However, in place of the encryption key, information on an identifier for identifying the encryption key, information obtained by converting the encryption key by a predetermined method, information obtained by converting the identifier of the encryption key by a predetermined method, or like information can be embedded.").

135. 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. 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). 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.

136. A POSITA would have been motivated to improve Nair's privacy indicator with Togawa. For example, 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. 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.*

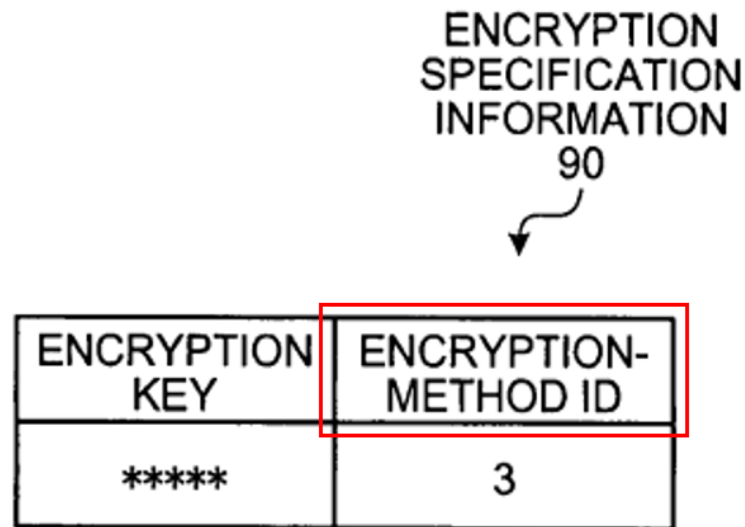
137. Nair teaches the benefits—saving time and reducing required resources—of using privacy indicators to assist the de-concealing server in determining information about the encryption process used within the data transmission. Ex. 1004, ¶[0043] (“[O]ne key reason to have such an indication specified 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. 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. 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.

138. In my opinion, 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. 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.

139. In my opinion, 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. 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..



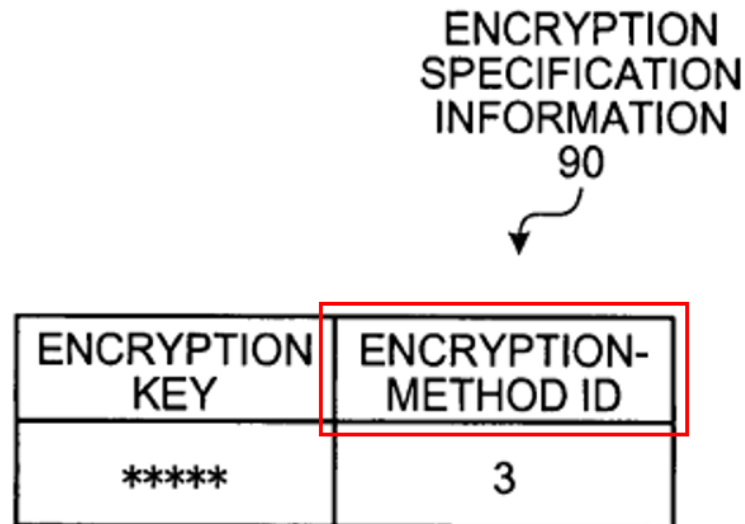
Id., Fig. 13 (annotated); *see also id.*, 23:17-25.

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

2. Independent Claim 1

141. 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, in my opinion, 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.

142. Togawa teaches 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 (which is 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. A POSITA would have been

motivated to use Togawa's encryption scheme identifier in place of Nair's privacy indicator, as I explained above in the previous section.

3. Claims 2-17

143. As I explained in Ground 1, claims 2-17 are obvious over Nair in light of Forsberg. Each of these claims also 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." Accordingly, 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 above.

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

144. Claims 8 and 14 include the limitation that the encryption scheme is an Elliptic Curve Integrated Encryption Scheme. In my opinion using an Elliptic Curve Integrated Encryption Scheme would have been obvious to a POSITA at the time of the invention in light of the combinations of Grounds 1 and 2, in further combination with 5G-Ensure D3.1.

1. Claims 8 and 14

145. In my opinion Nair in combination with Forsberg and 5G-Ensure D3.1 and Nair in combination with Forsberg, Togawa, and 5G-Ensure D3.1 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. 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.

146. In my opinion, 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. This is because 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. 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.

147. A POSITA would have been motivated to consult 5G-Ensure D3.1 to complement Nair's system with predictable results 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],. 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. 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.

IX. CONCLUSION

Declaration of Harry Bims, Ph.D.
U.S. Patent No. 10,425,817

148. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: March 15, 2024

By: 

Harry Bims, Ph.D.