

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.,
Petitioner

v.

TELEFONAKTIEBOLAGET LM ERICSSON,
Patent Owner

Case: IPR2024-00702
U.S. Patent No. 10,425,817

DECLARATION OF DR. MARK MAHON

TABLE OF CONTENTS

I. INTRODUCTION	1
II. EDUCATIONAL BACKGROUND AND QUALIFICATIONS.....	2
A. OVERVIEW	2
B. EXPERIENCE WITH TELECOMMUNICATIONS SYSTEMS.....	6
III. MATERIALS REVIEWED.....	8
IV. LEGAL STANDARDS.....	9
A. PATENT CLAIMS.....	10
B. BURDEN OF PROOF FOR INVALIDITY	11
C. CLAIM CONSTRUCTION	11
D. PERSON OF ORDINARY SKILL IN THE ART	12
E. ANTICIPATION.....	12
F. OBVIOUSNESS	13
V. PERSON OF ORDINARY SKILL IN THE ART.....	16
VI. BACKGROUND OF THE RELEVANT TECHNOLOGY	17
A. THE '817 PATENT	18
B. ALLEGED PRIOR ART	24
1. Ground 1 – Nair in combination with Forsberg	24
2. Ground 2 – Nair and Forsberg in further combination with Togawa	35
3. Ground 3 and 4 – Grounds 1 and 2 in further combination with 5G- Ensure	38
VII. PETITIONER'S GROUNDS DO NOT ANTICIPATE OR RENDER OBVIOUS THE CHALLENGED CLAIMS.....	39
A. GROUND 1 – NAIR IN COMBINATION WITH FORSBERG.....	39
B. GROUND 2 – NAIR AND FORSBERG IN FURTHER COMBINATION WITH TOGAWA 54	
C. GROUND 3 AND 4 – GROUNDS 1 AND 2 IN FURTHER COMBINATION WITH 5G- ENSURE.....	56
VIII. CONCLUSION	59

I. Introduction

1. I have been retained on behalf of Patent Owner Telefonaktiebolaget LM Ericsson (“Ericsson”). My opinions are in relation to the ongoing *Inter Partes* Review of U.S. Patent No. 10,425,817 (the “’817 Patent”). I understand that the Board chose to institute IPR, and I have been asked to evaluate the grounds on which Petitioner Lenovo alleges that the claims of the ’817 Patent are invalid.

2. This Declaration summarizes the independent opinions that I have formed to date, based on the material currently available to me. I reserve the right to modify my opinions, if necessary, based on further review and analysis of information that I receive after the filing of this Declaration, including in response to any positions taken by Petitioners or their experts that I have not yet been provided with.

3. My findings, as explained below, are based on my study, experience, knowledge and background in the fields discussed. I am informed by my education and my extensive experience in the fields of telecommunications and security. I have also relied on my review and analysis of the prior art, information provided to me and information I have independently reviewed.

II. Educational Background and Qualifications

4. I have summarized in this section my educational background, career history, publications, and other relevant qualifications. I understand my full *curriculum vitae* is being submitted as Ex-2006 to this proceeding.

A. Overview

5. I am a Teaching Professor in the School of Electrical Engineering and Computer Science at Pennsylvania State University, University Park, PA (“Penn State” or “PSU”). I have worked on telecommunications networks, including AMPS, IS-95, CDMA2000, GSM, EDGE, UMTS/WCDMA, LTE, and 5G cellular systems since 1988.

6. I received my B.S. in Electronics Engineering from the University of Scranton in 1987. I received my M.S. in Electrical Engineering and Ph.D. in Acoustics from Penn State in 1991 and 2001, respectively.

7. In 1988, after I received my bachelor’s degree, I joined the Central Intelligence Agency (CIA) while pursuing my M.S. degree at Penn State part-time. My first job at the CIA involved designing and testing systems to automatically capture and characterize telecommunication signals and emissions from various computer networking devices.

8. I returned to Penn State in early 1990 to pursue graduate research full-time and complete my M.S. degree. My graduate research work focused on

wideband beamforming and adaptive signal processing. After completing my M.S. degree in EE in 1991, I accepted a full-time faculty research position at the Applied Research Lab at PSU, primarily working on classified programs, and began working on diverse radio frequency and acoustic sensor systems including wireless communications and small wireless networks for acoustic tracking, source localization, and feature extraction.

9. I began pursuing my Ph.D. part-time in 1993 while continuing my faculty research position. In 1997, as part of my faculty research position, I began working on classified programs focused on mathematical analytical modeling of cellular communication networks and the development of hardware and software systems to test against cellular networks with a primary focus on analyzing and identifying security signaling, procedures, architectures, and vulnerabilities. My role was to develop the algorithms and write the code running on a specially developed embedded system. For this work, I received a letter of recognition as the “genius behind the VELA software algorithms” from the Director of National Reconnaissance Office (NRO) Systems Engineering and Technology Office. As part of this same work, I was extensively involved in protocol and signaling analysis as well as researching model-specific performance and unique functional characteristics associated with individual mobile devices. The work involved testing dozens of handsets from many manufacturers in controlled and real-world

environments against network simulators and live operational networks for each research project.

10. In 2000 my research extended into utilizing non-orthogonal wavelets for improving detection and localization of cellular handsets from high altitude sensor systems. In 2001, I completed my Ph.D. My research focused on the utilization of advanced communication signals for wideband characterization and remote sensing of propagation channels.

11. Beginning in 1997 my cellular communications research work focused on CDMA, GSM, EDGE, UMTS, LTE, and 5G cellular systems primarily under grants sponsored primarily by the Department of Defense. This classified research work required 3GPP protocol analysis and development of real-time embedded hardware and software systems capable of interacting with cellular networks and cellular handsets. A large portion of my work was directed at architectures, protocols, software, and signaling.

12. I have been working on classified projects since 1988. Before 1998, because the work was not deemed highly classified, I was able to publish eight journal and conference papers prior to 2000. Between 1999 and 2015, however, I was allowed to publish only one article in an unclassified symposium and published and presented about a dozen articles in classified settings. This is because during this period, the vast majority of my research was highly classified. As a result, nearly all

my research results were summarized in classified reports and not available to the general public. Further, because the U.S. government owns any intellectual property resulting from the sponsored research work, I did not pursue or file patent applications.

13. In 2015, I transferred to the School of Electrical Engineering and Computer Science at Penn State as a teaching faculty member. In that role, I have continued teaching graduate and undergraduate courses, guiding Ph.D. and M.S. students in communication and mobile networking (including LTE and 5G cellular networks) and pursuing research in this and related areas. Since 2015, I have been an author on nine refereed papers as listed in my *curriculum vitae*.

14. Because of my decades of research and my continuing work at Penn State, I have intimate knowledge of telecommunication networks, including the technology involved in the patent in this case. I have been highly recognized as an expert in such systems within the research community. I was recognized twice by the National Reconnaissance Office with commendation letters for work dealing with detecting cellular signals in low signal to noise ratio environments. The U.S. government awarded me over \$12M in grants between 2003 and 2015 for projects focused on mobile communication devices and networks, in which I served as a Principal Investigator (PI), Co- PI, and/or technical lead.

15. Additionally, during my research career, I interacted extensively with computer scientists and engineers responsible for the design, development, and testing of telephony and data networking systems and testbeds. As a research faculty member, I oversaw engineers and computer scientists that executed many joint projects with development organizations. These interactions exposed me to a wide range of computer scientists and engineers working on telecommunication network technologies. Since 2011, I have been teaching undergraduate and graduate classes in communication and mobile networking and am familiar with the curricula being taught to electrical engineers and computer scientists. The interactions with a wide range of computer scientists and engineers working on telecommunication network technologies and the familiarity with the classes taught to electrical engineers and computer scientists have allowed me to have a good understanding of the level of skills possessed by a person of ordinary skill in the field of cellular technology.

B. Experience with telecommunications systems

16. I have extensive experience with telecommunications systems in general and LTE and 5G specifically. While most of my research efforts between 1998 and 2015 are highly classified, I can state that they included detailed investigation of network architectures, signaling, and functional behavior primarily focused on authentication and key management and related security procedures at the network and RF layers. A typical research effort would involve studying 3GPP,

3GPP2, IEEE, and other protocol standards to fully comprehend all aspects of L1, L2, and L3 requirements including timing, bit-level construction of the control and user plane messages, and timing characteristics for a given standard as well as functional behavior of network components and user equipment.

17. From 2006 through 2015 my research focused specifically on LTE. My research continues to this day, although I am no longer operating in a classified environment. During this time, I investigated the performance and functional differences of many varied network and handset devices to see how differing signaling and environmental factors influenced the behavior of user equipment in a given network environment. This included how synchronization, timing, and signal to interference plus noise ratio (SINR) for a given device would affect specific functional aspects including elements of the receiver structure, decoding and demodulation performance, calculation of parameters used by the device for making decisions and deriving parameters reported to the network.

18. As part of my research work, I built several custom LTE platforms that implemented specific network-side and user equipment-side functionality including custom signal generation and processing structures, particularly the signal processing chains on both the transmit and receive sides. This equipment was developed using network simulation hardware in a laboratory environment and was later tested with LTE networks in both controlled and fully operational

environments. Implementing the transmit and receive chains for custom built LTE-enabled equipment required me to gain an intimate understanding of the relevant 3GPP protocol specifications and the underlying OFDM and WCDMA structures. Since 2015, I have been primarily focused on guiding graduate students pursuing research into multiple-input multiple-output (MIMO) techniques to improve throughput in dense-user environments, optimized distributed processing algorithms, and the implementation of block chain coding techniques to improve handover security in 4G (LTE)/5G (NR) networks.

19. My *curriculum vitae* provides additional information regarding my education, technical experience, and publications.

III. Materials Reviewed

20. The opinions set forth in this Declaration are based on my professional judgment, education, experience, and knowledge regarding the telecommunications security technologies that are discussed in the '817 Patent. In addition, I have based my opinions on my review of documents, including those listed below:

Title	Exhibit Number
U.S. Patent No. 10,425,817	1001
Declaration of H. Bims	1002
U.S. Application No. 2018/0324585	1004
U.S. Application No. 2013/0003971	1005
U.S. Patent No. 8,005,219	1006
3GPP Tr 33.899 v1.1.0	1007
U.S. Provisional Patent Application 62/502,266	1008
Certified File History of the '817 Patent	1009

5G-Ensure Deliverable D3.1 5G-PP security enablers technical roadmap (early version)	1010
A Survey of the Elliptical Curve Integrated Encryption Scheme	1011
Excerpts from Dr. Bims' ITC deposition	2001
Security in 5G Networks – How 5G Networks Help Mitigate Location Tracking Vulnerability	2002
TDoc S3-172106 LS on Security aspects of ECIES for concealing IMSI or SUPI	2003
<i>Curriculum Vitae</i> of Dr. Mark Mahon	2006
Deposition Transcript of H. Bims	2007
Staff's Post-Hearing Brief (Redacted)	2008
Respondents' Post Hearing Brief ('817 Patent Excerpts)	2009
Transcript of ITC-1375 on July 16, 2024 (open session)	2010
Lenovo's Petition for IPR U.S. Patent No. 10,425,817	—
Ericsson's Patent Owner's Preliminary Response	—
Decision Granting Institution of IPR	—

IV. Legal Standards

21. I am not an attorney or a legal expert, and I do not opine on matters of law. All the legal standards, which are listed in this section and which I applied in reaching the conclusions expressed throughout this Declaration, were provided to me and explained to me by counsel. In preparing this Declaration, I have endeavored to faithfully apply these legal standards. I do not intend to offer opinions on the law. Below, I describe the legal standards that I applied in my analysis of the claims of the 817 Patent.

22. I have been informed by counsel that an issued patent is presumed valid and that the challenger of a patent's validity bears the burden of proving invalidity of the patent.

A. Patent Claims

23. I have been informed by counsel that a patent's claims describe the invention made by the inventors and describe what the patent owner owns and what the owner may prevent others from doing.

24. I have been informed by counsel that claims may describe products, such as machines or chemical compounds, or processes for making or using a product. Claims are usually divided into parts or steps called limitations.

25. I have been informed by counsel that there are two types of claims: independent claims and dependent claims. An independent claim sets forth all the requirements that must be met in order to be covered by that claim. Thus, it is not necessary to look at any other claim to determine what an independent claim covers. A dependent claim does not itself recite all of the requirements of the claim but refers to another claim for some of its requirements. In this way, a dependent claim depends on another claim. The law considers a dependent claim to incorporate all of the requirements of the claims to which it refers.

26. I have been informed by counsel that that a dependent claim then adds its own additional requirements. To determine what a dependent claim covers, it is necessary to look at both the dependent claim and any other claims to which it refers.

27. I have been informed by counsel that in a case where a dependent claim incorporates the limitations of an independent claim upon which it depends, if a

reference fails to disclose any of the limitations of the independent claim, the claims which depend on that independent claim cannot be made invalid by such a reference. As a result, any of the references at issue in this proceeding that fail to disclose all of the limitations of an independent claim necessarily also fail to disclose all of the limitations of claims which depend on that independent claim.

B. Burden of Proof for Invalidity

28. I have been informed by counsel and I understand that the party challenging the validity of an issued U.S. patent in an IPR bears the burden of proving invalidity through facts supported by a preponderance of the evidence. I

29. have been informed that a “preponderance of the evidence” means evidence sufficient to prove that a fact is more likely true than it is not.

C. Claim Construction

30. I have been informed by counsel and I understand that the first step in determining validity is to properly construe the claims. I have further been informed by counsel that, in this proceeding, the Board must determine the scope of the claims by using the same claim construction standard that United States District Courts use. Under this standard, the words of a claim are given their “ordinary” and “customary” meaning as would have been understood by a person of ordinary skill in the art at the time of the invention. I have been informed that such a person looks to the claims,

specification, and file history in understanding the meaning of the claim terms. I have applied this understanding in this declaration.

D. Person of Ordinary Skill in the Art

31. I have been informed by counsel and I understand that a person having ordinary skill in the art may be defined by factors such as, when considered at the time of the alleged invention: (a) the levels of education and experience of the inventor and other persons actively involved in the field; (b) the types of problems encountered in the field; (c) prior art solutions to those problems; (d) rapidity with which innovations are made; and (e) the sophistication of the technology.

E. Anticipation

32. I have been informed by counsel and I understand that a patent claim can be found invalid as anticipated if each and every element of the claim, as properly construed, is found either explicitly or inherently in a single prior art reference. If the single prior art reference does not disclose explicitly or inherently any one claim limitation, then that claim is not anticipated. I have further been informed that the single prior art reference cannot merely disclose each element; rather, it must disclose all of the elements as arranged in the claim. I have been informed that for a prior art reference to “inherently” disclose something, the reference must necessarily function in accordance with, or include the claimed limitations, to anticipate. The missing descriptive matter cannot merely probably or

possibly include the claimed limitations. I have further been informed by counsel that, with respect to an anticipation analysis, it is improper to combine separate, distinct embodiments of a single prior art reference.

33. I have been informed that for a reference to be anticipatory, the reference must contain an enabling disclosure. I have been informed that merely naming or describing the subject matter is insufficient if it cannot be produced without undue experimentation.

F. Obviousness

34. I have been informed by counsel that a patent claim can be found invalid as obvious if the differences between the claim and the prior art references would have been obvious to a person of ordinary skill in the art at the time of the invention, taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any objective indicia of non-obviousness. I have further been informed by counsel that a claim can be found to be obvious in light of either a single prior art reference or multiple prior art references. I have been informed that references qualify as prior art for an obviousness determination only when they are analogous to the claimed invention. Two separate tests define the scope of analogous prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed; and (2) if the reference is not within the field of the inventor's endeavor,

whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.

35. I have been informed that to be obvious in light of a single prior art reference or multiple prior art references, there must be a reason either to modify the single prior art reference or to combine the two or more prior art references to achieve the claimed invention. I have been informed by counsel that this reason may come from a teaching, suggestion, or motivation to combine which may come from the reference or references themselves, the knowledge or “common sense” of one skilled in the art, or from the nature of the problem to be solved, and may be explicit or implicit from the prior art as a whole.

36. I have been informed by counsel that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.

37. I have further been informed by counsel that there is no suggestion to combine, however, if a reference teaches away from its combination with another source. A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant, or if it suggests that the line of development flowing from the reference’s disclosure is unlikely to be productive of the result sought by the

applicant. If, when combined, the references would produce a seemingly inoperative device, then they teach away from their combination. I have been informed that it is improper to combine references where the references teach away from their combination.

38. I have been informed by counsel that the degree of teaching away will depend on the particular facts; in general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant. I have been informed that a reference teaches away, for example, if (1) the combination would produce a seemingly inoperative device, or (2) the references leave the impression that the product would not have the property sought by the applicant.

39. I have been informed by counsel that if the teachings of a prior art reference would lead one skilled in the art to make a modification that would render another prior art device inoperable, then such a modification would generally not be obvious. I have been informed that if a proposed modification would render the prior art device unsatisfactory for its intended purpose, then the proposed modification would generally not be obvious.

40. I have been informed by counsel that it is improper to use hindsight in making the obviousness determination.

41. I have been informed by counsel that some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness must be made. I have been informed that, for example, there may be no rational underpinning to support the legal conclusion of obviousness where systems are already complete and the party challenging validity seeks to mix and match components, which each exist in the separate systems, from these complete systems.

V. Person of Ordinary Skill in the Art

42. July 25, 2017, is the effective filing date for the '817 Patent. Therefore, in my opinion below, when I refer to a POSITA regarding the '817 Patent, I refer to one of ordinary skill in the art as of July 25, 2017.

43. With regard to the '817 Patent, it is my opinion that a POSITA is one having a bachelor's degree in electrical engineering, computer engineering, or computer science with (1) at least three years of experience in the field of telecommunications or wireless systems; and/or (2) an advanced degree in electrical engineering, computer engineering, or computer science in the field of telecommunications or wireless systems.

44. 14. Based at least on my educational and work experience, I qualify as a person of ordinary skill in the art as of the filing dates of the '817 Patent.

VI. Background of the Relevant Technology

45. The '817 Patent is related to security in cellular systems. In cellular systems, an IMSI (International Mobile Subscriber Identifier) is used to identify UEs to networks when they connect. This IMSI comes from the SIM card included in a device, which is why users can replace their phones, swap the SIM card, and carry on communicating as though little had changed.

46. The IMSI consists of three parts: The IMSI consists of three parts: the MCC (mobile country code), the MNC (mobile network code), and the mobile subscriber identification number (MSIN). Only the MSIN is unique to a subscriber, and this is the part used to determine what subscriber is attempting to connect to a network when an attach request is received.

47. The IMSI represented a potential vulnerability in early telecommunications systems because it could be recorded by a malicious actor during registration. Members of the Department of Computer Science from the Ohio State University published a paper describing this problem titled “Security in 5G Networks – How 5G Networks Help Mitigate Location Tracking Vulnerability.” *See generally* Ex-2002. The paper explains how “IMSI catchers” could be used to intercept an IMSI, allowing malicious actors to engage in unwanted activities such as tracing a user’s location. *Id.* at 1, 3; *see also* Ex-2003 at 1. IMSI catchers also threatened network operators, because they could be used to intercept network traffic

and inspect it while posing as legitimate network operator base stations. This is the problem that motivated the 3GPP to adopt the '817 Patent's solution into the 5G standard.

A. The '817 Patent

48. Early attempts to solve the problem designated above had been made, as the '817 Patent describes. These included using a temporary subscription identifier so that the real IMSI would not need to be sent over the air. *See* Ex-1001 at 1:24-31. However, this was not a comprehensive solution because the temporary identifier could only be established after an initial registration, during which the IMSI would be sent as plaintext.

49. In order to solve this problem more fully, the inventors of the '817 Patent introduced the concept of a Subscription Concealed Identifier, or SUCI, that could be used to deliver the IMSI to the core network during registration without ever exposing its plaintext form. *See id.* at 1:50-61, 8:19-35. The '817 Patent's Figure 3 shows the structure of this SUCI:

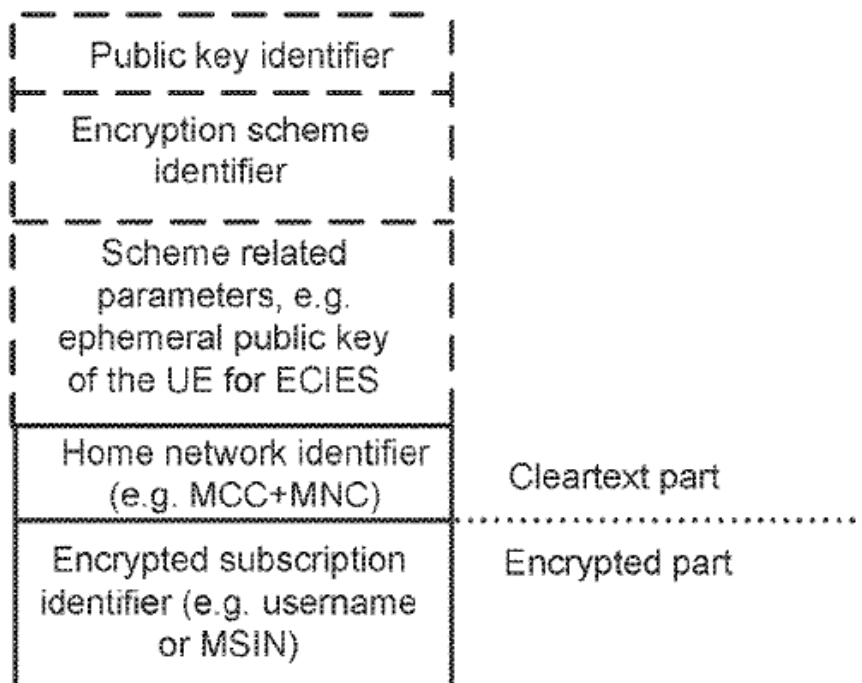


Fig. 3

50. The SUCI contains two parts, one cleartext (meaning that it can be read without decryption) and one “encrypted part” consisting of ciphertext that conceals the MSIN discussed above. *See id.* at 8:36-61, 9:4-6. The cleartext portion of the SUCI additionally includes two important components: the “encryption scheme identifier” and “public key identifier,” the utility of which I will discuss later in this section.

51. The ’817 Patent illustrates the process by which a UE uses the SUCI to register with the core network in Figure 6, which I have reproduced below. *See id.* at 10:25-10:37.

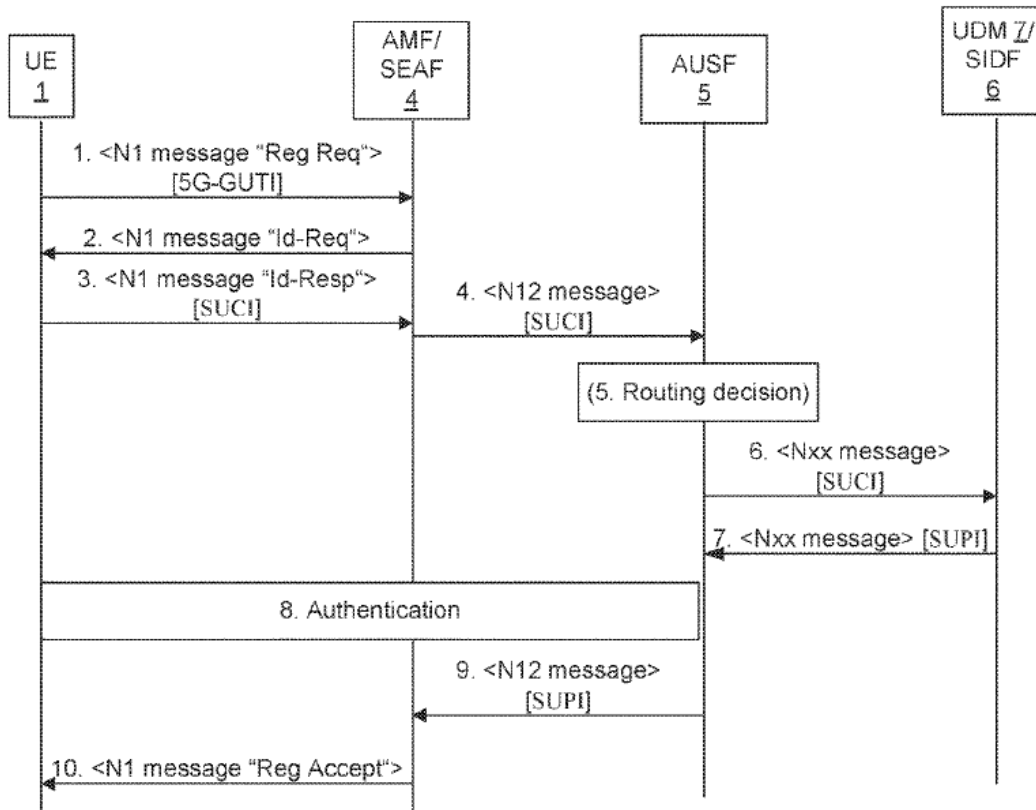


Fig. 6

52. The registration steps (described in Ex-1004 at 10:25-11:46) are as follows:

- Step 1 – The UE sends a registration request to the core network which is received at the AMF/SEAF (Authentication and Mobility Management Function/Security Anchor Function).
- Step 2 – If the core network needs the UE's identity (such as during initial registration) the AMF/SEAF responds with a request for identification.

- Step 3 – The UE sends a SUCI such as the one claimed in the '817 Patent back to the core network.
- Step 4 – the AUSF sends the SUCI to the AUSF (Authentication Server Function) to be used for authentication.
- Step 5 – The AUSF determines which SDF (Subscription Identifier De-concealing Functions) it should forward the SUCI to for decryption using the encryption scheme identifier in the cleartext part of the SUCI.
- Step 6 – The AUSF forwards the SUCI to the SDF, where it is decoded using the private key corresponding to the public key identifier in the cleartext part of the SUCI.
- Step 7 – The SDF retrieves the SUPI (Subscriber Permanent Identifier), which includes data from the now fully-decrypting IMSI and returns it to the AUSF.
- Step 8 – Using the SUPI, the AUSF initiates an authentication process by which it issues a challenge to the UE and validates a response. *See id.* at 11:25-30.
- Step 9 – The AUSF returns the SUPI to the AMF/SEAF to indicate that the associated subscriber has authenticated with the network.
- Step 10 – The AMF/SEAF returns a message to the UE that informs it that its registration has been accepted. This message does not include

the SUPI, which is now cleartext and unsuitable for transmission outside the core.

53. As mentioned, the “encryption scheme identifier” and “public key identifier” are important parts of the process just described.

54. The “encryption scheme identifier” serves to inform the core what encryption scheme the UE has used to encrypt the SUCI. The encryption scheme identifier is used in various places throughout the ’817 Patent. *See* Ex-1001 at Figs. 4, 5, 15. For example, the SUCI uses the encryption scheme identifier to signal to the core network what encryption method should be used to decrypt it. Additionally, the core uses the encryption scheme identifier to construct a privacy key used to select a privacy scheme, which includes the same encryption scheme identifier, so that it can be used for decryption of a SUCI. *See id.* at Fig 4, 9:23-39 (privacy key), Fig. 5, 10:17-24.

55. The ’817 Patent lists a variety of data structures which can be used to represent the “encryption scheme identifier.” *Id.* at 10:20-24. These include:

- “4-bit identifier,”¹
- “integer,”
- “numeric string,”

¹ A 4-bit identifier would be able to identify 2⁴ or 16 possibilities.

- “alphanumeric string”
- “bit string.”

56. The commonality among these data structures is that they are all more than one bit, and can therefore represent more than two states. A 4-bit identifier is clearly 4 bits, an integer may commonly be 8, 32, or 64 bits, strings can be allocated to an arbitrarily large size. Based on this, it is my opinion that the “encryption scheme identifier” in the context of the ’817 Patent is a variable that is intended to identify two or more encryption schemes and not simply an “on” or “off” Boolean state.

57. The ’817 Patent identifies several encryption schemes that can be used for the encryption scheme identifier, such as a null-scheme, ECIES, or RSA (named for Rivest, Shamir, and Adleman, who first described it). *See id.* at 10:17-24, 10:55-59. This provides a larger variety of potential encryption schemes to both network operators and UE manufacturers, who may wish to select among them based on the compute capabilities of UEs. For example, ECIES is known to be a strong algorithm, but requires more computational resources than RSA, which is often sufficient for security applications.

58. The “public key identifier” is also important, because it identifies the particular public key which the UE has been provisioned with to encrypt its identity when sending it over air. To decrypt the IMSI, both the correct encryption scheme

and correct private key are inputs into the de-encryption scheme, so the AUSF must use the encryption scheme id to select the correct SIDF, and the SIDF must use the public key identifier to select the correct private key to use.

59. The sum of these disclosures of the '817 Patent is a system that is able to mitigate the risks that were previously associated with registration in prior telecommunications systems such as 3G and 4G/LTE. It is my opinion that the '817 Patent is inventive, and that its solutions are non-obvious. This is evident due to its adoption into the 5G standard, which reflects the 3GPP's recognition of its valuable contribution to telecommunications security as next generation, 5G networks continue to be broadly deployed by carriers throughout the United States.

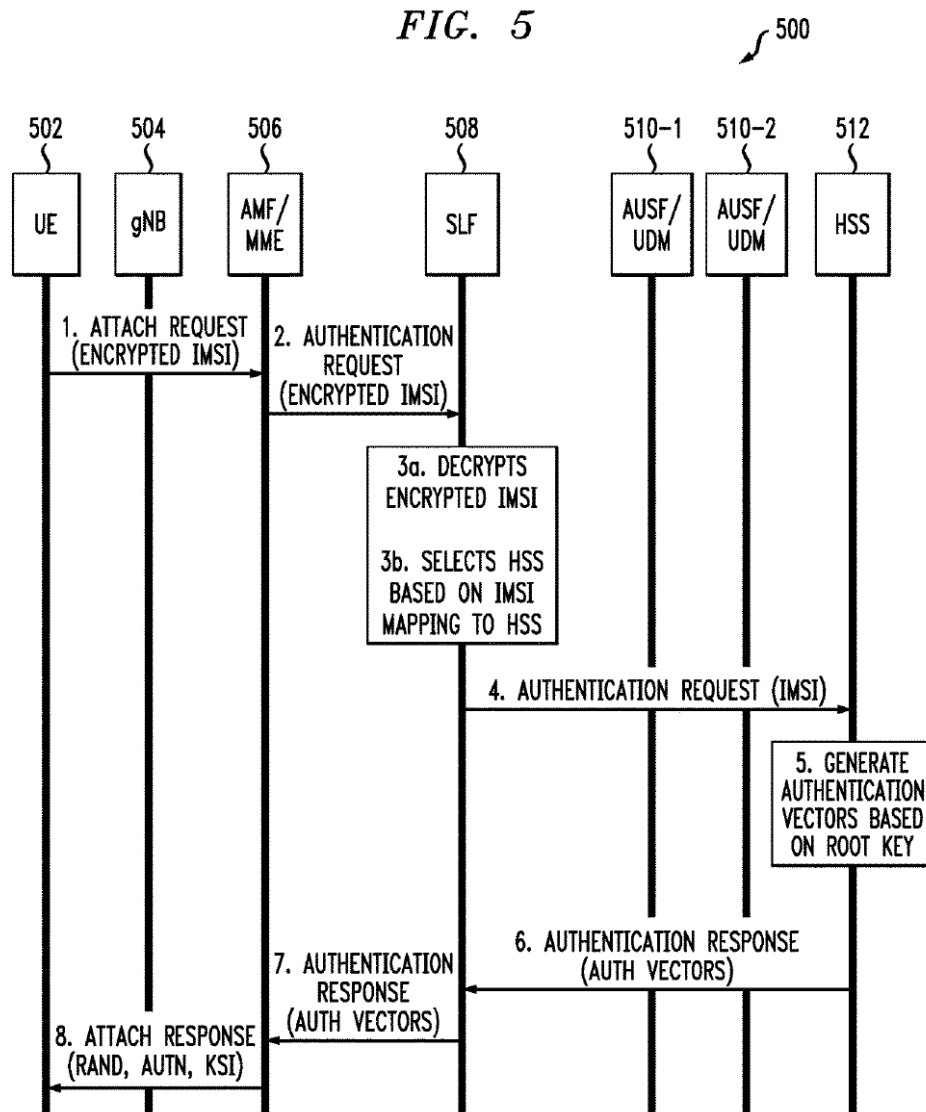
B. Alleged Prior Art

1. Ground 1 – Nair in combination with Forsberg

a) U.S. Application No. 2018/0324585 (“Nair”)

60. It is my understanding that Nair is not prior art to the '817 Patent at least because Nair was published on November 8, 2018. Nair claims priority to an application (15/794,856) dated October 26, 2017, but Dr. Bims fails to show subject matter disclosing the limitations at issue is actually present in Nair's provisional application (62/502,266) (“the Nair Provisional”). Dr. Bims fails to provide any detailed explanation for alleged support for the Nair claims in the Nair Provisional.

61. Nair provides for a privacy indicator for controlling authentication requests. Nair at (54). Figure 5 of Nair shows one embodiment for a 4G LTE and 5G network. Ex-1004 at Fig. 5, [0074] – [0076].

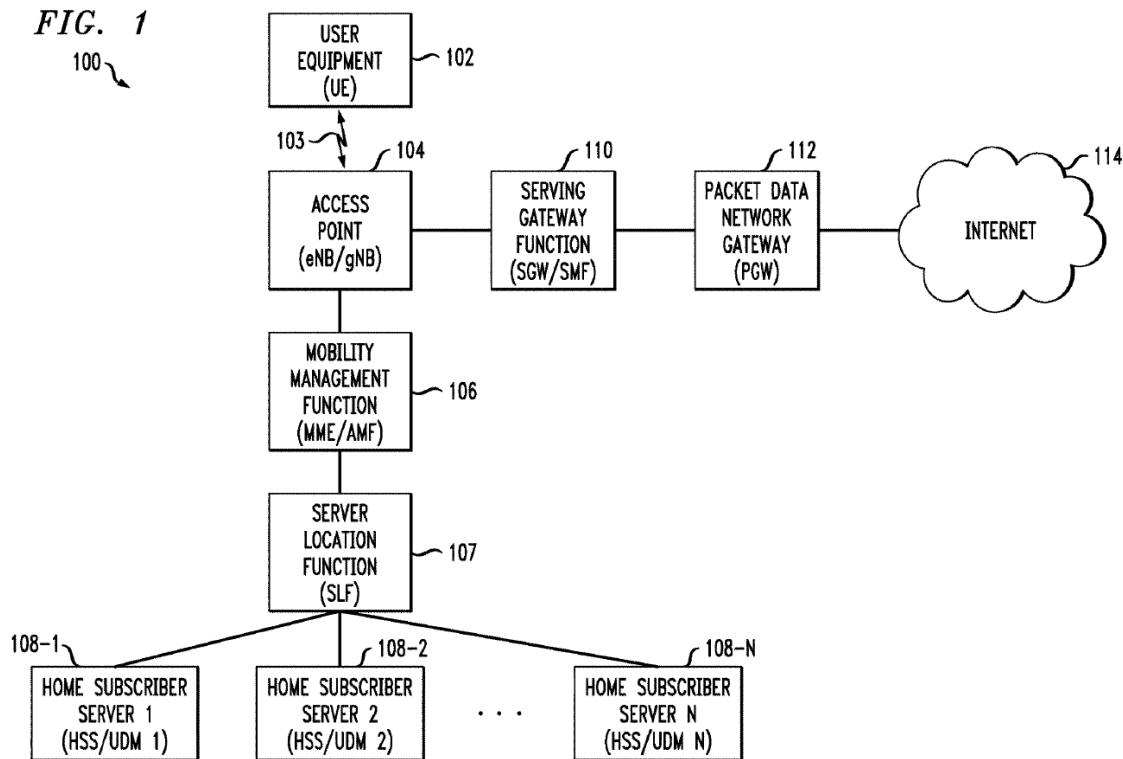


62. As Figure 5 depicts, the process starts with a User Equipment (“UE”) (502) sending an “attach request” that includes an encrypted International Mobile Subscriber Identity (“IMSI”) to the Access and Mobility Management

Function/Mobile Management Entity (“AMF/MME”) in the core network of telecommunications system. *Id.* at Fig. 5, [0074] – [0076]. An “attach request” is used by a UE during initial connection to a particular network such as a 5G network. *Id.* at [0048], [0054].

63. In the next step, the AMF/MME sends an authentication request (which contains the encrypted ISMI) to a Server Location Function (called an “SLF”). *Id.*

64. The SLF is a central device that is implemented in front of a series of Home Subscriber Servers (each called an “HSS”). *Id.* at Fig. 1, [0054]. It can receive messages from the MM/AMF, which receives the messages from the UE (through an access point, such as a base station, or “eNB”/“gNB”). *Id.* at Fig. 1, [0049] – [0058].



65. The SLF then performs two steps: it decrypts the encrypted IMSI (at step 3a). *Id.* at Fig. 5, [0074] – [0076]. This yields the unencrypted IMSI. *Id.* Based on that IMSI, the SLF determines the HSS for that subscriber, *i.e.*, based on the subscriber’s home network. *Id.* The SLF then sends the unencrypted IMSI to the HSS for the subscriber (through an AUSF/UDM, which refers to an “Authentication and Security Function”/“User Data Management”). *Id.* Next, the HSS generates authentication vectors and sends an authentication response that ultimately results in the UE receiving an attach response. *Id.* Figures 4 and 6 show message flows for a “registration request” rather than an “attach request”; Figure 3 shows an “attach request” that is not encrypted; and Figure 7 does not mention encryption. *Id.* at Figs. 3, 4, 6, 7, [0070] – [0071], [0072] – [0075], [0077] – [0078], [0079] – [0080].

66. According to Nair, one purpose of the SLF is to have the encryption/decryption handled by a central server, rather than each HSS (of which there may be many), to simplify the privacy management of the IMSI in 5G networks. *Id.* at [0038].

[I]t is advantageous to perform the decryption of the encrypted IMSI at the SLF instead of in the HSS. Hence, instead of an HSS storing the private key, now the SLF would need to store and use the network private key. An SLF is placed in the home operator's domain and considered trusted. In general, an SLF could be assumed in a large operator network. The usage of an SLF simplifies the new privacy management for the HSS/UDM in 5G networks up to the point that HSS/UDM is not changed at all for the protection of subscription identifiers over the air interface, but the SLF needs to perform the additional functionality of encrypted IMSI decryption and then perform the IMSI-to-HSS resolution.

67. Nair discloses that the “attach request” may include “one or more privacy indicators comprising a flag indicating whether the subscription identifier in the attach request is privacy-protected.” *Id.* at [0010], [0014]; *see also id.* at [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.”).

68. Nair's “privacy indicator” does what it says: it indicates whether the MSIN is encrypted, *i.e.*, whether encryption is “switched on.” It does not identify which encryption scheme is utilized. Nair instead discloses that the receiving device

(such as the SLF) already has the key needed for the decryption. *Id.* at [0035] (“[T]he home operator provides its public key to all home network subscribers Only the home HSS can decrypt the message because it possesses the private key that corresponds to the public key.”); *id.* at [0038] (“[I]t is advantageous to perform the decryption of the encrypted IMSI at the SLF instead of in the HSS. Hence, instead of an HSS storing the private key, now the SLF would need to store and use the network private key.”).

69. There is no disclosure of multiple encryption keys or encryption schemes in Nair; there is only the disclosure the receiving device (such as the SLF) already containing the key needed for decryption and decrypting the encrypted portion of the IMSI if the privacy indicator states that encryption was used.

70. This is one of the main differentiating factors between the ’817 Patent and Nair. Nair exchanges reduced complexity (*i.e.*, identifying only whether or not a message includes an encrypted IMSI) for reduced flexibility in a system which implements its technique. Because the privacy indicator does not identify an encryption scheme, a network operator would only be able to use a plaintext IMSI scheme or one encrypted using a single secure encryption scheme.

71. Nair’s disclosure of why the attach request can include a privacy indicator reinforces that it does not identify an encryption scheme but acts a switch

to save a processing step (*i.e.*, the “first attempt” to resolve a request that is encrypted). *Id.* at [0043].

It could be suggested that the HSS or SLF, even without this privacy indicator, will figure out after the first attempt to solve the request and, if encrypted, to attempt the decryption. But one key reason to have such an indication specified is that this saves processing time and fewer resources are needed. Thus, in this first illustrative embodiment, the SLF can make the decision on the processing by looking at this flag. If not set, the SLF will assume the provided IMSI is unencrypted If the flag is set, the SLF will recognize that the provided IMSI is encrypted and use the network private key to decrypt the MSIN part to form the real unencrypted IMSI If no SLF is used, the same principle can be used by the HSS/UDM. That is, HSS/UDM has to check whether the 5G UE has set a flag and then decide whether decryption is needed.

72. The receiving device can only “figure out after the first attempt” to decrypt the message if the device already knows the encryption scheme utilized and already has the public and private keys to perform that decryption. Nair’s system thus would not operate if the attach request included an encryption scheme identifier because it would not resolve after a “first attempt” because the system would not know, from the message, the encryption scheme utilized or the corresponding encryption keys.

73. Nair has the receiving device (such as an SLF) try to decrypt the MSIN right off the bat. This is a separate approach from the solutions of the '817 Patent. In particular, Nair touts the benefit of having a central SLF perform the decryption instead of having that capability spread across multiple components. *Id.* at [0045].

[P]lacing an SLF capable of identifying an encrypted MSIN and decrypting it before routing the authentication request to an HSS helps to manage the coexistence of 4G and 5G core in an operator network. Enhancing the SLF to support the new identity 5G privacy feature is more advantageous than enhancing the HSS. If the HSS is enhanced, then in a large network with multiple HSSs, all the HSSs need to be updated together with capability to decrypt an encrypted IMSI. This may be more tedious to handle compared to solving the problem in a single central node (*e.g.*, the SLF).

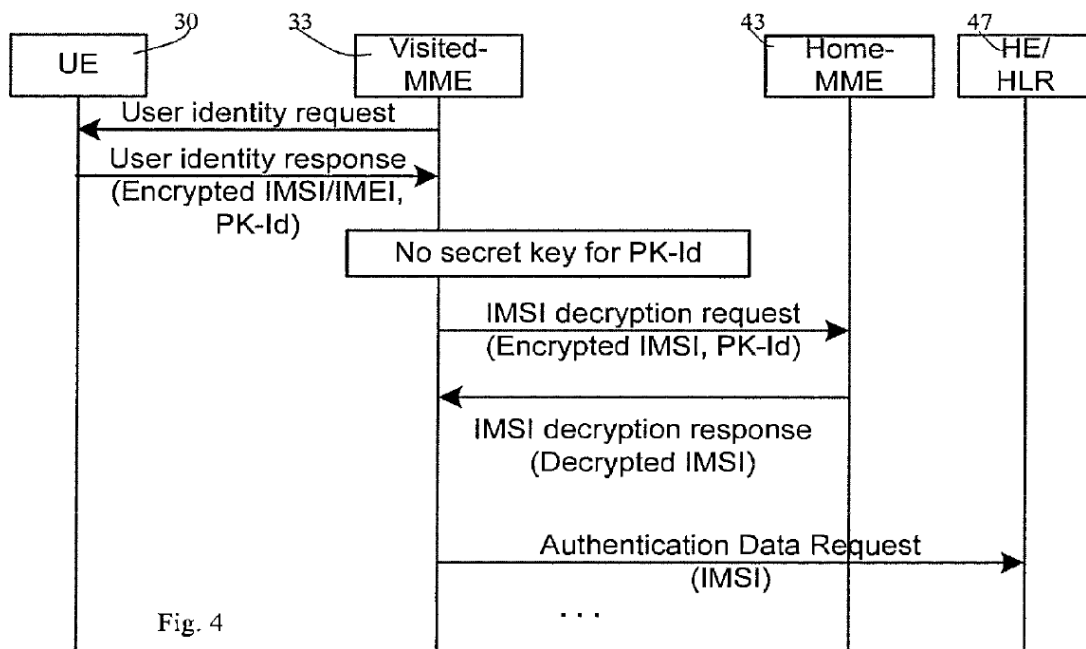
74. Thus, while Nair mentions the importance of privacy for subscribers, Nair is different than the '817 Patent. Nair is about provisioning privacy features in a communication network based on “privacy indicators.” Nair describes that these privacy indicators may be flags or fields to indicate whether or not encryption is used. Nair does not disclose the '817 Patent's subscription concealed identifier (SUCI). Nair does not disclose the '817 Patent's SUCI approach including the authentication server and de-concealing server.

b) U.S. Application No. 2013/0003971 (“Forsberg”)

75. Forsberg is entitled “Identifiers in a Communication System.” Ex-1005 at (54). The Patent Office expressly considered Forsberg during prosecution of the ’817 Patent. Ex-1001 at (56).

76. In Forsberg, a “first network entity” receives an identifier. Then the first network entity determines if it can decrypt that identifier. If the first network entity can decrypt the identifier, the first network entity does so. If the first network entity cannot decrypt the identifier, the first network entity will determine a second network entity based on the identifier. The first network entity then seeks assistance from that second network entity. The first network entity may then decrypt the identifier based on information kept in the second network entity.

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



78. In a network other than the UE's home network, also known as a visiting network, an MME sends a user identity request to the UE. Ex-1005, at Fig. 4, [0048] – [0056]. The UE then provides a response that includes an encrypted IMSI/IMEI (which are acronyms for “International Mobile Subscriber Identity” and “International Mobile Equipment Identity”). *Id.*

79. The Visiting MME then takes a series of steps outlined in Figure 2. *Id.* at Fig. 2, [0043] – [0046].

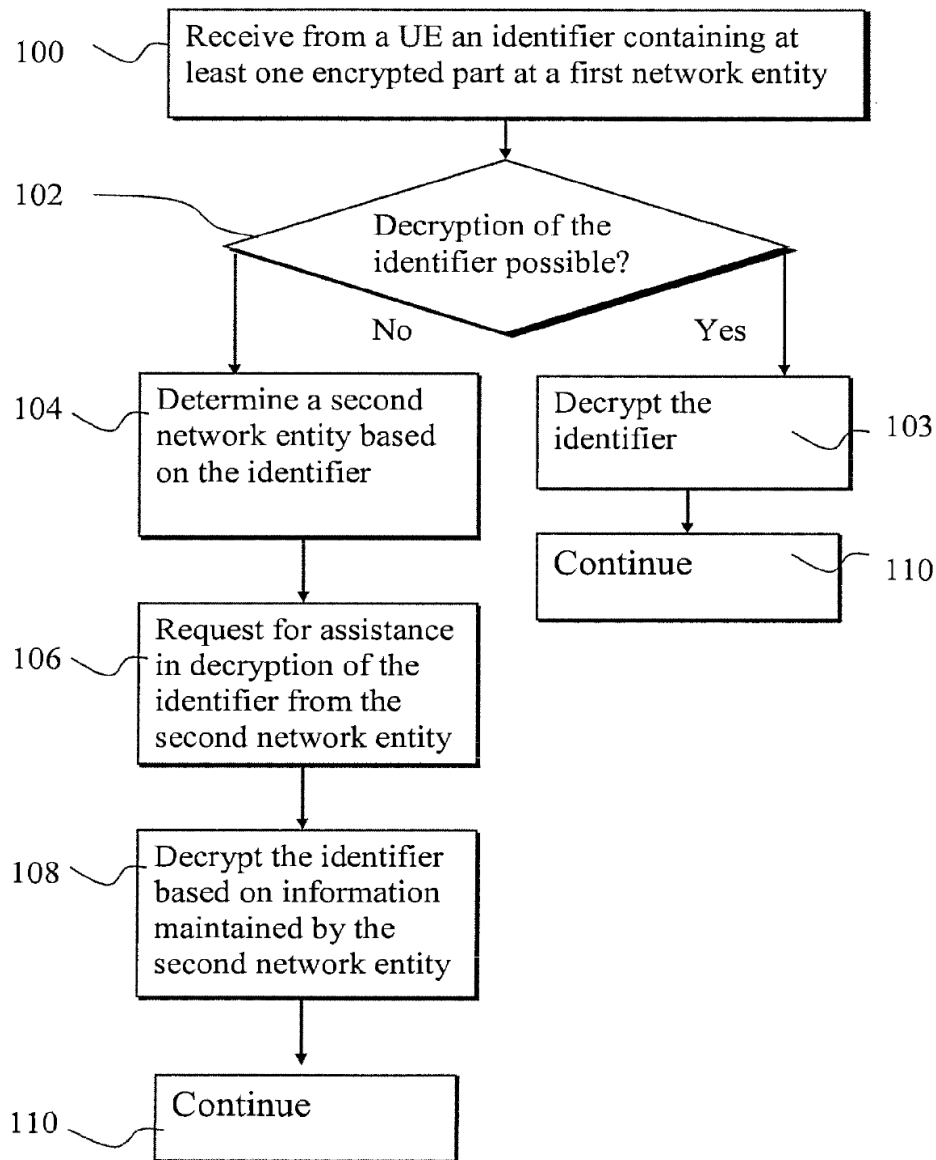


Fig. 2

80. After receiving the encrypted identifier, the MME determines if it can decrypt it. *Id.* at Fig. 2, [0043] – [0046]. If so, the MME decrypts the identifier; if not, the MME determines if there is another network entity that can decrypt the identifier (*e.g.*, another MME), requests assistance from the other entity, and obtains a decrypted identifier. *Id.*

81. These steps are shown in Figure 4, in which the Visiting MME determines that it does not have a secret key for the encrypted IMSI/IMEI, sends a decryption request to the Home MME, and obtains the decrypted ISMI in response. *Id.* at Fig. 4, [0048] – [0056]. Figure 5 shows a similar message flow but illustrates the case in which the Visiting MME found the secret key for the encrypted IMSI/IMEI and was able to decrypt the IMSI/IMEI without the assistance of the Home MME. *Id.* at Fig. 5, [0048] – [0056].

82. Like Nair, Forsberg recognizes that privacy is important. But again, Forsberg is quite different from the inventions of the '817 Patent. Forsberg does not disclose the '817 Patent's subscription concealed identifier (SUCI), nor does it disclose the '817 Patent's SUCI approach, including the authentication server and de-concealing server.

2. Ground 2 – Nair and Forsberg in further combination with Togawa

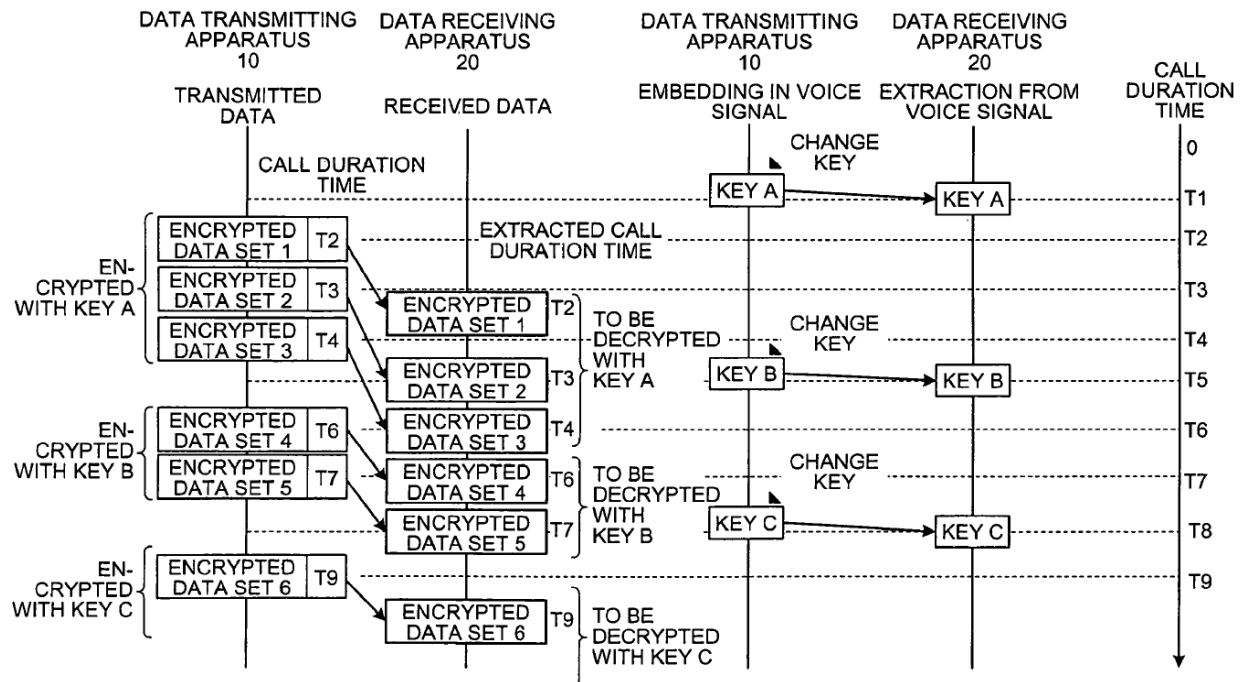
a) U.S. Patent No. 8,005,219 (“Togawa”)

83. Togawa attempted to create “a technique that allows an integrated communications service for carrying out data communications of user data, as well as two-way communications of multimedia information, to transmit user data securely and efficiently.” Ex-1006 at 2:21–25.

84. In general, Togawa teaches embedding encrypted data within a voice signal (*e.g.*, Encrypted Data Set 1–6) that the receiving device can decrypt with one

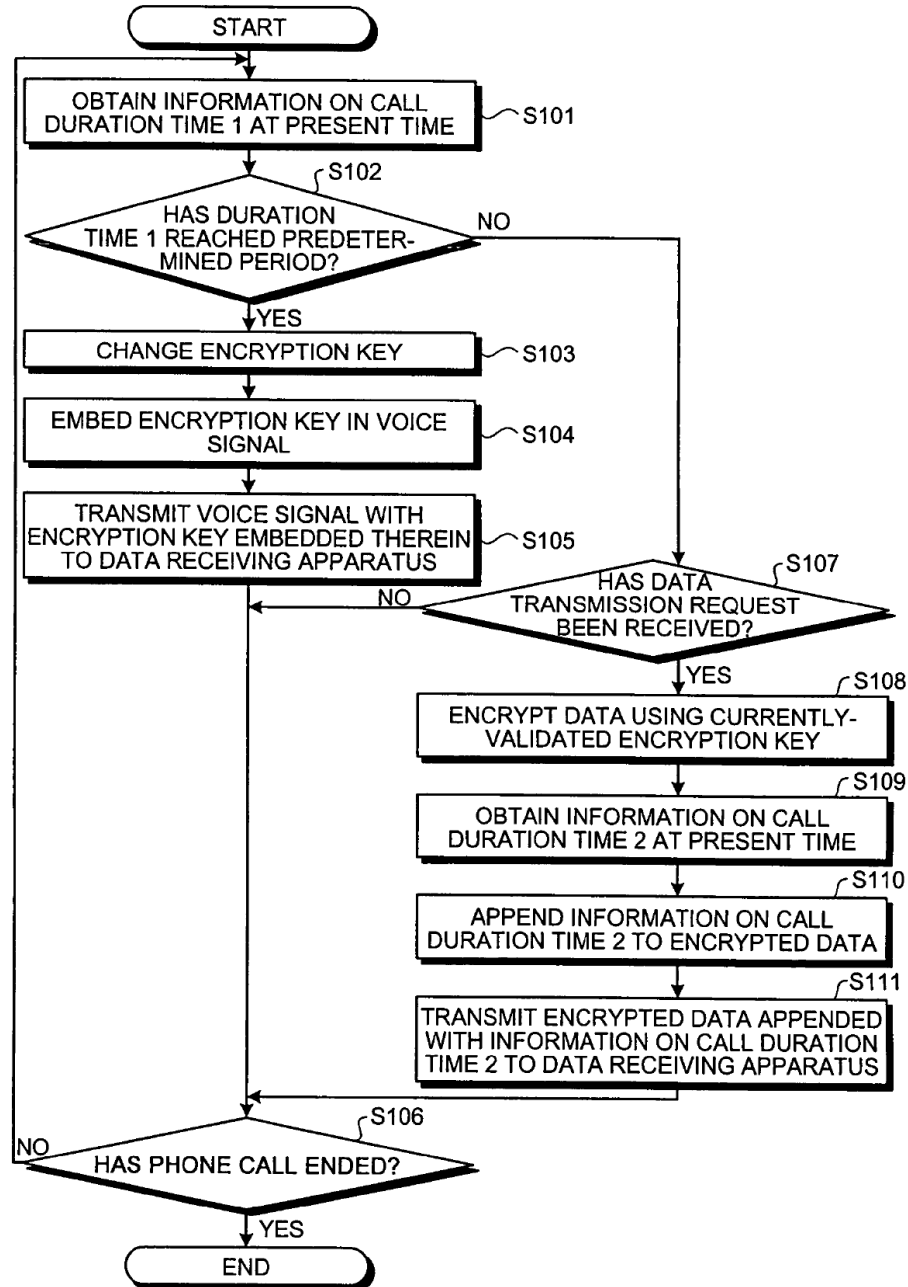
or more keys that change over time (e.g., Key A, Key B, and Key C). *Id.* at Fig. 1, 4:29–7:45; *see also id.* at Fig. 8, 12:15–14:7 (showing system in which the receiving apparatus initiates the key change).

FIG.1



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

FIG.4



86. Togawa does not relate to next-generation cellular networks (like 4G LTE or 5G) and does not relate to subscriber information (or even subscriber information in general). It does not teach a SUCI that, in the clear-text part, includes an encryption scheme identifier that identifies an encryption scheme used by the UE

to encrypt the subscription identifier in the SUCI. Nor does it appear to disclose any particular “server,” let alone the server elements recited in the ’817 Patent’s claims.

3. Ground 3 and 4 – Grounds 1 and 2 in further combination with 5G-Ensure

a) 5G-Ensure Deliverable D3.1 5G-PP security enablers technical roadmap (early version) (“5G-Ensure”)

87. 5G-Ensure arose from an EU-funded group of projects. 5G-Ensure reflects a desire to enable privacy more generally for users in the then-upcoming 5G Standard. 5G-Ensure discusses the high-level concept of encrypting subscriber identifier information in 5G networks. Ex-1010 at 32–34.

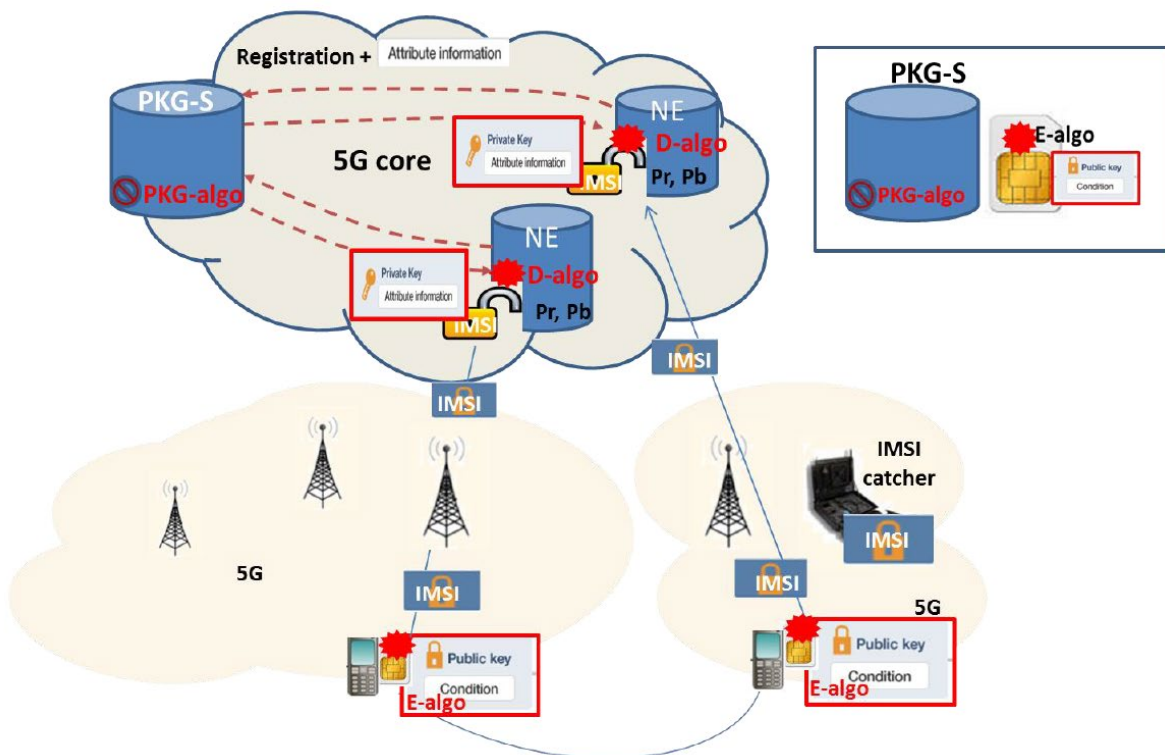


Figure 5: High level components of the feature “Encryption of Long Term Identifiers”

88. 5G-Ensure does not describe the messaging scheme to use for this proposal. 5G-Ensure also does not detail the structure of the transmitted subscriber information, which parts are clear-text, which parts are encrypted, and what other encryption-related metadata resides in the message (*e.g.*, fields identifying an encryption scheme or a public key). Further, 5G-Ensure does not provide specific detail of the servers involved in the process. Additionally, as I explain later in this declaration, 5G-Ensure teaches away from the use of ECIES—the very limitation that Dr. Bims claims it teaches.

VII. Petitioner’s grounds do not anticipate or render obvious the challenged claims.

A. Ground 1 – Nair in combination with Forsberg

a) Motivation to combine Nair and Forsberg

89. According to Dr. Bims, a POSITA would be motivated to combine Nair and Forsberg because they are in related fields and “to reduce the complexities of managing multiple public and private key pairs . . . as described in Nair.” Ex-1002 at ¶ 47; *see also* Ex-1002 at ¶¶ 45-54. I disagree with Dr. Bims, because Nair does not teach managing multiple public and private key pairs, and so would not have any of the problems that he suggests would motivate a POSITA to combine it with Forsberg.

90. Dr. Bims cites to a portion of Nair including paragraphs [0035] – [0038]. This portion of Nair describes two possible configurations of its disclosure.

91. In the first version, UEs send authentication requests which are encrypted with a network's public key. Ex-1004 at [0035]. The HSS holds the network's private key, and so is able to decrypt these requests. *Id.* Once decryption is complete, the IMSI can be used to identify the subscriber and authenticate them. Although this paragraph refers to an HSS/AuC "create[ing] authentication vectors (AVs) based on the distinct shared root key K between a user (subscriber) and the HSS/AuC," this does not refer to many public/private key pairs that the HSS must manage as Dr. Bims seems to suggest. Rather, the root key is a key that is included in a UE's SIM card when it is provisioned for/by the network operator, and that is used to authenticate the SIM card by ensuring that it responds correctly to a challenge-response type cryptographic exchange. The HSS only has to manage one public/private key pair—the network key pair mentioned earlier.

92. In the next paragraphs, Nair describes how multiple HSSs can be used to manage different sets of users. Ex-1004 at [0036]. This allows for more users to be supported by a network. However, because a user's authentication request must now be routed to the appropriate HSS, Nair introduces another concept: the Server Location Function (SLF). *Id.* The SLF uses the identity of the subscriber requesting authentication to send this request to the correct HSS, which means that it needs to be able to decrypt the IMSI. *Id.* at [0038]. The only way this is possible is if the SLF holds the network private key instead of the HSS (which no longer performs

decryption and thus no longer needs it). *Id.* Nair is still only describing one public/private key pair for the network, the private key has simply been moved to the SLF.

93. Accordingly, a POSITA implementing Nair will not encounter a situation in which they would look to Forsberg to “support this use of multiple keys.” Multiple keys are not used. For this reason, it is my opinion that a POSITA would not be motivated to combine Nair and Forsberg as Dr. Bims claims.

b) Claim 1

94. It is my opinion that claim 1 is valid in view of Ground 1 because Dr. Bims cannot show the limitations “encryption scheme identifier” or “public key identifier.”

i. “encryption scheme identifier”

95. Dr. Bims does not allege that Forsberg contains an encryption scheme identifier. Further, Dr. Bims is incorrect in his view that Nair includes an “encryption scheme identifier.” Therefore, it is my opinion that Petitioners’ Ground 1 fails because it does not teach the claimed “encryption scheme identifier” recited in claim 1 and each other challenged independent claim.

96. First, instead of disclosing “an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI,” Nair discloses a “privacy indicator,” which the reference teaches

operates as a flag or switch—it conveys whether encryption is “on” or “off,” as I explained in my description of Nair, above. The message in Nair does not identify an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI, it only identifies that encryption happened.

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

98. If the privacy indicator in Nair did identify the encryption scheme used to encrypt the subscription identifier in the SUCI, a POSITA would have expected the attach request to further include information needed to perform the decryption under that scheme, such as a key identifier. But Nair only contemplates one public/private key pair. *See* Ex-1004 at [0035], [0036], [0038]. The lack of this type

of information in the transmission reinforces that Nair does not teach an encryption scheme identifier, but instead an encryption if “on” or “off” indicator.

99. Likewise, there also is no disclosure in Nair that, based on the privacy indicator, the receiving device looks up the particular encryption scheme used (and the necessary key for that scheme). One would expect to see such disclosure if, in fact, the privacy indicator did identify an encryption scheme. This is because, if the privacy indicator identified a scheme, the receiving device could then look up the scheme and the cryptographic elements required to complete the decryption (*e.g.*, the necessary private key). There is no disclosure of supporting multiple encryption schemes in Nair, and Dr. Bims does not identify any such teaching.

100. Indeed, Nair relies on the opposite being the case. Instead of sending an encryption key along with the “attach request,” Nair teaches that the receiving device (*e.g.*, the SLF) already has the private key needed for the decryption; Nair touts this as an advantage of its simplified system. *See, e.g.*, Ex-1004 at [0035], [0038]. There is thus no need for Nair’s messages to identify an encryption scheme (and any additional information, such as information to identify a private key) because the receiving device (*i.e.*, HSS or SLF) already has the private key used to decrypt the message and knows what scheme to use in order to perform the decryption. Ex-1004 at [0036] (“the home HSS . . . possesses the private key that corresponds to the [subscriber’s] public key”), [0038] (“instead of the HSS storing

the private key, now [when using an SLF] the SLF would need to store and use the network private key”).

101. Despite this limited disclosure in Nair, Dr. Bims claims that “Nair’s implicit privacy indicator embodiment also ‘identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI,’” Ex-1002 at ¶ 79 (quoting Ex-1004 at [0042] – [0043] and Ex-1008 at 6:19-30). But Nair does not actually teach what Dr. Bims alleges.

102. Dr. Bims has selectively misquoted paragraph [0042] of Nair, which says the opposite of what Dr. Bims claims. I have reproduced paragraph [0042] below.

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).

103. This section states the opposite of what Dr. Bims alleges. It describes an “implicit” privacy indicator in which the receiving system “is informed of the privacy feature” by virtue of “the fact that the message is encrypted with a particular encryption algorithm.” Ex-1004 at [0042]. It does not disclose that the privacy indicator includes an encryption scheme identifier; it simply states that the receiving device can infer that the privacy indicator is set “by the fact that the message is encrypted with a particular encryption algorithm.” *Id.* Nair never teaches that the privacy indicator (whether explicit or implicit) itself contains an encryption scheme identifier. This section simply teaches that, if the message is encrypted, the receiving device can infer what the privacy indicator based on the results of trying to solve the received message.

104. In addition, the paragraphs 42 and 43 that Dr. Bims cites were new matter added to the Nair non-provisional application. That material is not included in the Nair Provisional application, including the 6:19-30 portion that Dr. Bims cites without discussing (reproduced below).

In a first illustrative embodiment, the 5G UE, if it wants to protect its privacy, adds an identity privacy flag (i.e., privacy indicator) to indicate that the MSIN is provided encrypted.

It could be suggested that the HSS or SLF, even without this privacy indicator, will figure out after the first attempt to solve the request and, if encrypted, to attempt the decryption. But one key reason to have such an indication specified is that this saves processing time and less resources are needed. Thus, in this first illustrative embodiment, the SLF can make the decision on the processing by looking at this flag. If not set, the SLF will assume the provided IMSI is unencrypted, will do the IMSI-to-HSS resolution, and will forward to the correct HSS/UDM, i.e., compatibility with 4G operation is maintained. If the flag is set, the SLF will recognise that the provided IMSI is encrypted and use the network private key to decrypt the MSIN part to form the real unencrypted IMSI, perform the IMSI-to-HSS resolution and then forward the Authentication Request to the correct HSS/UDM. If no SLF is used, the same principle can be used by the HSS/UDM. That is, HSS/UDM has to check whether the 5G UE has set a flag and then decide whether decryption is needed.

105. Contrary to Dr. Bims' claim that the privacy indicator includes the encryption algorithm of the message, this section describes that the "identity privacy flag (i.e., privacy indicator)" is something "to indicate that the MSIN is provided encrypted." Ex-1008 at 6:19–30. Because paragraphs 42 and 43 of Nair were not in the Nair Provisional application, I understand that they do not predate the '817 Patent's priority date. Dr. Bims does not even analyze whether paragraphs 42 and 43 are supported by a disclosure in the Nair Provisional.

106. Dr. Bims also claims that Nair's disclosure that a "privacy indicator" could be a "flag or field" means that Nair teaches an "encryption scheme identifier." Ex-1002 at ¶ 80. Dr. Bims does not actually explain what part of Nair discloses uses for a privacy field with more than just an "on" or "off" value because Nair never mentions this. Dr. Bims' allegation amounts to alleging that a POSITA would immediately jump from the word "field" to the inventions of the '817 Patent. I do not find this persuasive and disagree.

107. Dr. Bims further suggests that the existence of multiple encryption schemes would indicate to a POSITA that the privacy "field" or "flag" could be used to identify an encryption scheme because the SLF "would need to know the type of encryption used to encrypt an IMSI." Ex-1002 at ¶ 81. It is true that the SLF (or HSS) could not decrypt ciphertext without knowing the encryption algorithm to use, but all this would indicate to a POSITA is that Nair is a system that is only compatible with the use of one encryption scheme at a time.

108. This is apparent in the contrast between the '817 Patent and Nair. The '817 Patent discloses the use of multiple SIDFs (Subscription Identifier De-concealing Functions), each of which can be set up to handle different encryption schemes. Ex-1001 at 10:55-59. Conversely, Nair only discloses the use of a single SLF, which serves as the splitting point for incoming authentication requests to be routed to multiple HSSs. Ex-1004 at [0036]. This is consistent with the fact that Nair

never accounts for the use of multiple encryption schemes and, thus, cannot support them.

109. For the foregoing reasons, it is my opinion that Dr. Bims' opinions are incorrect because he is wrong in his conclusion that Ground 1 teaches an "encryption scheme identifier" as claimed in the '817 Patent.

ii. "public key identifier"

110. I disagree with Dr. Bims' opinion that the combination of Nair and Forsberg teaches the "public key identifier" recited throughout the '817 Patent. As an initial matter, I explain above why a POSITA would not be motivated to combine Nair with Forsberg. However, Dr. Bims makes additional errors in his opinions which I here address.

111. As I discussed above, Nair is built on the assumption that a single encryption scheme and a single public/private key pair will be used, obviating the need to signal anything how an IMSI is encrypted and allowing only an indication of if it is encrypted to suffice. Because the privacy indicator does not include any information other than whether encryption is "on" or "off," it has a very small memory footprint—as little as one bit. This is a design choice made by Nair which minimizes the data that must be transferred with its authentication requests.

112. However, Dr. Bims' proposed combination frustrates this choice. A privacy indicator alone is enough to tell Nair's HSS/SLF that a message includes

encrypted content and that its (single) private key should be used to decrypt it. Dr. Bims is suggesting adding additional data to the message that is effectively duplicative because, if it is known that the IMSI is encrypted, then there is no need to indicate how it is encrypted since Nair only accommodates one possibility. A POSITA would not be inclined to do this, because a POSITA would understand that transmitting more data than necessary in telecommunications signalling is wasteful of network resources. Accordingly, I disagree with Dr. Bims and hold the opinion that his Ground 1 does not teach a “privacy indicator” as recited in the claims of the ’817 Patent.

c) Claim 2

113. I understand that Claim 2 is a dependent claim of claim 1, and it is my opinion that the Dr. Bims has failed to show all the limitations of claim 1. Thus, I understand that claim 2 is not invalid for the same reasons.

114. I disagree with Dr. Bims that Nair discloses that “the determining of the de-concealing server is based on information received from the UE.” Dr. Bims argues that Nair’s disclosure of multiple SLFs (which Dr. Bims identifies with the “de-concealing server”) would suggest to a POSITA that information from a UE is used to determine a de-concealing server. Ex-1002 at ¶¶ 98-99. Dr. Bims misconstrues the disclosure of Nair when he states that, in Nair, “information received from the UE is used to determine the SLF . . . For example, Nair discloses

that the MNC and MCC sent in the UE’s authentication request is used to route [the] request to the correct home network.” *Id.* at ¶ 99 (citing Ex-1004 at [0035]). What Dr. Bims seems to have overlooked is that Nair is describing the SLF using the MNC and MCC to route a message to an HSS—there is no disclosure in Nair that the SLF is determined based on information from the UE. *See* Ex-1004 at ¶ [0036], [0038].

115. Dr. Bims has mapped the SLF to the “de-concealing server,” not the HSS. *See* Ex-1002 at ¶¶ 98-99. This aligns with Nair’s disclosure that, when an SLF is used to split message among different HSSs, the SLF possesses the network private key and performs decryption, not the HSS. *See* Ex-1004 at ¶ [0036], [0038]. Thus, Dr. Bims does not show that “the determining of the de-concealing server is based on information received from the UE.”

116. Dr. Bims also looks to Forsberg to support his arguments that this limitation is shown by Ground 1. *See* Ex-1002 at ¶¶ 100-101. As I discuss above, a POSITA would not be motivated to combine Forsberg with Nair because Nair does not contemplate multiple public/private key pairs to be managed by Forsberg’s system. Further still, what Dr. Bims points to in Forsberg only teaches using the MCC and MNC to route messages to a particular home network, not to a particular SLF, de-concealing server, or any other specific node in a network. *See id.* at ¶ 101 (citing Ex-1005 at ¶¶ [0049], [0051], [0053] – [0054]).

117. For these reasons, it is my opinion that claim 2 is valid.

d) Claims 3-6

118. I understand that Claims 3-6 are dependent claims of claim 1, and it is my opinion that the Dr. Bims has failed to show all the limitations of claim 1. Thus, I understand that claims 3-6 are not invalid for the same reasons.

e) Claim 8

119. I understand that Claim 8 is a dependent claim of claim 1, and it is my opinion that the Dr. Bims has failed to show all the limitations of claim 1. Thus, I understand that claim 8 is not invalid for the same reasons.

120. In addition, Dr. Bims relies on Nair's mentioning TR 33.899, which it says is incorporated by reference. Ex-1002 at ¶ 111. I am not aware of any portion of Nair that would prompt a POSITA to turn to TR 33.899 and decide to use ECIES. Nair only appears to reference TR 33.899 because it broadly addresses privacy in 5G. *See* Ex-1004 at [0007].

121. Nair also mentions that TR 33.899 discloses several "solution classes" for providing privacy which are, broadly: 1) replacing a subscription identifier with a temporary replacement, 2) encrypting the subscription identifier with a home network public key, 3) encrypting the subscription identifier with a serving network public key. Nair does not mention that a POSITA should turn to TR 33.899 to look for encryption schemes to apply to the IMSI, only to identify other classes of solution

to which the disclosure of Nair could possibly be applied. *Id.* at [0028] – [0031], [0034].

f) Claims 9-10

122. Claims 9 and 10 are independent claims for which Dr. Bims repeats the same opinions as he did for claim 1. *See* Ex-1002 at ¶¶ 112-119. Because Dr. Bims maintains the same opinions with respect to these dependent claims as he does for claim 1, it is my opinion that these claims are valid for the same reason as claim 1.

g) Claim 11

123. I understand that Claim 11 is a dependent claim of claim 10, and it is my opinion that Dr. Bims has failed to show all the limitations of claim 10. Thus, I understand that claim 11 is not invalid for the same reasons.

h) Claim 12

124. I understand that Claim 12 is a dependent claim of claim 10, and it is my opinion that Dr. Bims has failed to show all the limitations of claim 10. Thus, I understand that claim 12 is not invalid for the same reasons.

125. Dr. Bims refers to Nair’s disclosure of a USIM which “securely” stores information as teaching a “tamper resistant secure hardware component of the UE.” *See* Ex-1002 at ¶ 121. I disagree that the word “securely” suggests tamper resistance. Dr. Bims also suggests that the reference to 3GPP TR 33.899 made in Nair suggests the same element, but I disagree because nothing in Nair suggests that it is

referencing TR 33.899 for its discussion of the benefits of tamper resistance or how that might be achieved. *See id.*

i) Claim 13

126. I understand that Claim 13 is a dependent claim of claim 10, and it is my opinion that the Dr. Bims has failed to show all the limitations of claim 10. Thus, I understand that claim 11 is not invalid for the same reasons.

j) Claim 14

127. Dr. Bims makes only refers to his opinions on claim 8 for dependent claim 14. Thus, it is my opinion that claim 14 is valid for the same reasons I stated for claim 8.

k) Claim 15

128. I understand that, for claim 15, Dr. Bims repeats the same opinions he expressed for claim 1, with the addition of his opinion on element 15[c] which describes memory and processing circuitry. It is my opinion that Dr. Bims fails to show the functions which claim 15 describe the memory and processing circuitry being used to perform, as I describe with respect to claim 1 above. Thus, it is my opinion that claim 15 is valid, because Dr. Bims has not shown that all its elements are present in Nair in combination with Forsberg.

B. Ground 2 – Nair and Forsberg in further combination with Togawa

a) Motivation to combine Togawa with Nair and Forsberg.

129. I disagree with Dr. Bims’ opinions that a POSITA would be motivated to combine Nair and Forsberg with Togawa.

130. Dr. Bims suggests that Nair, Forsberg, and Togawa address the same problem of “securing messages within a communication system by identifying encryption and/or an encryption scheme identifier within the transmitted message.” Ex-1002 at ¶ 135. This is not quite right. Togawa only sends an “encryption-method ID” when keys are being exchanged between the receiving and transmitting device. Ex-1006 at 23:11-27. When the actual data message is transmitted between the two devices, no information about encryption scheme is included at all. But this is only one difference between the references.

131. Another, more prominent difference, is that Togawa contemplates multiple encryption schemes, but Nair only contemplates one encryption scheme. *Id.* at 23:6-11. Nair explains that the purpose of the “privacy indicator” is to save processing time by telling the HSS or SLF that encryption is turned on, so that it does not waste time trying to detect this. Ex-1004 at [0043]. However, this relies on there being only one encryption method used in Nair—otherwise the HSS/SLF could not expect an attempt to decrypt a message marked with a privacy “on” privacy indicator would yield a meaningful value.

132. Further still, it would no longer be possible for the SLF/HSS to interpret a failed decryption of the IMSI. One possible interpretation of such an event is that the UE had sent a message with fields that included errors. Another would be that the encryption scheme was chosen incorrectly and that another should be tried. Nothing in Nair discusses how to address such a problem, nor does it contemplate that the decryption could fail, because only one type of encryption is ever used. Accordingly, it is my opinion that Nair, Forsberg, and Togawa are incompatible.

b) Claim 1

133. I understand that Dr. Bims relies on Togawa to fix Ground 1's lack of disclosure for an "encryption scheme identifier," but I disagree with his opinions.

134. First, as I describe with respect to Ground 1, Nair and Forsberg fail to teach other limitations of claim 1. Second, Dr. Bims fails to justify why a POSITA would be motivated to combine Togawa with Nair and Forsberg. Nair and Forsberg are directed to an authentication system for 4G/5G networks, while Togawa is directed to a pre-smartphone era system for securing data communications over a voice call. A POSITA would not look at such an antiquated system to improve a modern telecommunications network. Further, a POSITA would not expect to succeed in combining Togawa with Nair or Forsberg because Nair does not support multiple encryption schemes. Further still Togawa teaches rotating its encryption

keys based on the passage of time during a voice call, which is a scenario that is not contemplated by Nair or Forsberg alike. *See* Ex-1006 at 4:38-60.

c) Claims 2-17

135. Dr. Bims collectively addresses claims 2-17 in his analysis of Ground 2. *See* Ex-1002 at ¶ 143. Dr. Bims only refers to his Ground 1 opinions that Nair and Forsberg teach the limitations of these claims, relying on Togawa only for the “encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI” limitation. *See id.* Accordingly, I disagree with Dr. Bims’ opinions on these claims for the same reasons I describe for Ground 1 and for claim 1 of this Ground.

C. Ground 3 and 4 – Grounds 1 and 2 in further combination with 5G-Ensure

136. Dr. Bims expresses the opinion that a POSITA would combine the references in Grounds 1 and 2 with the 5G-Ensure to incorporate an Elliptic Curve Integrated Encryption Scheme (ECIES). I disagree with Dr. Bims because 5G-Ensure actually opposes the use of an ECIES.

137. 5G-Ensure includes a section—the same section to which Dr. Bims refers—that discusses the use of Attribute Based Encryption (“ABE”) schemes. Ex-1010 at 32 (“an Attribute Based Encryption (ABE) could be used, instead of traditional public key encryption.”). 5G-Ensure is suggesting that ABE is an

alternative to “traditional public key encryption,” but Dr. Bims does not include any explanation of what Attribute Based Encryption is.

138. ABE is a complex encryption scheme that incorporates “attributes” into the public and private keys used in an ABE system. These attributes can be used to construct roles for various users. For example, a patient might have a public key with an attribute identifying them as a patient of an organization. The patient’s doctor, in turn, might possess a key identifying them as a doctor in the organization. By using these two keys together, a message can be encrypted by the patient such that it can only be decrypted by doctors in the organization who also have them as a patient. The utility of ABEs is that they allow organizations fine-grained control over what data is accessible to various parties.

139. By contrast, traditional public key encryption is simpler. In a standard public key encryption scheme, a public and private key pair exist such that the public key can encrypt messages and the private key can decrypt them. The two keys are generated simultaneously by a device, which retains the private key and shares the public key with other devices. Those devices with the public key can use it to encrypt messages that are only able to be opened by the holder of the private key. Importantly, a traditional public key encryption scheme does not include attributes in its keys, which would require an entirely different algorithm. Thus, ABE and traditional public key encryption are mutually exclusive.

140. ECIES is a traditional public key encryption. ECIES uses mathematical results from group theory and the analytical characteristics of elliptic curves to determine points on an elliptic curve which hold certain properties and serve as the basis for a public and private key pair. Determining one point from the other is computationally infeasible, but checking whether two points hold the appropriate properties is easily accomplished, which is generally necessary to construct a cryptographic algorithm. Because ECIES generates a standard public/private key pair, it is a traditional public key encryption scheme.

141. 5G-Ensure proposes that an ABE should be used to secure attach requests. Ex-1010 at 32-33. The only mention it makes of elliptic curves is that “ABE schemes based on elliptic curve pairings are practical” and inherently include certain useful properties. But 5G-Ensure is not suggesting the use of ECIES, because ECIES is not an ABE scheme. Instead, it is suggesting that an unspecified ABE scheme based on the mathematical theory of elliptic curves should be used.

142. Based on this, I understand that 5G-Ensure teaches away from using ECIES, and do not think that a POSITA would be motivated to use ECIES with Nair and Forsberg based on its disclosures. 5G-Ensure does not even mention ECIES, so it cannot possibly teach it. Accordingly, my opinion is that claims 8 and 14 are valid in view of Grounds 3 and 4.

VIII. Conclusion

143. This Declaration represents the opinions that I have formed to date based on the material currently available to me. I reserve the right to revise, supplement, and/or amend my opinions stated in this Declaration based on new information that becomes available to me and on my continuing analysis of the materials available.

144. 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 are made with the knowledge that willful false statements and the like so made are punishable by fine, imprisonment, or both, under 18 U.S.C. § 1001.

Dated: December 6, 2024


Dr. Mark Mahon