

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

PATENT OWNER'S RESPONSE

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

TABLE OF CONTENTS

I. INTRODUCTION	1
II. BACKGROUND	2
A. TECHNICAL BACKGROUND	2
B. THE '817 PATENT	3
C. ALLEGED PRIOR ART	8
1. Nair	8
2. Forsberg	10
3. Togawa	12
4. 5G-Ensure	13
III. CLAIM CONSTRUCTION OF “ENCRYPTION SCHEME IDENTIFIER”	14
IV. ARGUMENT.....	17
A. GROUND 1 – NAIR AND FORSBERG	17
1. A POSITA would not be motivated to combine Nair and Forsberg.	17
2. Independent Claim 1.....	20
3. Claim 2	25
4. Claim 3	27
5. Claim 4	27
6. Claim 5	27
7. Claim 6	27
8. Claim 8	27
9. Independent Claim 9.....	28
10.Independent Claim 10.....	28
11.Claim 11	28
12.Claim 12	28
13.Claim 13	29
14.Claim 14	29

15.Independent Claim 15.....	29
16.Claim 16	29
B. GROUND 2 – NAIR, FORSBERG, AND TOGAWA	29
1. A POSITA would not be motivated to combine Nair, Forsberg, and Togawa.	29
2. Independent Claim 1.....	32
3. Independent Claims 9, 10, and 15	33
4. Dependent Claims 2-6, 8, 11-14, and 16-17	33
C. GROUNDS 3 AND 4 – GROUNDS 1 AND 2 IN FURTHER COMBINATION WITH 5G- ENSURE.....	33
1. 5G-Ensure teaches away from using an “Elliptic Curve Integrated Encryption Scheme (ECIES).”	33
D. SECONDARY CONSIDERATIONS	36
V. CONCLUSION	37

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Callaway Golf Co. v. Acushnet Co.</i> , 576 F.3d 1331 (Fed. Cir. 2009)	27, 29
<i>In re De Seversky</i> , 474 F.2d 671 (C.C.P.A. 1973)	27
OTHER AUTHORITIES	
Investigation No. 337-TA-1375	passim
U.S. Application No. 2018/0324585	passim
U.S. Application No. 2013/0003971	passim
U.S. Patent No. 8,005,219	passim
U.S. Patent No. 10,425,817	passim

TABLE OF EXHIBITS

Ex. Number	Title	Previously Submitted
1001	U.S. Patent No. 10,425,817	X
1002	H. Bims Declaration in support of IPR	X
1004	U.S. Application No. 2018/0324585 (“Nair”)	X
1005	U.S. Application No. 2013/0003971 (“Forsberg”)	X
1006	U.S. Patent No. 8,005,219 (“Togawa”)	X
1008	U.S. Provisional Patent Application 62/502,266 (“Nair Provisional”)	X
1010	5G-Ensure Deliverable D3.1 5G-PP security enablers technical roadmap (early version)	X
1011	A Survey of the Elliptical Curve Integrated Encryption Scheme	X
2001	Excerpts of the May 31, 2024 Deposition Transcript of Harry V. Bims, Ph.D.	X
2002	Security in 5G Networks – How 5G networks help Mitigate Location Tracking Vulnerability	X
2003	3GPP TSG-SA WG3 Meeting #88 Tdoc S3-172106	X
2005	Declaration of Dr. Mark Mahon	
2006	CV of Mark Mahon	
2007	November 22, 2024 Deposition Transcript of Harry Bims	
2008	Investigative Staff’s Post-Hearing Reply Brief in Investigation No. 337-TA-1375 (Redacted)	
2009	Respondents’ Post-Hearing Brief in Investigation No. 337-TA-1375 (’817 Patent Excerpts)	
2010	July 16, 2024 Evidentiary Hearing Transcript in Investigation No. 337-TA-1375 (Open Session)	

I. Introduction

Following the Board’s Decision Granting Institution of *Inter Partes* Review (“Decision”), Patent Owner Telefonaktiebolaget LM Ericsson (“Ericsson”) sets forth the substantive errors, omissions, and shortcomings underlying the alleged grounds for invalidity argued in the Petition for *Inter Partes* Review of U.S. Patent No. 10,425,817 (the “’817 Patent”) (“Petition” or “Pet.”). Each of Petitioner’s Grounds are flawed.

First, Petitioner fails to show that Nair’s “privacy indicator,” which signals only whether encryption is “on” or “off,” satisfies the scope of the ’817 Patent’s “encryption scheme identifier” limitations. It does not, as Ericsson explains below.

Second, Petitioner cannot justify its combination of Nair and Forsberg, which it alleges would teach the “public key identifier” limitations of the challenged claims. But Nair and Forsberg are incompatible, and so this combination should fail.

Third, Petitioner fails to show motivation to combine Togawa with Nair or Forsberg in its Ground 2. Togawa is directed to a system for encrypting user data over a voice signal and is entirely unrelated to 4G/LTE or 5G communications systems.

Fourth, Petitioner’s Grounds 3 and 4 rely on the combination of 5G-Ensure with the preceding Grounds in an effort to satisfy the “Elliptic Curve Integrated Encryption Scheme (ECIES)” limitations of dependent claims 8 and 14. However,

as Ericsson will explain, Petitioner's argument is inapposite because 5G-Ensure teaches away from using ECIES.

In support of this Patent Owner's Response, Ericsson provides a declaration from its expert, Dr. Mark Mahon (Ex-2005). Dr. Mahon's CV is attached as Ex-2006. Additionally, the same references were previously asserted as prior art in the International Trade Commission ("ITC") Investigation No. 337-TA-1375. During that investigation, the commission Investigative Staff filed a Post-Hearing Brief (Ex-2008) which addressed issues related to validity of the '817 Patent in light of Nair, Forsberg, Togawa, and 5G-Ensure, which Ericsson provides citation to where relevant.

Ericsson respectfully requests that the Board reject Petitioner's flawed arguments and find that the '817 Patent's challenged claims are valid.

II. Background

A. Technical background

The '817 Patent claims techniques to securely communicate subscriber identifiers in cellular systems like 5G. In cellular systems, the SIM card in user equipment ("UE") such as cell phones includes a unique, long-term identifier that is used to identify the user to networks. In 5G, 4G, and earlier technologies standardized by the 3GPP, this identifier is called an International Mobile Subscriber Identifier ("IMSI"). The IMSI consists of three parts: the MCC (mobile country

code), the MNC (mobile network code), and the mobile subscriber identification number (MSIN). The MSIN part is used to uniquely identify a user when a UE attempts to attach to it. This allows the network to identify the subscriber and authenticate the UE to complete the attach process with the network.

Because the IMSI can be used to identify a UE as belonging to a particular user, preventing the IMSI from being obtained by malicious actors is an important security concern for network operators and users alike. So-called “IMSI catchers” could be used to capture the ISMI and track the user or engage in other unwanted activity. Ex-2002 at 1, 3. Earlier 3GPP systems such as 4G (sometimes referred to as LTE) and 3G provided some degree of security against such attacks by generating a short-term subscription identifier for UEs which could be used to identify the UE after its initial connection to the network. Ex-1001 at 1:24-31. Even if a temporary subscription identifier was obtained by an attacker, it would become invalid after a short time, meaning that it had limited utility to a would-be attacker. However, these earlier standards still required that the IMSI be sent over the air in plaintext form during the initial registration of the UE with the network. Thus, temporary identifiers only reduced the risk of IMSIs being caught but could not eliminate it.

B. The '817 Patent

Recognizing these problems, the inventors of the '817 Patent proposed a design change that could be incorporated into the next generation 5G standard.

While the identifiers from past standards would be retained, an additional layer of security was added by encrypting the IMSI itself and including it in a subscription concealed identifier (“SUCI”). *See* Ex-1001 at 1:50-61, 8:19-35.

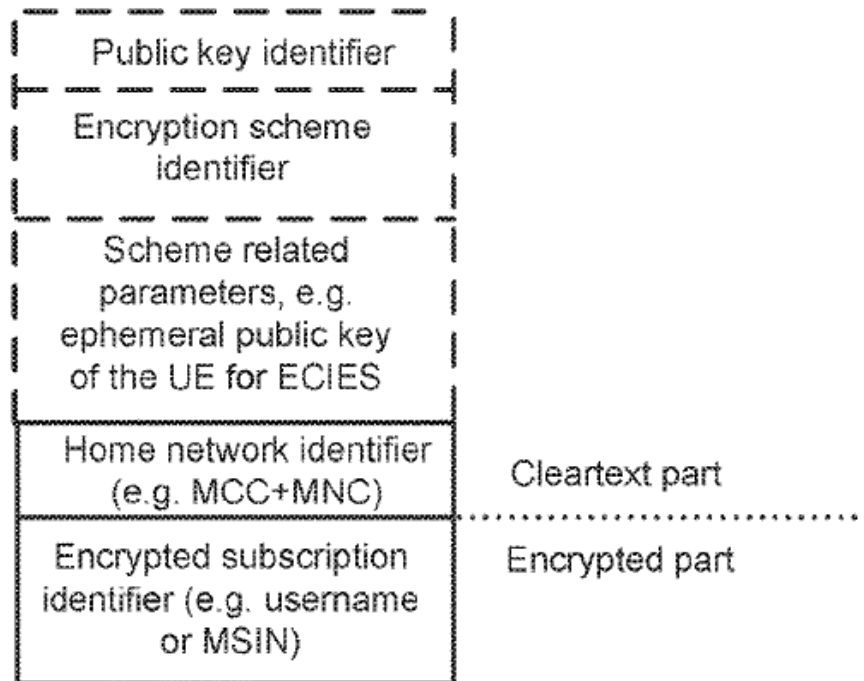


Fig. 3

The SUCI, illustrated in Figure 3, contains both an encrypted part and a clear-text part. *See id.* at 8:36-40. The clear-text part includes information for routing the attach request, namely a home network identifier consisting of the MCC and MNC parts of the IMSI, and information necessary for decrypting the contents of the encrypted part. *See id.* at 8:41-61, 9:4-6. The encrypted part contains the MSIN (*i.e.*, the portion of the ISMI that identifies the subscriber). *See id.* at 8:62-67.

The “encryption scheme identifier” and “public key identifier” are both key concepts with respect to Ericsson’s arguments below. An “encryption scheme identifier” refers to a value (typically four bits) that encodes the identifier for the encryption scheme (*e.g.*, the null-scheme, ECIES, or RSA) that the UE has used to encrypt the subscriber-identifying portion of the IMSI. *See id.* at 10:17-24, 10:55-59. The ’817 Patent describes deploying multiple Subscriber Identification De-Concealing Functions (“SIDFs”) in the network, each responsible for decrypting a different encryption scheme, wherein its scheme identifier is used to select the appropriate scheme when handling an encrypted SUCI. *Id.* Similarly, the public key identifier corresponds to the public key which the UE used along with the encryption scheme when preparing the encrypted part. It allows the SIDF to pick the appropriate private key with which to decrypt the SUCI’s encrypted payload. The ’817 Patent illustrates the registration process using the SUCI in Figure 6.

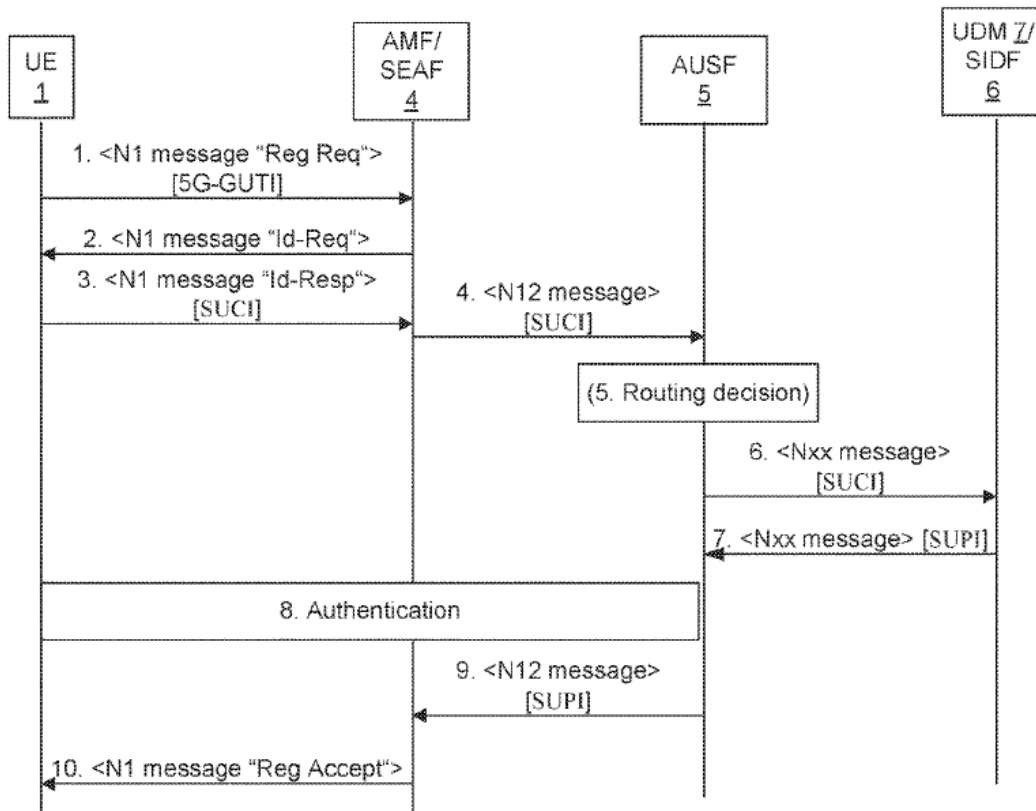


Fig. 6

In Step 1, the UE sends a registration request to the Authentication and Mobility Management Function (“AMF”) and Security Anchor Function (“SEAF”) of the core network. *See id.* at 10:38-43. For a UE performing initial registration, the AMF/SEAF will respond with a request for identification from the UE in Step 2. *See id.* In Step 3, the UE sends the SUCI discussed above and illustrated in Figure 3 to the AMF/SEAF. *Id.* In Step 4, the AMF/SEAF passes the SUCI to the Authentication Server Function (“AUSF”) for authentication. *Id.* At Step 5, the subscriber identification information is still encrypted, so the AUSF uses the clear-text portion of the SUCI to determine how to route a request for decryption to one of the available

SIDFs. *See id.* at 10:48-11:12. The SIDF decrypts the SUCI, and this information is forwarded back down the chain to the AUSF for authentication and to the AMF/SEAF to complete registration and notifies the UE that its registration request was accepted. *See id.* at 11:11-36.

Using this methodology, the '817 Patent's inventors resolved the long-standing risk to privacy that plaintext IMSIs posed to users and network operators alike. Ex-2005 at ¶¶ 47, 59. In addition, they did so in a way that provided flexibility for network operators and UE manufacturers. *Id.* As observed by the authors of Security in 5G Networks, the solution claimed in the '817 Patent, and eventually adopted into the 5G standard, means that “network operators can choose which of the encryption schemes they want to use” from a variety of secure options. Ex-2002 at 4. One of these options is ECIES, a “resoundingly secure” encryption scheme with high computational complexity, but the '817 Patent contemplates other, lower complexity schemes such as RSA¹ as well. *Id.*; Ex-1001 at 10:55-59; Ex-2005 at ¶ 57. This means that network operators can choose to implement multiple encryption

¹ RSA is another encryption scheme, named for Rivest, Shamir, and Adleman, who first described the algorithm. Ex-2005 at ¶ 57. RSA is not considered as secure as ECIES, but it requires less computational resources to encrypt and decrypt. Accordingly, RSA may be preferred by low-cost UEs which cannot execute the ECIES algorithm without impacting performance of the device. *Id.*

schemes in their networks, and UEs can choose their preferred scheme when encrypting subscriber information.

C. Alleged Prior Art

1. Nair

Every one of Petitioner's Grounds relies on U.S. Application No. 2018/0324585 ("Nair"), published November 8, 2018. Nair addresses the problem of encrypting an IMSI during authentication of a UE in a way that differs from the '817 Patent's claimed inventions because it does not provide flexibility in identifying an encryption scheme or public key to be used for securing the IMSI. *See* Ex-2005 at ¶ 68-70. In particular, Nair assumes that an IMSI will either not be encrypted or that it will be encrypted using a fixed scheme that is not communicated between the UE and the network. *See id.* As a result, a UE connecting using Nair's security approach has no flexibility in selecting an encryption scheme that suits its privacy and processing needs, because the only choice available to a UE is turning encryption "on" or "off." *See id.*

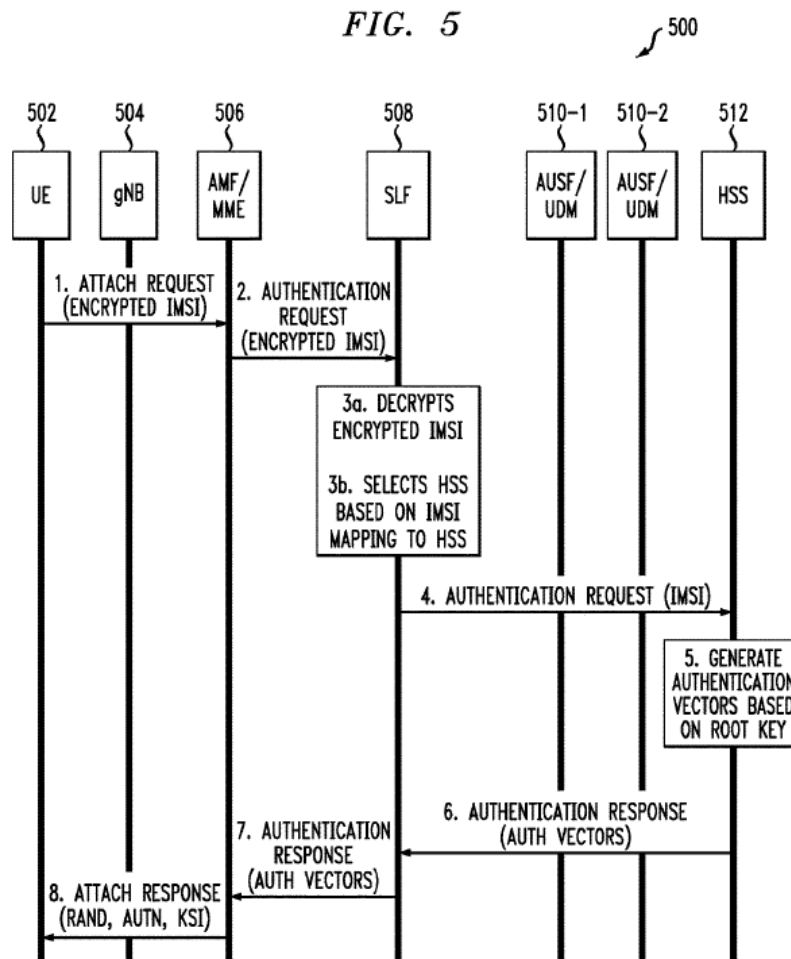


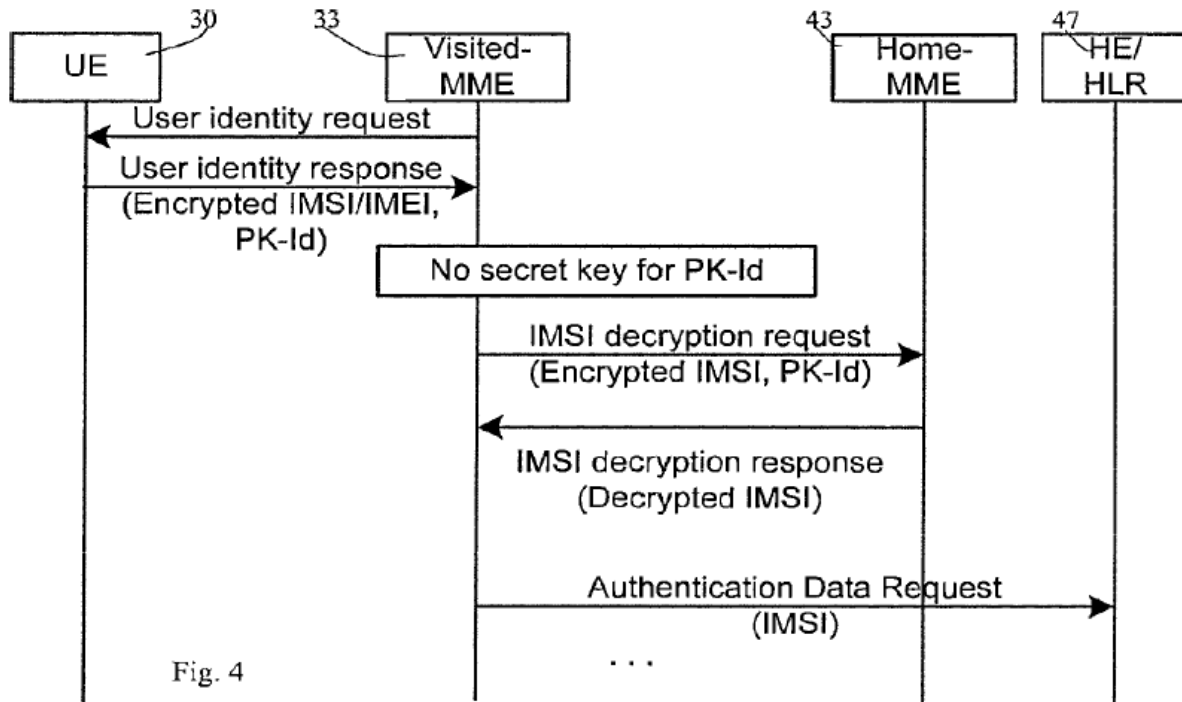
Figure 5 of Nair depicts the general process that is relevant to each of Petitioner's Grounds. A UE sends an attach request to a 4G or 5G core network, including an "encrypted IMSI." Ex-1004 at ¶¶ 74-76. The request is received by the AMF/MME (506) which forwards the request to the Subscriber Location Function or "SLF" (508) to decrypt the IMSI. *Id.* Subsequent authentication functions are performed before an attach response is returned to the UE. *Id.*

The structure of the “attach request” is of critical importance to the present dispute. Nair describes a “‘privacy’ attach request” which includes a “privacy flag” or “privacy indicator” which indicates if the subscriber identifier is provided in encrypted form. *Id.* at ¶¶ 40-41. The purpose of this privacy indicator is to save processing time in the SLF. *Id.* at ¶ 43. Because, as the Board noted, Nair’s privacy indicator serves solely to indicate if encryption has been applied to the IMSI and does not contain information about the type of encryption used (if any), there are only two possible values for the indicator. *See id.* at ¶¶ 42-43; Decision at 24-25. Accordingly, the SLF needs only to attempt to decrypt the encrypted content of the request, after which it will know if the content was encrypted or already provided in plaintext form. Ex-1004 at ¶¶ 42-43; Ex-2005 at ¶¶ 71-72. If the IMSI contained in the request is encrypted, the SLF uses a network private key to perform the decryption. Ex-1004 at ¶ 43. It is not necessary for the UE to signal what encryption method has been used or what public key it used to encrypt the IMSI, because the SLF relies on the assumption that the UE will use the algorithm and public key corresponding to its algorithm and private key. Ex-2005 at ¶¶ 68, 111.

2. Forsberg

Petitioner also relies on U.S. Application No. 2013/003971 (“Forsberg”), published January 3, 2013, for each of its asserted Grounds. Forsberg discloses a process for authenticating an MME when it is roaming, meaning that it is outside its

home network. *See* Ex-1005 at ¶ 41. Figure 4 of Forsberg illustrates the disclosed process.



The reference describes a roaming UE communicating with “Visited MME” in the visited network and sending identity information, containing an encrypted IMSI, to the Visited MME. *Id.* at ¶ 43, 49. Forsberg discloses that a Visited MME may not be able to decrypt the IMSI, and thus, may request assistance from the MME in the home network for the UE. *Id.* at ¶¶ 44-45, 50-51. The Home MME then decrypts the IMSI and returns the unencrypted value to the Visited MME. *Id.* at ¶ 54.

3. Togawa

U.S. Patent No. 8,005,219 (“Togawa”) was issued on Aug. 23, 2011 and describes an entirely different and unrelated system from the one claimed in the ’817 Patent. Togawa does not relate to LTE or 4G. It instead describes a system for embedding encrypted data within a voice signal and a key rotation technique for maintaining security over the course of a voice call. *See* Ex-1006, 4:29-7:45, Fig. 1.

Togawa describes that, during establishment of a voice call, an encryption key can be sent between the two devices participating in the voice call and then used for encrypting user data. *Id.* at 4:38-46. Over the course of the call, the devices keep track of the call duration, and periodically change the encryption key used (*i.e.*, “from a ‘key A’ to a ‘key B’ to a ‘key C’”). *Id.* at 4:61-5:4. When encrypted user data is received, the receiving device references the call duration and uses it to select a key to decrypt the user data. *Id.* at 5:5-13.

Nowhere in Togawa is authentication of a UE discussed, nor is an IMSI or the need to decrypt the IMSI when it is sent to the core network disclosed. Indeed, Togawa does not seem to contemplate encrypted data being transmitted to the core network at all, but instead, describes encrypting data between two cellular phones participating in a voice call. *See id.* at 2:15-20 (explaining that improved techniques are needed because cellular phones have lower processing power). Togawa has nothing to do with the problems solved by the ’817 Patent.

4. 5G-Ensure

Petitioner relies on 5G-Ensure Deliverable D3.1, the “5G-PPP security enablers technical roadmap (early version)” (“5G-Ensure”) as a secondary reference for Grounds 3 and 4. 5G-Ensure was developed by the 5G-PPP, which is an EU-funded group of projects related to 5G security. Ex-2005 at ¶ 87.

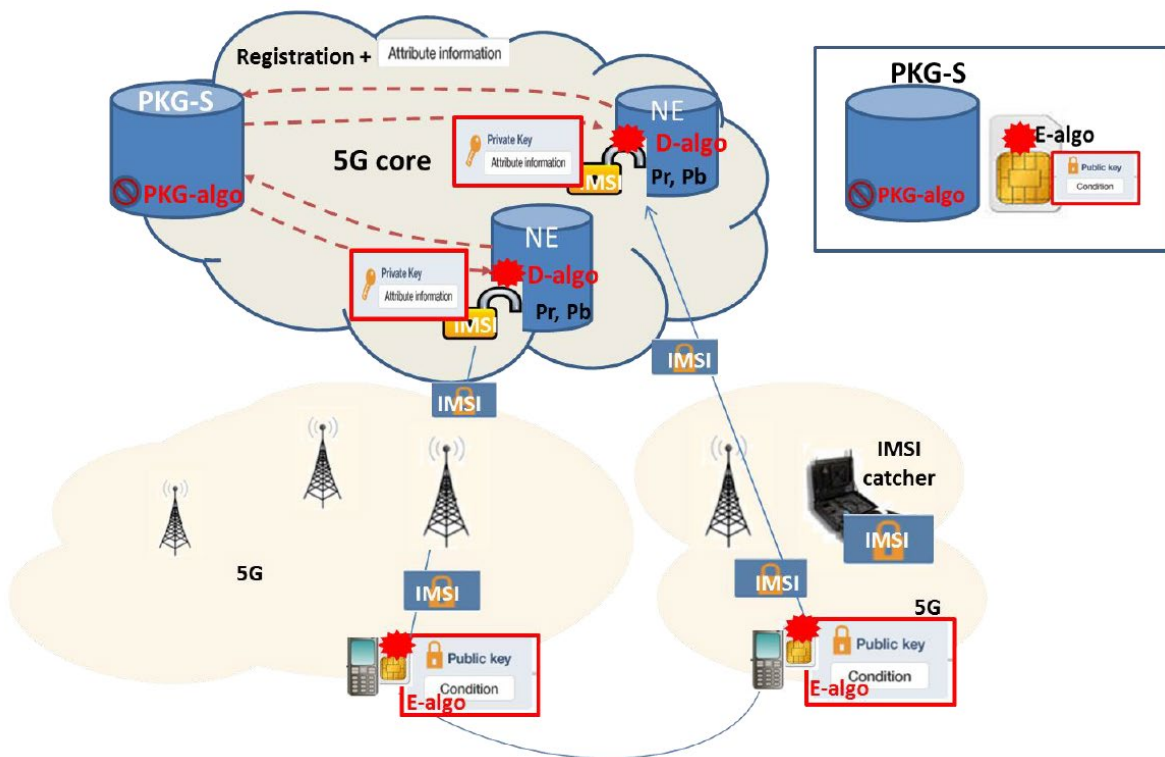


Figure 5: High level components of the feature “Encryption of Long Term Identifiers”

As its name suggests, 5G-Ensure is a road map that discusses high-level concepts relating to the encryption of long-term identifiers in 5G network while avoiding implementation details. See Ex-1010 at 32-34, Fig. 5. The reference does not disclose the structure of transmitted subscriber information, which parts are clear-text, which parts are encrypted, and what other information must be included

in a message to enable routing or decryption (*e.g.*, an encryption scheme identifier or public key identifier). 5G-Ensure further does not address the network nodes that should be used in such an implementation.

III. Claim Construction of “Encryption Scheme Identifier”

The Board recognized that the meaning of the term “encryption scheme identifier” is a determining factor in whether the challenged claims of the ’817 Patent are valid. *See* Decision at 25. In particular, the Board requested clearly designated analysis of Ericsson’s position on whether the limitation “encryption scheme identifier” is satisfied by a flag indicating whether encryption is on or off. *See id.* at 25-26. It is not, because an “encryption scheme identifier” must be capable of identifying at least two possible encryption schemes.

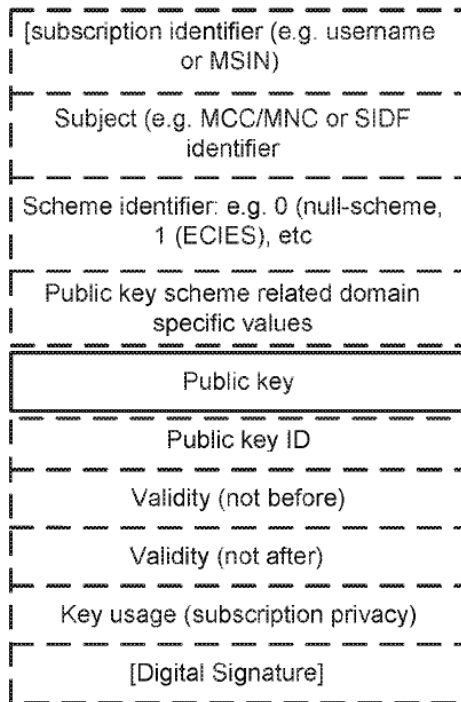


Fig. 4

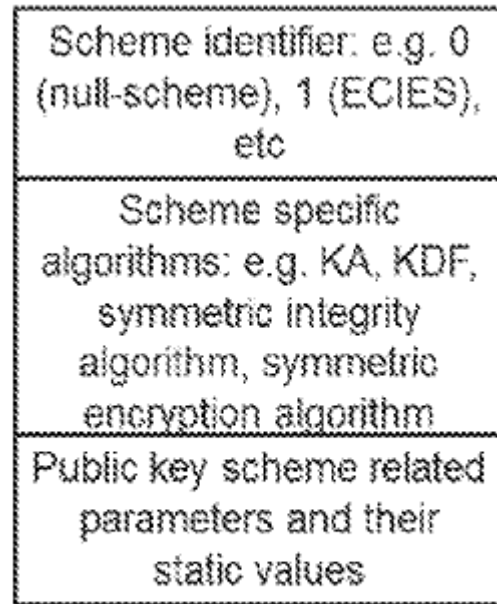


Fig. 5

The scope of this limitation is supported throughout the '817 Patent. For example, Figure 4, reproduced above, depicts “an example of a privacy key” as claimed in the '817 Patent, which includes a “Scheme identifier: e.g. 0 (null-scheme), 1 (ECIES), etc.” Ex-1001 at 5:45, Fig. 4. Similarly, Figure 5 (also reproduced above) illustrates a 3GPP public key privacy scheme, with the same “Scheme identifier: e.g. 0 (null-scheme), 1 (ECIES), etc.” information included. *Id.* at 5:46, Fig. 5. This identical “scheme identifier” disclosure between the privacy key and the privacy scheme is present because the privacy key identifies the privacy scheme by setting its “encryption scheme identifier” to a value corresponding to that of the scheme used. *See* Ex-2005 at ¶¶ 54-57. Importantly, in both instances, the

example provided includes values of 0, 1, etc., plainly indicating that the encryption scheme is capable of accommodating more than simply an on or off indicator; it identifies the actual encryption scheme that the UE used to encrypt the SUCI (*e.g.*, ECIES). This same disclosure is once again repeated in Figure 5. *See id.*, Fig. 5.

Each time the '817 Patent discusses the scope of the term “encryption scheme identifier,” the capability of identifying more than two options is reiterated. The detailed description of Figure 5 explains: “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.” *Id.* at 10:17-20. In addition, the null-scheme and ECIES, the '817 Patent also discloses that the SIDF, which is used for decrypting the encrypted portion of the IMSI, may be configured to handle RSA. *See id.* at 10:55-58. The '817 Patent also contemplates many data structures which may be used to embody the “encryption scheme identifier,” including a “4-bit identifier,” an “integer,” a “numeric string,” an “alphanumeric string” or a “bit string.” *Id.* at 10:20-24. As Dr. Mahon explains in his Declaration, each of these data structures is capable of representing more than two different states (*e.g.*, a four-bit identifier could identify up to 16 encryption schemes). Ex-2005 at ¶ 55. Conspicuously omitted are any data structures that would not be capable of identifying more than two schemes such as a boolean or a single bit. *Id.* at ¶ 56. Nor is there a disclosure where the

identifier only indicates that a message is encrypted but does not identify *which* encryption scheme.

Dr. Mahon’s opinion on the scope the term “encryption scheme identifier” is uncontroverted. When asked if an “encryption scheme identifier” could refer to “a scheme other than the elliptic curve scheme and null scheme” during deposition, Petitioner’s expert, Dr. Bims, answered “I don’t have an opinion on the scope of claim 1 includes other encryption schemes other than what is expressly disclosed in the patent.” Ex-2007 at 41:9-42:3. But every instance in which the ’817 Patent expressly speaks to the scope of the term “encryption scheme identifier” contemplates the capability of identifying more than two encryption schemes. Accordingly, the Board should find that a proper claim construction for “encryption scheme identifier” could not encompass a flag that is nothing more than an on or off indicator and does not itself identify an encryption scheme.

IV. Argument

A. Ground 1 – Nair and Forsberg

1. A POSITA would not be motivated to combine Nair and Forsberg.

The foundation of Petitioner’s argument that a POSITA would be motivated to combine Nair and Forsberg is the reasoning that “Nair teaches the benefits of using multiple keys during the encryption process to facilitate key mapping to

multiple HSSs,” and a POSITA would look to Forsberg to aid in “the complexities of managing multiple public and private key pairs within an SLF.” Pet. at 19-20. The problem with this argument is that it misunderstands the Nair disclosure to which it cites. *See id.* (citing Ex-1004 at ¶¶ 35, 36, 38).

As Dr. Mahon explains, Nair’s paragraph 35 summarizes the process of a UE authenticating with a network that contains only one HSS. Ex-2005 at ¶ 91. The paragraph explains that a UE will send an encrypted IMSI to the HSS, which the HSS will use the network operator’s private key to decrypt. Ex-1004 at ¶ 35 (“the home operator provides its public key to all home network subscribers . . . the home HSS can decrypt the message because it possesses the private key that corresponds to the public key”); *id.* The HSS, having identified the IMSI, will then “create authentication vectors (AVs) based on the distinct shared root key K between a user (subscriber) and the HSS/AuC.” Ex-1004 at ¶ 35. These authentication vectors are only created after the decryption of the IMSI is complete, and the “distinct shared root key” is nothing more than the key included on a user’s SIM card, not an additional value which the HSS must now track. Ex-2005 at ¶ 91. There is only one key pair of importance: the network’s public key (shared with the UE) and the network’s private key (shared with the HSS). *Id.*

The same is true in the following paragraphs 36 and 38. Nair discloses that an operator may choose to have more than one HSS, so that users can be split up across

them. Ex-1004 at ¶ 36. Nair introduces the SLF, which sits in between the UE and multiple HSSs to facilitate this configuration. *See id.* (“a Server Location Function (SLF) may be implemented in front of a set of HSSs . . . and routes [the authentication request] to the correct HSS.”). Because each HSS handles a distinct group of users, the SLF cannot direct the message to the correct one until it knows what user is requesting authentication, which means it must be the one to decrypt the IMSI. *See id.* at ¶ 38 (“if the home operator uses an SLF to split its set of subscribers, the SLF would need to evaluate the received identifier first.”). Thus, “instead of an HSS storing the private key, now the SLF would need to store and use the network private key.” *Id.* There is still only one key pair here, but it resides with the SLF instead of with the multiple HSSs. Ex-2005 at ¶ 92.

Given this disclosure, it is not clear why Petitioner believes “Nair teaches the benefits of using multiple keys during the encryption process to facilitate key mapping to multiple HSSs.” Pet. at 19. It does not. *See* Ex-2005 at ¶ 93. This also means that a POSITA would not be looking for a solution to “the complexities of managing multiple public and private key pairs within an SLF” as Petitioner suggests, because there is only one key pair within the SLF. Pet at 20; Ex-1004 at ¶ 38 (“the SLF would need to store and use *the* network private key.”). Contrary to what Petitioner argues, a POSITA would not be motivated to combine Nair and Forsberg. Accordingly, the Board should reject Petitioners’ Ground 1.

2. Independent Claim 1

a) Neither Nair nor Forsberg disclose an “encryption scheme identifier.”

The Nair and Forsberg references do not expressly disclose an “encryption scheme identifier.” Petitioner’s expert, Dr. Bims, does not dispute this. Ex-2007 at 31:14-19, 48:18-21; Ex-2010 at 1317:12-15, 1317:19-21 (stating the same during the ITC hearing). In its Decision, the Board raised the question of whether these references “teach or suggest” the limitation. Decision at 25. They do not.

As an initial matter, there is no dispute that Forsberg does not teach an “encryption scheme identifier” as required by the challenged claims. Petitioner relies solely on Nair to satisfy this limitation for its Ground 1. Petitioner’s expert agreed that he “[had] not identified an encryption scheme identifier in Forsberg.” Ex-2007 at 48:18-21; *see also* Ex-2008 at 9 (Investigative Staff agreeing that Forsberg does not disclose an “encryption scheme identifier”).

Nair’s privacy indicator does not identify an encryption scheme at all because it is a single-bit value representing whether or not encryption has been applied to the IMSI included in the attach request—not what encryption scheme, if any, has been used. Ex-1004 at ¶¶ 16, 43. As discussed above in Section III, an “encryption scheme identifier” requires more than a simple “on” or “off” flag. *See* Ex-1001 at 10:17-24. The purpose of the ’817 Patent’s encryption scheme identifier is, as the name states,

to allow the core network to map the received SUCI to the appropriate encryption scheme to be used for decryption. *See id.* at 10:53-58 (describing the AUSF using the scheme identifier to route the received SUCI to the appropriate SDF). Nair's privacy indicator does not accomplish this because it assumes that only one encryption scheme used, and therefore can figure out if encryption was used by a single trial or error test. *See* Ex-1004 at ¶ 43.

In fact, Nair discloses only a single Server Location Function ("SLF") which performs decryption of the received payload. *See id.* at ¶ 39. This is a direct result of the single encryption scheme accommodated by Nair. *See* Ex-2005 at ¶¶ 107-108. In contrast, the '817 Patent discloses multiple SDFs, deployed separately to handle the different encryption schemes that can be indicated by the "encryption scheme identifier." *See id.*; Ex-1001 at 10:55-59. A POSITA would not understand Nair's "on" or "off" flag to teach an identifier for multiple encryption schemes when Nair has no need to make use of such an identifier for routing encrypted data to the appropriate node. *See* Ex-2005 at ¶¶ 107-108.

Nair never discloses that its "privacy indicator" is ever used for anything other than a simple check to determine whether decryption is needed. *See* Ex-1001 at 6:19-30; *see also* Ex-2005 at ¶ 97. This check is simply performed to save processing time over attempting to solve the received authentication request and determining that it was encrypted if a plaintext value is not present. Ex-2005 at ¶¶ 97-98. Nair never

uses the privacy indicator to determine *what* encryption scheme is used. *Id.* There would also be no need for identifying an encryption scheme because Nair does not disclose multiple encryption schemes. *Id.* at ¶ 99.

Nair also cannot teach an “encryption scheme identifier” based on some shared agreement between the UE and SLF as Petitioner attempts to argue. Pet at 34-35. Nair’s SLF merely assumes that a privacy indicator showing that encryption has been applied means that the encryption scheme which it is configured to decrypt was the one applied. *See* Ex-1004 at ¶ 43; Ex-2005 at ¶ 68-70. This does not imbue the SLF with knowledge of the encryption scheme “used by the UE” because it is not based on actual identification of an encryption scheme that comes from the UE. A UE could just as easily use another encryption scheme and (correctly) set the privacy indicator of Nair to show that the IMSI has been encrypted. From the SLF’s perspective, there is no difference in this malignant case because nothing the SLF receives actually “identifies an encryption scheme used by the UE.” Ex-1001 at Claim 1, 9, 10, 15.

Further, the Board agreed with Ericsson that the Nair application post-dates the priority date of the ’817 Patent and that the disclosures of Nair are only prior art to the extent that they are also included in the Nair Provisional (Ex-1008). *See* Decision at 15-16. Nonetheless, Petitioner and their expert rely on disclosure in Nair that is new, such as Nair’s alleged disclosure of an “implicit privacy indicator” that

“informs” “the network element/function receiving the message from the UE” that a “particular encryption algorithm” has been used. *See* Pet. at 33-34 (citing Ex-1004 at ¶ 42-43); Ex-1003 at ¶ 79; Ex-2005 at ¶¶ 104-105. This new matter is unsupported in the Nair Provisional and Petitioner’s expert, Dr. Bims, does not provide any analysis of why he believes that it qualifies as prior art disclosure. Ex-2005 at ¶¶ 104-105.

As Ericsson explained in its Patent Owner Preliminary Response, the ’817 Patent is the subject of parallel proceedings before the ITC. In those proceedings, the Staff agreed with Ericsson that Nair does not teach an “encryption scheme identifier” because Nair relies on the UE and network both knowing what the encryption scheme is rather than identifying the scheme. *See* Ex-2008 at page 6. Indeed, even Lenovo conceded in its post-hearing brief, as did its expert during the ITC hearing, that Nair does not disclose the encryption-scheme identifier—and that a POSITA would have needed to look to Togawa for that teaching. Ex-2009 at 12; Ex-2010 at 1280:8-14. Accordingly, the Board should find that Petitioners’ Ground 1 fails to disclose an “encryption scheme identifier” as required by the challenged claims.

b) Nair does not teach a “public key identifier” and combination with Forsberg does not cure this deficit.

Petitioner contends that the combination of Nair and Forsberg teaches a “public key identifier.” Pet at 38. There is no dispute that Nair does not discuss public key identifiers. *See* Ex-2007 at 31:20-32:2; Ex-2010 at 1317:16-18 (Dr. Bims stating the same at the ITC hearing). Nair only discloses a single public key, so there would be no need to identify it. *See* Ex-1004 at ¶ 35 (“the home operator provides its public key to all home network subscribers.”). To cure this deficit, Petitioner argues that Nair would be combined with Forsberg such that it would have multiple public keys at its disposal and include a “public key identifier” alongside its privacy indicator when an encrypted IMSI to the network. Pet. at 39-40. This is not the case.

Nair is built around the assumption that a single encryption scheme and public key/private key pair will be used. *See* Ex-2005 at ¶¶ 100, 107-108, 111. As discussed in the preceding section, the privacy indicator signals that encryption has been applied to the IMSI so that the HSS or SLF saves processing time by treating the contents accordingly. Ex-1004 at ¶ 43. But combining a public key identifier with the privacy indicator makes little sense, because it would include wasteful data in the attach message. As Dr. Mahon explains, if a public key was identified, it would already indicate that encryption had been applied, rendering Nair’s privacy indicator superfluous. Ex-2005 at ¶ 112. A POSITA would not be inclined to include

duplicative information in a telecommunications request. *Id.* But Petitioner does not address this problem. Instead, their argument relies on the conclusion that a combination of Nair and Forsberg would include both an identifier for the public key, as well as an “on” or “off” flag that they contend is an “encryption scheme identifier.” Pet. at 33, 34-35.

As discussed above, during the ITC investigation, Staff also agreed that a Lenovo had not provided a basis for combining both Forsberg’s “public key identifier” and Nair’s “privacy indicator” into the same telecommunication system. *See* Ex-2008 at page 8. Accordingly, the Board should find that Claim 1 is valid.

3. Claim 2

Claim 2 depends from claim 1 and is valid for the same reasons enumerated above.

Further, Nair does not disclose a method in which “the determining of the de-concealing server is based on information received from the UE.” Petitioner contends that Nair’s disclosure that “[a] given alternative embodiment may of course include larger numbers of such system elements” as the SLF teaches the limitations of the present claim, but this is wrong. Pet. at 45, Ex-1004 at ¶ 57.

First, as Dr. Mahon explains in his declaration, Petitioners’ expert, Dr. Bims, has misunderstood the Nair reference, and argues that the SLF (which he alleges is a “de-concealing server”) is selected based on information sent from the UE. Ex-

2005 at ¶ 114-115. In actuality, it is the SLF that selects an HSS (which is not a de-concealing server) based on the MCC and MNC sent in an authentication request by a UE. *Id.*

Further, the '817 Patent teaches the use of multiple de-concealing servers so that different servers can handle different encryption schemes. *See* Ex-1001 at 10:55-59. Nair's SLF only ever handles a single method for encryption, and Nair's privacy indicator only ever indicates whether encryption was used—not the type of encryption. As such, Nair's multiple SLFs simply serve a load balancing purpose, allowing the work of decrypting many incoming requests to be distributed across multiple machines. *See, e.g.,* Ex-1004 at ¶ 38. This distribution is not, however, based on information sent from the UE. In Nair's architecture, a message from a UE can be handled just as well by one SLF as another. Accordingly, Nair does not teach "the determining of the de-concealing server is based on information received from the UE."

Forsberg also does not cure this deficit. A POSITA would not be motivated to combine Forsberg with Nair for the reasons described above. *See* Ex-2005 at ¶¶ 89-93, 116. Further, Petitioner points only to Forsberg's disclosure of using the MCC or MNC to route messages to the appropriate home network. *Pet.* at 46. This is not the same as using information from a UE to route the message to a particular de-concealing server, which is a specific node in a network. Ex-2005 at ¶ 116.

4. Claim 3

Claim 3 depends from claim 1 and is valid for the reasons described above.

5. Claim 4

Claim 4 depends from claim 1 and is valid for the reasons described above.

6. Claim 5

Claim 5 depends from claim 1 and is valid for the reasons described above.

7. Claim 6

Claim 6 depends from claim 1 and is valid for the reasons described above.

8. Claim 8

Claim 8 depends from claim 1 and is valid for the reasons described above.

Nair does not disclose an “Elliptic Curve Integrated Encryption Scheme (ECIES)” anywhere, and so Petitioner relies on Nair’s alleged incorporation by reference of 3GPP TR 33.899 v1.1.0 (Release 14). Pet. at 51. But the Federal Circuit has held that “[t]o incorporate matter by reference, a host document must contain language ‘clearly identifying the subject matter which is incorporated and where it is to be found’; a ‘mere reference to another application, or patent, or publication is not an incorporation of anything therein....’” *Callaway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1346 (Fed. Cir. 2009) (citing *In re De Seversky*, 474 F.2d 671, 674 (C.C.P.A. 1973)). Nair only includes a bare reference to TR 33.899 and Petitioner fails to

identify a basis for the incorporation of ECIES as disclosed therein. Ex-2005 at ¶¶ 120-121; *see also* Ex-2010 at 1322:9-24.

9. Independent Claim 9

Petitioner relies on no new arguments with respect to claim 9, instead referring to its arguments on claim 1. Claim 9 is valid for the same reasons enumerated for claim 1 above.

10. Independent Claim 10

Petitioner also relies on no new arguments with respect to claim 10, instead referring to its arguments on claim 1. Claim 10 is valid for the same reasons enumerated for claim 1 above.

11. Claim 11

Claim 11 depends from claim 10 and is valid for the reasons described above.

12. Claim 12

Claim 12 depends from claim 10 and is valid for the reasons described above. Further, Petitioner cannot point to any disclosure by Nair or Forsberg that a “tamper resistant secure hardware component of the UE” is used to generate the SUCI, and again relies on TR 33.899’s incorporation by reference into Nair. Pet. at 55. As before, Petitioner also does not point to disclosure in Nair “clearly identifying the subject matter which is incorporated and where it is to be found,” instead relying on

portions of the document which are never mentioned in the specification of Nair. *Callaway Golf Co*, 576 F.3d at 1346; *see also* Ex-2005 at ¶ 125.

13. Claim 13

Claim 13 depends from claim 10 and is valid for the reasons described above.

14. Claim 14

Petitioner relies on no new arguments with respect to claim 14, instead referring to its arguments on claim 8. Claim 14 is valid for the same reasons enumerated for claim 8 above.

15. Independent Claim 15

Petitioner relies on no new arguments with respect to claim 15, instead referring to its arguments on claim 1. Claim 15 is valid for the same reasons enumerated for claim 1 above.

16. Claim 16

Claim 16 depends from claim 15 and is valid for the reasons described above.

B. Ground 2 – Nair, Forsberg, and Togawa

1. A POSITA would not be motivated to combine Nair, Forsberg, and Togawa.

Petitioner's arguments for motivation to combine Togawa with the Ground 1 references Nair and Forsberg are threadbare, offering little justification for the modifications they propose. *See* Pet. at 59-63. Petitioner's first reason is not really a reason, only a statement that a POSITA would have been motivated to use Togawa

and Nair occupy the same general field of technology. *See id.* at 59-60. The second similarly argues only that both references contemplate sending information about if or alternately how something is encrypted. *See id.* at 60. Petitioner's fourth reason also does little more than restate the benefit that Nair says can be derived from its privacy indicator. *See id.* 61. Petitioner does not explain how this benefit is related to Togawa or why it would motivate a POSITA to want to replace the privacy indicator with another variable. *Id.*

Petitioner's third argument alone lays out their substantive reasoning: Togawa can "identify more than one type of encryption scheme, something Nair cannot. *See id.* at 60-61. A POSITA would look to correct this clear deficit in Nair by replacing its "on" or "off" privacy indicator with a larger variable that is able to identify multiple types of schemes used to encrypt a message instead. But, as the Board observed, there is nothing in Nair that discloses support for multiple encryption schemes. *See* Decision at 33. To the contrary, Nair never discloses that multiple encryption schemes could be used and relies on the opposite being true. *See* Ex-2005 at ¶¶ 100, 131.

Nair's "privacy indicator" is a flag that only represents whether or not encryption was used, not the type of encryption. Ex-1004 at ¶ 16. Nair's operation relies on this fact. Nair even discloses that its privacy indicator could be omitted because the HSS or SLF can attempt to solve the request and determine that it is

encrypted “after the first attempt” to do so fails. *Id.* at ¶ 43 (explaining that the utility of the privacy indicator is skipping this initial attempt). Petitioner has not pointed to anything in Nair that indicates that the privacy indicator would be improved by including additional information about the encryption scheme used.

In fact, as Dr. Mahon explains, if multiple encryption schemes were permitted in Nair, then the HSS or SLF would not be able to differentiate between a failure to decrypt a received IMSI because it used the wrong encryption algorithm, and an erroneous transmission by the UE. *See* Ex-2005 at ¶ 132. Accordingly, a POSITA would not look to Togawa’s disclosure of switching keys and encryption schemes to improve Petitioner’s first Ground because their approaches to security are incompatible. *See id.* at 130-132.

Further still, Togawa is directed to an entirely different technology than either Nair or Forsberg. While Nair and Forsberg relate to the authentication of a UE in an LTE or 5G network, Togawa is directed to the encryption of user data transmitted over a voice signal during a voice call. *See* Ex-1004 at ¶¶ 26, 36; Ex-1005 at ¶¶ 43-45; Ex-1006 at 4:38-65. Because Togawa’s data transmitting apparatus establishes an encryption key at the start of a voice call and periodically thereafter as the key changes, there is never a need for an encryption scheme, or even a privacy indicator, to be included with encrypted user data. *See* Ex-2005 at ¶¶ 84-86. A POSITA would not look to apply a technique for transferring data through a voice call to a system

for securing communication between a UE and the core network and would not have a reasonable expectation of success in doing so.

Accordingly, a POSITA would not look to Togawa to improve Nair or Forsberg by including an “encryption scheme identifier” as claimed in the ’817 Patent. Petitioner’s Ground 2 should be rejected.

2. Independent Claim 1

Petitioner’s only new argument with respect to claim 1 is that Togawa’s “encryption-method ID,” once substituted for Nair’s “privacy indicator,” would satisfy the “encryption scheme identifier” limitations of the ’817 Patent. Pet. at 63-65. This is wrong because a POSITA would not make such a substitution for the reasons discussed in the preceding section.

Petitioner contends that a POSITA would be motivated to alter Nair and Forsberg to use the “encryption method ID” disclosed in Togawa. Pet. at 62. According to Petitioner, Togawa’s disclosure that multiple encryption schemes could be specified for encrypting user data over a voice signal would be a natural substitute for Nair’s privacy indicator. *Id.* at 60. This is wrong for the reasons discussed above. Nair is not configured to accommodate multiple encryption schemes, and a POSITA would have no expectation of success in combining them. *See* Ex-2005 at ¶¶ 131-134.

3. Independent Claims 9, 10, and 15

Petitioner addresses independent claims 9, 10, and 15 collectively, referring back to prior argument with respect to claim 1 and making no new arguments with respect to claims 9, 10, and 15. Claims 9, 10, and 15 are valid for the same reasons enumerated for claim 1 above.

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

Petitioner also addresses dependent claims 2-6, 8, 11-14, and 16-17 collectively to refer back to prior argument made for the same dependent claims in Ground 1. Pet. at 65-66. Petitioner offers no arguments relying on Togawa for these claims. *Id.* Accordingly, the enumerated dependent claims are valid for the same reasons explained above with respect to Ground 1.

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

1. 5G-Ensure teaches away from using an “Elliptic Curve Integrated Encryption Scheme (ECIES).”

Petitioner’s Grounds 3 and 4 combine their prior Grounds with 5G-Ensure, which Petitioner argues renders challenged claims 8 and 14 obvious. Pet. at 66. Petitioner offers no arguments on any other claims for these Grounds.

Claims 8 and 14 depend from claims 1 and 10 respectively, and add the limitation that the encryption scheme used be an “Elliptic Curve Integrated Encryption Scheme (ECIES).” Ex-1001 at 21:48-49, 22:50-51. Petitioner resorts to

piling yet another reference on top of these grounds because none of Nair, Forsberg, or Togawa ever mentions an “Elliptic Curve Integrated Encryption Scheme (ECIES).” 5G-Ensure does not ever reference ECIES either. The word “elliptic” appears only once in 5G-Ensure, and Petitioner points to this occurrence (in conjunction with papers establishing the existence of ECIES) to carry the burden of Grounds 3 and 4. Ex-1010 at 33; Pet. at 66-67. But Petitioner’s argument is flawed—5G-Ensure teaches away from using ECIES.

Petitioner points to the language in 5G-Ensure that states “[t]he 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.” Pet. at 66-67. As discussed in the reference’s prior paragraph, 5G-Ensure is suggesting that an attribute-based encryption (“ABE”) scheme could be used “instead of traditional public key encryption.” Ex-1010 at 32. As Dr. Mahon explains, ABE schemes are a class of encryption scheme that differ from public key encryption because they allow multiple different private keys to decrypt data encrypted with the same public key depending on attributes built into the private keys when they are computed. *See id.*; Ex-2005 at ¶¶ 137-138. In public key encryption, by contrast, each public key corresponds to just one private key that is capable of decrypting its ciphertext. Ex-2005 at ¶ 139. ABE schemes are used to provide fine-grained access control, which

is not possible with traditional public key encryption. Accordingly, ABE schemes and traditional public key encryption schemes are mutually exclusive. *Id.* The problem with Petitioner’s argument is that ECIES is a traditional public key encryption scheme. *Id.* at ¶ 140; *see also* Ex-1011 at 2 (“Elliptic curve cryptographic schemes are public-key mechanisms”).

As Dr. Mahon explains, ECIES is a symmetric encryption scheme built around the mathematics of elliptic curves, which provide the computationally intractable problem necessary for most cryptographic algorithms. Ex-2005 at ¶ 140. When using ECIES, a single public key is used to encrypt data, which can then be decrypted by a single private key. *See id.* In other words, it is a traditional public key encryption scheme. *Id.* Although 5G-Ensure mentions “ABE schemes based on elliptic curve pairings,” it is only referring to ABE schemes built around the same mathematical principle as of elliptic curves, not ECIES. Ex-2005 at ¶ 141. ECIES can never serve as a substitute for an ABE scheme, even one based on elliptic curve principles—it lacks support for the attribute-based access policies that define an ABE scheme. Accordingly, the Board should find that 5G-Ensure does not teach the use of ECIES and actually suggests that ECIES and other traditional public key encryption schemes should not be used for encrypting the IMSI.

D. Secondary Considerations

In addition to the foregoing reasons, secondary considerations support the non-obviousness of the challenged claims of the '817 Patent. The inventions of the '817 Patent addressed a long-felt need in the field of telecommunications and were the subject of industry praise and commercial success.

Industry praise. The technologies claimed in the '817 Patent have been the subject of praise. For example, the paper “Security in 5G Networks – How 5G Networks Help Mitigation Location Tracking Vulnerability” explores a pre-5G vulnerability where an “IMSI catcher” could be used to track a user’s device based on the unencrypted IMSI. *See* Ex-2002 at 3. This problem is solved by the security techniques claimed in the '817 Patent, which further give network operators latitude to select an encryption scheme that suits their needs. *See id.* at 4. Additionally, the technologies disclosed in the '817 Patent would eventually be incorporated into the 3GPP’s 5G standard. Ex-2005 at ¶ 59. Standardization is high praise within the telecommunications field, as standard-setting organizations like the 3GPP aim to select only the best solutions to problems from many competing submissions by industry participants. *Id.* Investigative Staff in the ITC proceeding also agreed that the '817 Patent was the subject of industry praise. Ex-2008 at 11.

Long-felt need. The same paper also discusses how privacy risks associated with sending an IMSI as plaintext were known for some time prior to the '817 Patent

and its incorporation into 5G. *See* Ex-2002 at 3. Despite multiple incidents in which IMSI catchers were used to compromise privacy, only weak solutions that still left the subscriber's identity vulnerable, such as temporary subscription identifiers, had been implemented. *See id.*; Ex-1001 at 1:22-36. The inventors of the '817 Patent recognized this need and proposed a solution that completely addressed these problems.

Commercial Success. Finally, the commercial success of the '817 Patent's inventions is evident. 5G networks have been broadly deployed, and telecommunications companies continue to expand their coverage every day. Ex-2005 at ¶ 59. The continued success of 5G—while driven by numerous contributions to the standard—is due in part to the improved security which the standard provides and which the inventions of the '817 Patent helped to enable.

V. Conclusion

For the foregoing reasons, Patent Owner respectfully requests that the Board reject Petitioner's arguments and uphold the challenged claims of the '817 Patent as valid.

Dated: December 6, 2024

Respectfully submitted,

/s/Scott W. Hejny

Scott W. Hejny

Reg. No. 65,320

shejny@mckoolsmith.com

Christian J. Hurt

Reg. No. 63,659

churt@mckoolsmith.com

Joseph W. Micheli

Reg. No. 81,245

jmicheli@mckoolsmith.com

McKool Smith, P.C.

300 Crescent Court, Suite 1500

Dallas, Texas 75201

Telephone: (214) 978-4000

Facsimile: (214) 978-4044

Counsel for Patent Owner,
Telefonaktiebolaget LM Ericsson

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER'S RESPONSE** specified in 37 C.F.R. § 42.24 have 7,890 words, in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24(b)(1).

This word count was prepared using Microsoft Word 2016.

Respectfully submitted,

Date: December 6, 2024

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

CERTIFICATION OF SERVICE

The undersigned hereby certifies that a copy of this **PATENT OWNER'S RESPONSE** is being served electronically via e-mail on December 6, 2024, in its entirety, on the following counsel for Petitioner:

Robert A. Appley
rappleby@kirkland.com

W. Todd Baker
todd.baker@kirkland.com

John R. Rhine
john.rhine@kirkland.com

Lenovo_PTAB@kirkland.com

Dated: December 6, 2024

Respectfully submitted,

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