

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.
Petitioner

v.

TELEFONAKTIEBOLAGET LM ERICSSON,
Patent Owner

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

Case IPR2024-00702

**DECLARATION OF HARRY BIMS, Ph.D.
IN SUPPORT OF PETITIONER'S REPLY TO PATENT OWNER'S
RESPONSE**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND AND QUALIFICATIONS	2
III.	PERSON OF ORDINARY SKILL IN THE ART AND THE TIME OF THE ALLEGED INVENTION	2
IV.	CLAIM CONSTRUCTION	2
A.	“encryption scheme identifier”	3
V.	Motivation to Combine Nair and Forsberg	9
VI.	Motivation to Combine Nair, Forsberg, and Togawa	17
VII.	Grounds 2-3	26
VIII.	Secondary Considerations	27
A.	Commercial Success.....	27
B.	Industry Praise	29
C.	Long-Felt but Unsolved Need	29
D.	Simultaneous Invention.....	30

IX. CONCLUSION.....	30
---------------------	----

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

I. INTRODUCTION

1. I have been retained by Lenovo (United States) Inc. (“Lenovo” or “Petitioner”) as an independent expert consultant in this proceeding before the United States Patent and Trademark Office (“PTO”) against Telefonaktiebolaget LM Ericsson, (“Patent Owner”) regarding U.S. Patent No. 10,425,817 (“the ’817 patent”) (Ex. 1001).¹

2. I previously submitted a Declaration in support of this IPR on March 15, 2024, which I incorporate herein in its entirety. Ex. 1002. I apply the same viewpoint of a POSITA as expressed therein. In forming my opinions expressed in this declaration, I reviewed the materials listed in paragraph 17 of my opening declaration. Ex. 1002, ¶ 17. I also reviewed any other materials I refer to in this declaration in support of my opinions.

3. I am being compensated at a rate of \$750/hour for my work in this proceeding. My compensation is in no way contingent on the nature of my findings,

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

the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding.

II. BACKGROUND AND QUALIFICATIONS

4. My background and qualifications are set forth in my March 15, 2024 Declaration, which is incorporated herein by reference. Ex. 1002

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

5. See Section IV of Ex. 1002.

IV. CLAIM CONSTRUCTION

6. I understand that claim terms are typically given their ordinary and customary meanings, as would have been understood by a person of ordinary skill in the art at the time of the alleged invention, which as I explained above, I have been asked to assume is around July 25, 2017. In considering the meaning of the claims, however, I understand that one must consider the language of the claims, the specification, and the prosecution history of record.

7. I have been informed that claim terms are customarily given their ordinary and customary meaning as understood by a POSITA and that the claims must be interpreted in the context of the entire patent. I understand that the claims, specification, and file history (along with their incorporated and cited references, as well as filings and evidence included in *inter partes* review (IPR) proceedings) are

considered intrinsic evidence that are of primary importance in determining the meanings of the claim terms.

8. I understand that a claim term, however, will not receive its ordinary meaning if the patentee acted as his own lexicographer and set forth a definition of a disputed claim term in either the specification or during prosecution.

9. I understand that if the meaning of a term is clear from the claim language and the intrinsic evidence, the claim construction stops there. However, if the meaning of the claims cannot be determined after assessing the intrinsic evidence, then I have been informed that extrinsic evidence such as publications, dictionaries, and textbooks may be considered. I understand that whether or not extrinsic evidence is considered, the claim construction cannot be inconsistent with the intrinsic evidence.

10. I have been asked to consider the claim terms under their plain meanings and thus I have considered the claims, specification and prosecution history for the '817 patent in doing so in support of my opinions concerning the '817 patent and the prior art discussed herein. (Ex. 1001; Ex. 1004.)

A. “encryption scheme identifier”

11. I understand Patent Owner proposed that “the limitation ‘encryption scheme identifier’ is [not] satisfied by a flag indicating whether encryption is on or

off . . . because an ‘encryption scheme identifier’ must be capable of identifying at least two possible encryption schemes.” Paper 14 at 14-17. Patent owner also said 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.” Paper 14 at 17. As discussed below, I disagree.

12. I have also reviewed Dr. Mahon’s testimony (Ex. 2005 ¶¶ 54-57) and I disagree with his conclusions, as discussed below.

13. In my opinion, Dr. Mahon’s interpretation of “encryption scheme identifier” is contrary to the plain meaning. Throughout the specification, the “encryption scheme identifier” is described as an identifier that “identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI.” Ex. 1001 at Abstract, 1:56-59, 2:4-5, 3:54-56, 19:55-58, 20:24-26.

14. In my opinion, a POSITA would understand that the plain meaning of “encryption scheme identifier” read in the light of the specification is “an identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI.” I am not aware of anything in the claims, specification, or other intrinsic or extrinsic record that suggests otherwise.

15. As I explained in paragraph 28 of my opening declaration, the '817 patent describes an example of an encryption scheme being the “null-scheme,” which actually performs no encryption. *See* Ex. 1001, 3:27-28 (“[T]he encryption scheme may be a null-encryption scheme”), 9:11-12 (“[T]he encrypted part of the SUCI may use a null encryption scheme....”), 15:9-11 (“The null-scheme is implemented such that it returns the same output as the input....”). Though it may seem counterintuitive that a scheme that performs no encryption could be an “encryption scheme,” the '817 Patent expressly states that the “encrypted part” of the SUCI may be generated using the null-encryption scheme. *See id.*, 9:11-13 (“[T]he encrypted part of the SUCI may use a null encryption scheme, *e.g.*, if the UE 1 has not been provisioned with the public key of the home network.”), 15:7-9 (“Because the UE initially has no privacy key in this scenario, the UE uses a null-scheme or null-encryption method to create the SUCI.”).

16. As I explained in paragraph 27 of my opening declaration, the specification provides only one other specific non-null example of encryption schemes that is indicated by an encryption scheme indicator: ECIES. This is shown in Figs. 4 and 5, for example. Ex. 1001 at Figs. 4 and 5. While the '817 patent also mentions RSA encryption in another embodiment, it never shows an encryption scheme identifier with that express option. If multiple non-null schemes were

fundamental to an encryption scheme identifier, I would expect that RSA or some other specific examples would be shown in Fig. 4. Yet, there are only two specific examples of encryption schemes are that is indicated by an encryption scheme identifier are null-scheme and ECIES. All of the examples of encryption scheme identifiers in the patent would have been understood to a POSITA to be exemplary and non-limiting. It is therefore not my opinion that the '817 patent intends to exclude RSA or any other scheme. But a POSITA would also understand that the number of schemes is not limiting and could be as few as one.

17. Read in light of the specification, an indicator that identifies between null encryption (off) and encryption (on) qualifies as an example of an encryption scheme identifier in the context of the '817 Patent. The example encryption scheme identifier in Figure 4 (below) is such an example. When the encryption scheme indicator is "0" or "off," both the UE and deconcealing server in the '817 patent have a shared understanding that "null-scheme" encryption is used. Ex. 1001 at Fig. 4. And when it is "1" or "On", ECIES is used based on the shared understanding that "1" means ECIES encryption. *Id.* The "etc." in Figure 4 suggests that more schemes could be used, but a POSITA would not understand that they are required. As I said, there is no second non-null example show in Fig. 4 or any other embodiment.

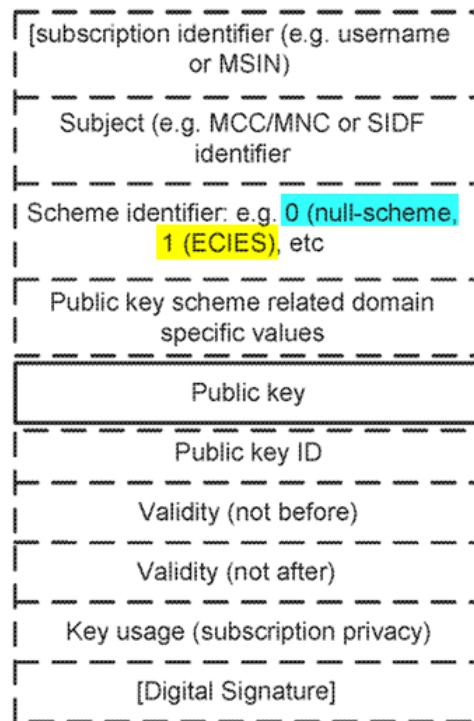


Fig. 4

18. Based on my review, in my opinion, the '817 patent never states or suggests that an encryption scheme identifier must be able to indicate two non-null encryption schemes. All that is required is that the indicator identifies the scheme used to encrypt the SUCI. There is no embodiment with two specific examples of non-null schemes.

19. In paragraphs 55 through 56 of his declaration (Ex. 2005), Dr. Mahon lists examples of encryption scheme identifiers, “4-bit identifier,” “integer,” “numeric string,” “alphanumeric string,” and “bit string.” A POSTA would

understand these are non-limiting examples. Looking at these disclosures in context is instructive:

FIG. 5 illustrates an *example* 3GPK scheme. 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. The identifier *may be* e.g. a 4-bit identifier. *Other embodiments may format the scheme identifier in other ways*, including *but not limited to* one or more integers, numeric strings, alphanumeric strings, bit strings, *and/or other data types*.

Ex. 1001 at 10:17-24. I note that the '817 patent also says that the “embodiments described herein are to be considered in all respects as illustrative and not restrictive.” Ex. 1001 at 20:56-58. For these reasons, a POSITA would understand that all the examples listed by Dr. Mahon are illustrative and non-limiting.

20. I also note that Dr. Mahon left out examples that do not suit his opinion. For example, the specification explains the “scheme identifier” may be “one [] integer” such as “0” or “1” or “other data types.” Ex. 1001 at 10:17-24. A POSITA would understand that a “flag” or “Boolean” is such an “other data type.”

21. As another example, specification teaching “[e]ach scheme adopted as standard may be assigned a specific **identifier**” could be a few as one scheme because a POSITA would have understood a future standard may ultimately only

adopt one non-null scheme. Nothing in the '817 patent suggests the number of adopted schemes must be larger than 1 to fit within the scope of its invention.

V. Motivation to Combine Nair and Forsberg

22. As I explained in my opening declaration, in my opinion, a POSITA would have been motivated to combine the teachings of Nair and Forsberg to arrive at the claimed invention of claims 1-6 and 8-16. Ex. 1002, Section VIII.A.

23. A POSITA would have been motivated to use Forsberg's public key identifiers to reduce the complexities of managing multiple public and private key pairs to allow the use of multiple Home Subscription Servers within a communications network, as described in Nair. Indeed, Nair teaches the benefits of using multiple keys to map to multiple HSS allows an operator to manage different groups of users in different HSSs/UDMs. Ex. 1004, ¶[0036] ("An operator in his network may have implementations of multiple HSSs which allows him to manage distinct sets of users in different HSSs/UDMs. Because of the multiple HSSs, a Server Location Function (SLF) may be implemented in front of a set of HSSs. ... The SLF analyzes the authentication request for a user received from the MME/AMF and routes it to the correct HSS."); Ex. 1008, 5:7-10. In my opinion, Nair's teachings would lead a POSITA to seek Forsberg for its teachings of an identifier to support this use of multiple keys in the encryption process for these reasons.

24. Dr. Mahon disputes a POSITA would be motivated to combine Nair and Forsberg “because Nair does not teach managing multiple public and private key pairs.” Ex. 2005, ¶¶ 89-93. Dr. Mahon disagrees because “Nair is still only describing one public/private key pair for the network, the private key has simply been moved to the SLF.” *Id.* ¶ 92. Implicit in Dr. Mahon’s opinion are two incorrect assumptions: first, that there is only one SLF in Nair, and second, that each SLF only has one key. I disagree with both.

25. As I explained in my opening declaration, Nair explicitly discloses multiple SLFs because Nair explains that there “may of course” be an alternative embodiment that includes large numbers of system elements, such as SLF elements. Ex. 1004, ¶[0057] (“[A]lthough only single UE, eNB/gNB, MME/AMF, ***SLF***, SGW/SMF and PGW elements are shown in the FIG. 1 embodiment, this is for simplicity and clarity of description only. A given alternative embodiment may of ***course include larger numbers of such system elements***, as well as additional or alternative elements of a type commonly associated with conventional system implementations.”); Ex. 1008, 10:14-20. This is unsurprising, as 5G networks would have known to include multiple SLFs since each operator must have at least one and likely very many.

26. A POSITA would understand that each SLF would at least have one key, and nothing in Nair suggests all SLFs across various operators would share the same key.

27. Additionally, Dr. Mahon's assumption that each SLF only uses a single key pair is unsupported by Nair's disclosures. Nair tells a POSITA that each HSS is understood to be its own home network. Ex. [0054] ("These HSSs/UDMs represent the home networks of UEs"), Fig. 1. Accordingly, when Nair says "the network private key" for "an HSS" (Ex. 1004, [0038]), a POSITA would understand Nair is referring to the key associated with the HSS. And since there are multiple HSS, the SLF would need to have a key for each. Thus, Nair teaches that the SLF has a key pair for each of the multiple HSSs.

28. Additionally, as I explained in my opening declaration, a POSITA would have been motivated to consult and apply Forsberg because Forsberg teaches key identifiers to manage multiple keys used in encryption. Ex. 1005, ¶¶[0055] ("[A] valid public key and secret key pair along with a key identifier may be sent in message 4 to the requesting mobile management entity. The public key and secret key pairs are identified so that the correct secret key can be used to decrypt the IMSI. In this option *the user equipment provides public key identifier* along with the encrypted IMSI (e.g. similar to the key set identifier, KSI)."), [0049] ("Other

information, such as information about public key identifiers may also be included in the response.”), [0056] (“[T]he public key and secret key pairs are provided with an identifier [and] [t]he user equipment may then send the identifier with the encrypted IMSI to the visited mobile management entity, and the decryption can be accomplished on these basis [*sic*].”), [0058] (“A validly authenticated network can then update the user equipment with a valid new public key, *key identifier* and other information with a validity period.”); *see also* Figs. 4 & 5 (depicting the transmission of a user identity response comprising encrypted IMSI and a public key identifier (PK-Id)). Thus, Forsberg discloses a SUCI comprising an encrypted subscription identifier (*i.e.*, encrypted MSIN) and a clear-text home identifier (*i.e.*, MCC+MNC) and public-key identifier. Due to the express teachings of Forsberg, a POSITA would have understood the benefits of applying public key identifiers to manage the implementation of multiple keys. I do not see Dr. Mahon dispute these opinions in his testimony. Ex. 2005. My opinion would not change even if Nair did not disclose multiple key pairs.

29. A POSITA would have understood that home networks that use multiple public/private key pairs enhance security because, even if one private key is compromised, messages encrypted using other keys will remain protected. A POSITA would have found it obvious to use the secure process disclosed in Nair to

authenticate UE's with home networks utilizing multiple public/private key pairs, such as those disclosed in Forsberg, to further enhance the privacy of a UE's subscription identifier.

30. Thus, in my opinion, a POSITA would have been motivated to implement key management techniques such as the use of public key identifiers as taught by Forsberg to support this use of multiple keys and multiple private and public key pairs in the encryption process, as taught by Nair. But my opinion would not change even if Nair did not disclose multiple key pairs.

31. For the same reasons discussed in my opening declaration, Nair provides teaching, suggestion, and motivation that would have led a POSITA to combine its teachings with Forsberg to arrive at the combined Nair-Forsberg system. Ex. 1002 ¶¶ 45-55.

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

1005, ¶[0047]. This is because the decrypted IMSI (*i.e.*, SUPI) contains the permanent subscriber identity for the UE, which allows the authentication server to identify the UE and determine whether the UE should be granted access. A POSITA would be motivated to apply that benefit to Nair's system. The combination represents combining prior art elements (Nair's authentication method and system with Forsberg's method of transfer the decrypted identifier back to the authentication server) according to known methods to yield predictable results (authenticating a visiting UE).

33. Additionally, a POSITA would have understood that Forsberg's public key identifier could be used to improve a similar system (the combined Nair-Forsberg system) in a similar way (improved public and private key pair management) based on complimentary and overlapping disclosures in Nair and Forsberg and for the reasons stated above. Likewise, a POSITA would view Nair to be ready for improvement with respect to particular implementations requiring distributed subscriber management across multiple HSSs, and that Forsberg's public key identifiers would provide that improvement in predictable ways. *Id.* And, a POSITA would have been prompted to try variations of Forsberg in the same field of endeavor—such as by applying it to Nair—based on design incentives (improved subscriber authentication management during the registration process).

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

35. Dr. Mahon also opines that the public key identifier is superfluous in the Nair-Forsberg combination because Nair only has a "(single) private key" that is already indicated by the privacy indicator. (Ex. 2005, ¶ 112) I disagree that Nair only has one key pair. As discussed above, Nair teaches multiple key pairs.

36. But even if Nair only had one key pair, I would disagree with Dr. Mahon. As I explained above, a POSITA would have been motivated to implement multiple key pairs (as disclosed by Forsberg) in Nair's system due to the benefits described by Forsberg, such as enhanced security and protection in the case that one or more keys was compromised. Accordingly, even if Nair did not teach multiple

keys, a POSITA would be motivated to add them based on the teachings for Forsberg.

37. I note that in its Patent Owner Response, Ericsson argues that Forsberg's public key identifier "render[s] Nair's privacy indicator superfluous" and cites Dr. Mahon's paragraph 112. Patent Owner is not accurately characterizing Dr. Mahon's testimony. Ex. 2005, ¶ 112. Dr. Mahon opined that Nair's privacy indicator rendered the key indicator superfluous, not the other way around. Ex. 2005, ¶ 112. This is clear because Dr. Mahon says "privacy indicator alone is enough" and then says "Dr. Bims is suggesting adding additional data to the message that is effectively duplicative." *Id.* The additional data he is referring to is Forsberg's public key indicator. It is unclear to me why Patent Owner inverted Dr. Mahon's opinion.

38. I also disagree with Patent Owner's argument that Forsberg's public key identifier "render[s] Nair's privacy indicator superfluous." Forsberg's public key indicator doesn't have an option to indicate null encryption because it is not intended to indicate null encryption. Accordingly, a privacy indicator is still required. Hypothetically, the public key indicator could be modified so that certain values indicated null-encryption, but that result would be both an encryption scheme identifier and a public key identifier because it would include values that indicate encryption schemes, satisfying both limitations.

39. Regardless, eliminating Nair's privacy indicator would only save a single bit. Such a small increase in efficiency would not motivate a POSITA to omit the privacy indicator even if it could be done. Dr. Mahon does not even contend it would. Ex. 2005, ¶ 112.

VI. Motivation to Combine Nair, Forsberg, and Togawa

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

41. A POSITA would have been motivated to use Togawa's encryption scheme identifier in place of Nair's privacy indicator for several reasons. The combination of Nair, Forsberg, and Togawa represents the use of known techniques to improve similar devices in the same way. Nair and Togawa relate to the same field of privacy-protection scheme identification. Ex. 1004, ¶[0010] ("The message may comprise an attach request comprising a subscription identifier for a subscriber of the communication network associated with the user equipment, the one or more privacy indicators comprising a flag indicating whether the subscription identifier in the attach request is privacy-protected."), *with* Ex. 1006, 10:31-39 ("[T]he

encryption-specification embedding unit 10f of the data transmitting apparatus 10 embeds an encryption key in a Voice signal. However, in place of the encryption key, information on an identifier for identifying the encryption key, information obtained by converting the encryption key by a predetermined method, information obtained by converting the identifier of the encryption key by a predetermined method, or like information can be embedded.”).

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

43. A POSITA would have been motivated to improve Nair's privacy indicator with Togawa. For example, Togawa represents a known improvement to an encryption identifier by its ability to identify more than one type of non-null encryption scheme, which may easily be integrated with the authentication method of Nair with a reasonable expectation of success. In other words, the Nair-Forsberg-Togawa combination represents the simple substitution of one known element of Nair's privacy indicator for another (Togawa's encryption scheme identifier) to achieve a predictable result with a reasonable expectation of success. *Id.*

44. Nair teaches the benefits—saving time and reducing required resources—of using privacy indicators to assist the de-concealing server in determining information about the encryption process used within the data transmission. Ex. 1004, ¶[0043] (“[O]ne key reason to have such an indication specified is that *this saves processing time and fewer resources are needed*. Thus, in this first illustrative embodiment, *the SLF can make the decision on the processing by looking at this flag*.”). Ex. 1008, 6:21-23. The inclusion of a privacy indicator (*e.g.*, encryption scheme identifier) allows a de-concealing server to begin the decryption process immediately using the decryption method indicated by the identifier. This technique frees the de-concealing server from first having to figure

out which decryption scheme was used to encrypt the message and which decryption technique to apply to decrypt the message.

45. In my opinion, a POSITA reading Nair would have understood the time and resource-saving benefits of providing encryption technique identification to a de-concealing server rather than wasting server resources deciphering the encryption technique manually. A POSITA would have been motivated to consult and apply Togawa for its teachings of an encryption scheme identifier to take advantage of the faster processing time and resource-reducing benefits that Togawa provides and that Nair extols the benefits of.

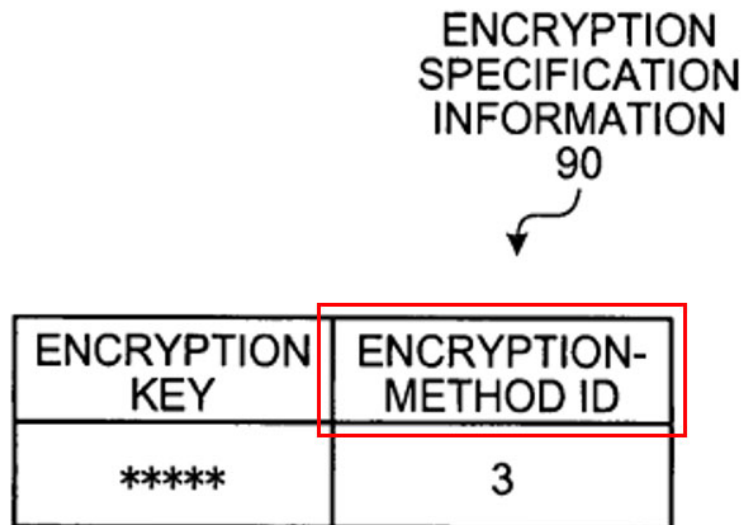
46. In my opinion, a POSITA reading Nair would have been motivated to seek and apply additional techniques for flagging encryption schemes to a de-concealing server, such as the use of an encryption method ID (*i.e.*, encryption scheme identifier) as taught by Togawa and depicted in Fig. 13, to leverage the benefits taught by Nair.

47. I understand Dr. Mahon disagrees because Nair only allegedly discloses one encryption scheme. Ex. 2005, ¶¶ 131-32. I note that Nair clearly teaches two schemes, the null-scheme and the public/private key scheme, as I discussed in my opening declaration. As I explained at the ITC, Nair doesn't expressly disclose which public/private key scheme it uses. But that is because a POSTA would

understand that a number of suitable schemes could be used. Although Nair doesn't expressly disclose to the *reader* of Nair which scheme is used, the SLF in Nair would have obviously have to know which scheme is indicated, for the reasons discussed in my opening report. And as discussed in my opening report in the context of claim 8, Nair through TR 33.899 discloses ECIES as an option.

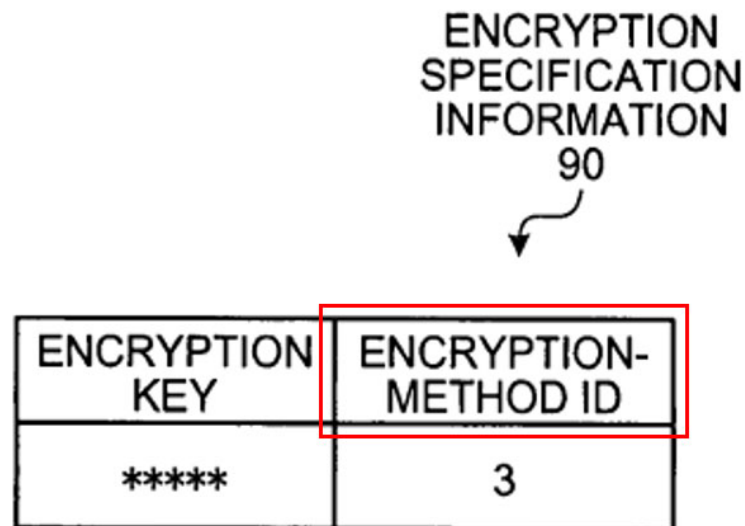
48. Regardless, my opinions do not rely on Nair disclosing multiple non-null schemes. In my opinion, Togawa's recognition of the benefits of multiple non-null encryption schemes stands independently and does not rely on Nair's teachings.

49. Indeed, upon consultation with Togawa, a POSITA would have understood the benefits of applying an encryption method ID as taught by Togawa to manage the implementation of multiple non-null encryption methods.



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

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



Id., Fig. 13 (annotated). Togawa’s “encryption specification information 90” specifies which of a plurality of encryption methods was used. *Id.*, 23:1-4 (noting the encryption method changes over time), 23:17-39. In other words, Togawa’s

encryption method ID thus specifies which of a plurality of encryption methods was used and allows for the flexibility of an encryption method that can change over time. Togawa teaches the benefit of an encryption scheme identifier by explaining that its encryption method ID allows “apparatuses that exchange data can be notified of the encryption specification appropriately with each other, which allows secure and efficient data exchange therebetween.” Ex. 1006 at 23:36-39. A POSITA would have been motivated to use Togawa’s encryption scheme identifier in place of Nair’s privacy indicator to allow for the capability of multiple non-null encryption schemes. My opinion regarding Togawa’s teachings do not change if Togawa was considered on its own.

51. However, Nair’s teaching regarding the manual (or what Dr. Mahon calls trial-and-error) deciphering technique further supports the proposed combination regardless of how many non-null encryption schemes Nair discloses. Near teaches that the purpose of its privacy indicator is to avoid the trial-and-error process:

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.

Ex. 1004, [0043]. From this teaching, a POSITA would recognize and appreciate the benefits of a privacy indicator no matter the number of non-null encryption schemes it supports. A POSITA would have understood that trial-and-error would even less efficient when there more than two options to try based on Nair's disclosure that trial-and-error is inefficient when there are only two options (*e.g.*, null and non-null).

52. Additionally, the use of an encryption scheme identifier—including its benefits of providing faster processing times and reducing required resources—were well-known in the art at the time of alleged invention.

53. Dr. Mahon also opines that Nair and Togawa are incompatible because they teach a different number of schemes. Ex. 2005, ¶¶ 131-32. I disagree. Dr. Mahon failed to consider the proposed combination of Nair and Togawa that replaces Nair's privacy indicator with Togawa's encryption method ID to allow Nair's system to implement two or more non-null encryption methods.

54. For example, Dr. Mahon's criticism that Nair does not already have the capability to use two or more non-null schemes is irrelevant because Togawa's functionality encryption method ID with multiple non-schemes is replacing it in the proposed combination. Thus, the Nair-Forsberg-Togawa combination the system is

capable of encrypting multiple non-null schemes. Dr. Mahon did not dispute that Nair-Forsberg-Togawa **combination** would achieve multiple encryption schemes, but instead just focuses on Nair alone. Ex. 2005 ¶¶ 131-32.

55. Dr. Mahon says. “[n]othing in Nair discusses how to address” the problem of “interpret[ing] a failed decryption” when there are multiple non-null scheme, “nor does it contemplate that the decryption could fail, because only one type of encryption is ever used.” Ex. 2005, ¶ 132. But Togawa does teach a solution to that problem, which is why a POSITA would incorporate Togawa’s encryption method ID into Nair.

56. It is not relevant that Nair does not have the capability to use two or more non-null schemes without modification because Togawa teaches a solution to multiple non-null schemes. In my opinion, the use of additional non-null schemes, as taught by Togawa, is an obvious, predictable variation of Nair because supporting more than two possible non-null schemes is not a significant or inventive modification to Nair’s system. Nair already teaches how to indicate two schemes (one of which is non-null). Adding another non-null scheme is trivial and not inventive. Such a solution would be immediately apparent to a POSITA.

VII. Grounds 2-3

57. As I explained in my opening declaration, in my opinion, Nair in combination with Forsberg and 5G-Ensure D3.1 and Nair in combination with Forsberg, Togawa, and 5G-Ensure D3.1 each render claims 8 and 14 obvious. Ex. 1002 ¶¶ 144-47. Dr. Mahon disagrees because he contends that the Attribute Based Encryption (ABE) based on elliptic curve pairings disclosed by 5G Ensure teaches away from using ECIES because ECIES is not an ABE scheme. Ex. 2005, ¶¶ 136-42.

58. I disagree. ABE schemes using ECIES were well known at the time of the invention. For example, an article on “attribute-based encryption in vehicular cloud computing” discloses “lightweight attribute-based encryption (LABE) based on Elliptic Curve Integrated Encryption Scheme (ECIES).” Ex. 1023 at 3. The article also expressly discloses an ABE scheme using both public and private keys showing that ABE is compatible with public and private keys. *Id.* at 6 (“TA sets up its master secret key and its corresponding public key.”). Another example is the following article, which discloses another ABE scheme based on ECIES. *See also* Ex. 1024 at Abstract (“ABE scheme based [on ECIES]”), 7. At the time of the invention, a POSITA would have understood 5G Ensure’s teaching of Attribute Based

Encryption (ABE) based on elliptic curve pairings to refer specifically to such an ABE with ECIES scheme. Ex. 1010, §3.1.5.1 at 33.

VIII. Secondary Considerations

59. In my opinion, there are no secondary considerations of non-obviousness (sometimes called objective indicia of non-obviousness) with a nexus to the Challenged Claims of the '817 Patent that would support a determination that the at-issue claims are not obvious. To the contrary, in my opinion, the objective evidence makes clear that the Challenged Claims of the '817 Patent would have been, in fact, obvious to a POSITA.

60. In its Patent Owner Response, Ericsson has argued that there exist the following secondary considerations of non-obviousness with respect to the '817 patent: a long-felt need, receiving industry praise, and commercial success. POR at 36-37. In my opinion, none of these secondary considerations exist.

A. Commercial Success

61. In my opinion, Ericsson has not shown the required nexus to the claimed features of the '817 Patent. Accordingly, Ericsson's attempt to demonstrate commercial success related to "5G" generally fails to demonstrate secondary considerations supporting non-obviousness for the '817 Patent because there is no nexus to the Challenged Claims.

62. Because there are over 75,000 patents are declared essential to the 5G standard, *see* <https://www.questel.com/resourcehub/5g-standard-essential-patents-the-reality-behind-the-numbers/>, in my opinion, it is illogical for Ericsson to attempt to credit the '817 Patent with the success of 5G.

63. Moreover, to the extent that the sections of the 5G NR standard itself (or alternatively, devices supporting the 5G NR standard in general) have been commercially successful (which Ericsson appears to assume is the case, without providing evidence), there is no evidence to suggest a nexus between the alleged inventive aspect of the '817 patent and that commercial success. There are many technologies incorporated into the standard, such as TS 38.212. There is no reason to conclude that the alleged commercial success is due to the specific technology claimed in the '817 Patent. Many versions of the 5G standard, such as 5G Non-Standalone (NSA) cannot use a SUCI, for example. Currently, 5G Non-Standalone (NSA) is significantly more popular than 5G Standalone (SA). This informs my opinion that any success of 5G is not due to the alleged invention at all.

64. In my opinion, Ericsson fails to show how the '817 Patent allegedly came to be incorporated into the 3GPP standard and how that necessarily provides indicia of non-obviousness.

65. Further, in my opinion, the incorporation of a claimed feature of the '817 Patent into the 5G standard is not evidence of commercial success, which is, in my opinion, commercially successful for reasons completely unrelated to the '817 Patent.

B. Industry Praise

66. Ericsson cites a paper titled “Security in 5G Networks – How 5G networks help Mitigate Location Tracking Vulnerability” (Ex. 2002). Ex. 2005 ¶ 59. In my opinion, this document highlights the key feature as “IMSI of the UE is never sent in plaintext at any time during the initial registration with the network.” Ex. 2002 at 4. But Ericsson did not invent that concept as the background section of the '817 patent explains. Ex. 1001 at 1:39-40. While the document describes the encryption scheme identifier and public key identifier (Ex. 2002 at 4), it does not praising them. Regardless a single instance of one academic paper calling a feature “key” is not sufficient evidence of industry praise of the '817 Patent or evidence of non-obviousness.

C. Long-Felt but Unsolved Need

67. In my opinion, while the issue of subscriber privacy was long felt, as I explained above, it was not unsolved. And, while the problem of IMSI catching in 3G and 4G systems was well known, in my opinion, it was widely expected that the

5G standard would address this issue and there were many proposals for solving this issue pre-dating the '817 Patent, such as Nair As with the '817 Patent, many of these solutions were based on encrypting the IMSI with the public key of the UE's home network. *See id.* In my opinion, because the key element of encrypting the IMSI was well-known, there was no problem left to be solved by Ericsson. *See, e.g.,* '817 Pat. at 1:37–44. Because of this, in my opinion, the fact that the 5G standard solved a long-felt problem (IMSI catching) with what the '817 Patent admits was a known solution (IMSI encryption) is not evidence of the '817 Patent's alleged non-obviousness.

D. Simultaneous Invention

68. As discussed above, numerous others have invented and applied subscriber-identity encryption technologies. Accordingly, this simultaneous invention provides strong evidence that the claimed invention of the '817 Patent would have been obvious.

IX. CONCLUSION

69. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the

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

like so made are punishable by fine or imprisonment, or both, under Section 1001 of
Title 18 of the United States Code.

Dated: February 24, 2025



Harry Bims, Ph.D.