

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

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	CLAIM CONSTRUCTION OF “ENCRYPTION SCHEME IDENTIFIER”.....	1
II.	GROUND 1: NAIR IN COMBINATION WITH FORSBERG	5
A.	A POSITA Would be Motivated to Combine Nair with Forsberg.....	5
B.	Nair Teaches an Encryption Scheme Indicator.....	7
C.	The Combination of Nair and Forsberg Teaches a “Public Key Identifier”	11
D.	The Combination of Nair and Forsberg Renders Obvious Claim 2	12
E.	Nair in view of Forsberg Renders Obvious Claims 8 and 14 Through Nair’s Express Incorporation of TR 33.899.....	13
F.	Nair in view of Forsberg Renders Obvious Claim 12.....	16
G.	Nair in view of Forsberg Renders Obvious Claims 3, 4, 5, 6, 9, 10, 11, 13 and 15	16
III.	GROUND 2: NAIR IN COMBINATION WITH FORSBERG AND TOGAWA.....	16
A.	A POSITA Would be Motivated to Combine Nair with Forsberg and Togawa.....	16
B.	The Combination of Nair, Forsberg, and Togawa Teaches an Encryption Scheme Indicator.....	21
C.	Claims 2-6, 8-17 are Rendered Obvious by Nair in view of Forsberg and Togawa	22
IV.	GROUND 3 AND 4: GROUND 1-2 IN FURTHER COMBINATION WITH 5G-ENSURE	22
V.	THERE ARE NO SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS.....	23

IPR2024-00702

Petitioner's Reply to Patent Owner's Response

VI. CONCLUSION.....25

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Comark Commc'ns, Inc. v. Harris Corp.</i> , 156 F.3d 1182 (Fed. Cir. 1998)	4
<i>Cont'l Circuits LLC v. Intel Corp.</i> , 915 F.3d 788 (Fed. Cir. 2019)	4
<i>Harari v. Lee</i> , 656 F.3d 1331 (Fed. Cir. 2011)	15
<i>Intel Corp. v. PACT XPP Schweiz AG</i> , 61 F.4th 1373 (Fed. Cir. 2023)	20
<i>InterDigital Commc'ns, LLC v. Int'l Trade Comm'n</i> , 690 F.3d 1318 (Fed. Cir. 2012)	3
<i>In re Kao</i> , 639 F.3d 1057 (Fed. Cir. 2011)	24
<i>NeuMoDx Molecular, Inc. v. HandyLab, Inc.</i> , IPR2020-01133, Paper 23 (P.T.A.B. 2021).....	15
<i>Paice LLC v. Ford Motor Co.</i> , 881 F.3d 894 (Fed. Cir. 2018)	15, 16
<i>Wyers v. Master Lock Co.</i> , 616 F.3d 1231 (Fed. Cir. 2010)	25

All emphases are added unless otherwise noted.

LIST OF EXHIBITS

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

Petitioner's Reply to Patent Owner's Response

Exhibit No.	Description
1016	Declaration of Friedhelm Rodermund
1017	Declaration of Nathaniel E Frank-White
1018	Declaration of John Rhine
1019	Reply Declaration of Harry V. Bims, Ph.D.
1020	July 16, 2024 Transcript of ITC Hearing
1021	Deposition Transcript of Dr. Mark Mahon, February 12, 2025
1022	5G Standard Essential Patents: The Reality Behind the Numbers Presentation
1023	Nkenyereye, L., et al., A secure billing protocol over attribute-based encryption in vehicular cloud computing (2016)
1024	Meddah, N., et al., Scalable Lightweight ABAC Scheme for Secure Sharing PHR in Cloud Computing (2018)

Faced with a strong unpatentability challenge, Patent Owner (“PO”) resorts to a scattershot rebuttal that relies on mischaracterizations of the asserted art, misapplications of the law, and illusory distinctions between what is claimed in the ’817 patent and what a POSITA would have known in view of the prior art. Ultimately, as described below, PO’s positions are not supported by the ’817 patent, the prior art, or even its own expert.

I. CLAIM CONSTRUCTION OF “ENCRYPTION SCHEME IDENTIFIER”

PO proposes a construction of an “encryption scheme identifier” that requires it to be “capable of identifying at least two possible encryption schemes” and excludes “a flag that is nothing more than an on or off” (Paper 14 (“POR”) at 14 and 17). PO’s outcome-driven construction is unsupported and contrary to the plain meaning.

The specification repeatedly explains that the “encryption scheme identifier [] identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI,” reflecting the term's plain meaning, as Dr. Bims explains. *E.g.*, Ex. 1001 at Abstract, 1:56-59, 2:4-5, 19:55-58, 20:24-26; Ex. 1019, ¶ 13-14. Nothing in the claims, specification, or other intrinsic or extrinsic record suggests otherwise. *Id.*

Consistent with this plain and ordinary meaning, the ’817 patent discloses an encryption scheme identifier that uses a value of “0” to indicate a null-encryption

scheme and a value of “1” to indicate a non-null-encryption scheme (*e.g.*, ECIES).

Ex. 1001 at 10:17-20 & Figs. 4, 5; Ex. 1019, ¶ 15-16.

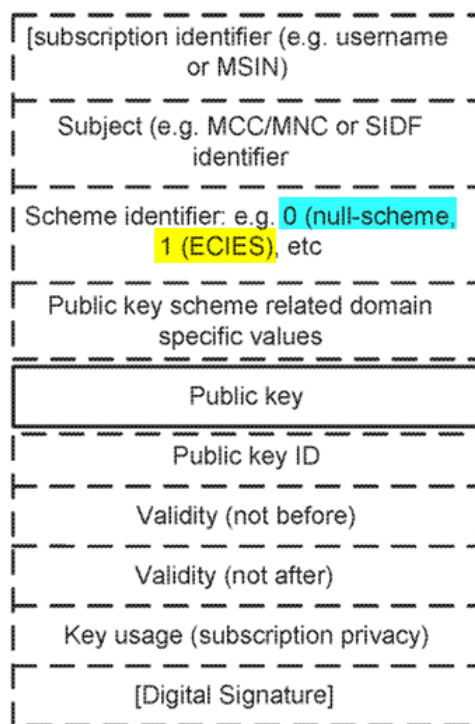


Fig. 4

To be clear, it is undisputed that in the context of the '817 patent, null-encryption (which is the same as not encrypting)¹ is an encryption scheme. *See* Ex. 1001, 3:27-28 (“The encryption scheme may be a null-encryption scheme”), 9:11-13, 15:7-9. Both experts agree that null-encryption is a valid encryption scheme. Ex. 2005, ¶ 57 (“[T]he '817 Patent identifies several encryption schemes that can be used for the encryption scheme identifier, such as a null-scheme.”); Ex. 1002, ¶ 28; Ex. 20. And

¹ Ex. 2021 at 44:1-3, 112:5-9.

POR also concedes the null-scheme is an example of an encryption scheme in the '817 Patent. POR at 15-16. The only non-null example of encryption scheme that is indicated by an encryption scheme identifier is ECIES. Ex. 1001 at Figs. 4 and 5; Ex. 1019, ¶ 16. Accordingly, in the light of the specification, an indicator that identifies between null encryption (off) and encryption (on) is an encryption scheme identifier under the plain and ordinary meaning. Ex. 1019, ¶ 17.

In arguing otherwise, PO improperly deviates from the ordinary meaning by asking that the claims of the '817 Patent be limited to an indicator with at least two possible **non-null** schemes. POR at 14-17. But PO does not argue lexicography or disclaimer and therefore the plain and ordinary meaning applies. *InterDigital Commc'ns, LLC v. Int'l Trade Comm'n*, 690 F.3d 1318, 1324 (Fed. Cir. 2012). Certainly, nothing in the claims or the specification of the '817 patent requires two **non-null** encryption schemes to be supported by an encryption scheme identifier. Ex. 1019, ¶ 18. As discussed above, the embodiment of Figure 4 does not even expressly disclose two, specific, non-null examples. Ex. 1001 at Fig. 4; Ex. 1019, ¶ 15-16.

PO's construction also improperly excludes embodiments thereby confirming that it is contrary to the plain meaning. 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. And PO cannot genuinely dispute that a "flag" or "Boolean"

is such an “other data type,” yet its construction expressly seeks to exclude that data type. Ex. 1019, ¶ 20. As another example, the specification's disclosure that “[~~e~~]ach scheme adopted as standard **may be** assigned a specific identifier” (*id.* at 10:17-24) is inconsistent with PO's construction as a POSITA would have understood the standard may ultimately only adopt one non-null scheme. *See* Ex. 2003 at 2 (“[T]here is a need of preferably more than one, **but at least one**, standardized public key encryption schemes[.]”); Ex. 1019, ¶ 21.

Additionally, PO's argument relies primarily on the specification's usage of “etc.” in the Figures 4 and 5, as well as the disclosure of “4-bit identifier” as evidence that second non-null scheme is always required. *See* POR at 15-16. But it is well settled “that limitations from the specification are not to be read into the claims.” *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1186-87 (Fed. Cir. 1998) (“[P]articular embodiments and examples appearing in the specification will not generally be read into the claims.”); *Cont'l Circuits LLC v. Intel Corp.*, 915 F.3d 788, 797 (Fed. Cir. 2019). Here, each example relied on by PO uses language that indicates said disclosure is exemplary and non-limiting in nature. Ex. 1019, ¶ 16. For example, Figure 4 illustrates a “**particular example** of the privacy key.” Ex. 1001 at 9:22-41, 5:45 (“FIG. 4 illustrates an **example** of a privacy key”). On cross-examination, Dr. Mahon admitted that Figure 4 “is not limiting it to a certain number.” Ex. 2021 at 33:10-21. Figures 4 and 5 also use “e.g.” to indicate that its

encryption scheme identifier is just an example. *Id.*, Fig. 4 (“Scheme identifier: *e.g.* 0 (null-scheme, 1 (ECIES), etc.”), Fig. 5, 10:17-25. A POSITA would understand that all these examples are illustrative and non-limiting. Ex. 1019, ¶ 19; Ex. 2021 at 33:10-21.

II. GROUND 1: NAIR IN COMBINATION WITH FORSBERG

A. A POSITA Would be Motivated to Combine Nair with Forsberg

PO argues that a POSITA would not be motivated to combine Nair with Forsberg based solely on the allegation that Nair itself does not teach multiple encryption key pairs. POR at 17-19. PO's argument fails.

First, as the Institution Decision recognized, “even if Patent Owner is correct that Nair's disclosures do not teach or suggest multiple key pairs, the record includes Dr. Bims's testimony that the combination would be motivated in order to allow use of Nair's teachings in networks that did use multiple keys, such as those disclosed in Forsberg.” Paper 7 at 27; Ex. 1002 ¶¶ 47, 49–50, 87. But neither the POR, nor Dr. Mahon, address Petitioner's argument that a POSITA would have been motivated to make the combination to allow the use of Nair's teachings in networks that did use multiple keys, such as those disclosed in Forsberg. POR at 17-19. As Dr. Bims explains, “a POSITA would have been motivated to consult and apply Forsberg because Forsberg teaches key identifiers to manage multiple keys used in encryption.” Ex. 1002, ¶ 48. Moreover, 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.” Ex. 1002, ¶ 49. Dr. Bim’s testimony is uncontroverted on this point. This alone is fatal to PO’s argument.

Second, contrary to PO’s assertions, Nair does suggest the use of multiple keys. PO argues that Nair only has one SLF and that each SLF has one and only one pair of keys. POR at 19. But Nair expressly discloses that “larger numbers of such system elements” such as the “SLF” may be used in its wireless cellular system. Ex. 1004, [0057], Ex. 1002, ¶ 89. This is unsurprising, as 5G networks will obviously include multiple SLFs since each operator must have at least one. Ex. 1019, ¶ 25; Ex. 1021 at 89:4-20. Indeed, PO admits later in its POR that Nair has “multiple SLFs.” POR at 26; Ex. 1021. 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. Ex. 1019, ¶ [26]. Accordingly, even if Petitioner were correct that Nair only discloses that SLF would only have a single key, Nair still suggests multiple keys by disclosing multiple SLFs.

Furthermore, PO and Dr. Mahon’s argument that each SLF only uses a single key pair is unsupported by the text of Nair. POR at 19. In Nair, each HSS is considered its own home network. Ex. 1004, [0054] (“These HSSs/UDMs represent the home networks of UEs”), Fig. 1. So when Nair says “the network private key”

for “an HSS” (Ex. 1004, [0038]), a POSITA would understand it is referring to the key associated with the HSS. Ex. 1019, ¶ 27. Accordingly, a POSITA would understand that Nair discloses that the SLF has a key pair for each of the multiple HSSs. Ex. 1002, ¶ 47; Ex. 1019, ¶ 27.

B. Nair Teaches an Encryption Scheme Indicator

As the Petition explains, Nair teaches “an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI,” as recited by claims 1, 9, 10, and 15. Pet. at 31.

PO argues that “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.” POR at 20. PO’s argument fails because Nair’s privacy flag indicates at least two potential encryption schemes, including the null-encryption scheme and Nair’s public/private encryption scheme, as Dr. Bims explains. Ex. 1002, ¶¶ 74-76. For example, Nair teaches that if the privacy indicator is not set (e.g., set to 0), the privacy indicator indicates the null-encryption scheme is used. Ex. 1004, [0043]; Ex. 1002, ¶ 74. And “[i]f the flag is set, the SLF will recognize that the provided IMSI is encrypted and use *the network private key* to decrypt the MSIN part to form the real unencrypted IMSI.” Ex. 1004, [0043]; Ex.

1002, ¶ 75. Accordingly, Nair's privacy indicator clearly indicates at least two possible encryption schemes.

PO's argument that Nair does not teach multiple encryption schemes is founded on the incorrect premise that not encrypting (*i.e.*, null-encryption) is not a valid encryption scheme. But as discussed above, there is no dispute amongst the experts that the '817 patent expressly considers null-encryption a valid encryption scheme. *See* Section I.

The POR also suggests setting Nair's privacy indicator does not indicate which encryption scheme is used because Nair's SLF and UE require a shared understanding regarding which encryption scheme is indicated by setting the privacy indicator. POR at 22. But the system described in the '817 patent also operates on a shared agreement as to the meaning of the indicator. Ex. 1002, ¶ 76. To use Figure 4 as an example, when the encryption scheme indicator is "0," both the UE and deconcealing

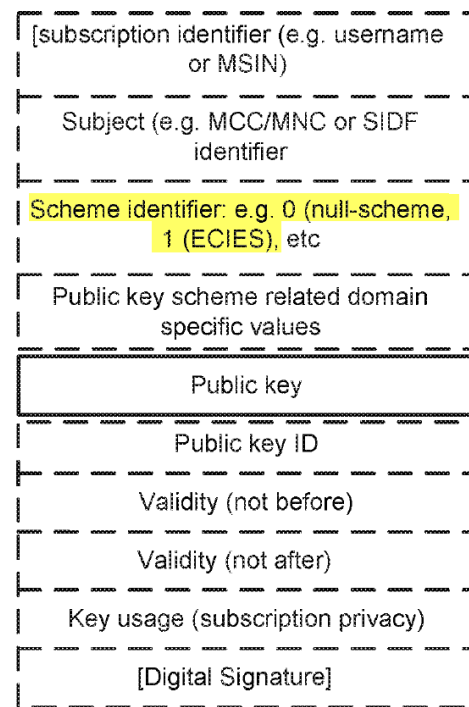


Fig. 4

server in the '817 patent need to have a shared understanding that "null-scheme" encryption is used. Ex. 1001 at Fig. 4; Ex. 1021 at 32:7-33:9. And when "1" is indicated, ECIES is used based on the shared understanding that "1" means ECIES

encryption. *Id.* Nair's privacy indicator works exactly the same way. Ex. 1002, ¶ 76. If it's not set (*e.g.*, 0) null encryption is used. Ex. 1004, [0043]. If it is set (*e.g.*, 1), the public/private key encryption scheme is used. *Id.* Thus, contrary to PO's argument (POR at 22), Nair's privacy indicator does imbue the SLF with knowledge of the encryption scheme used by the UE. Ex. 1002, ¶ 76.

PO also proposes an absurd hypothetical scenario where Nair's UE—for unexplained reasons—would use an encryption scheme unknown to the SLF and still set its privacy indicator. POR at 22. That scenario is not founded on any teaching of Nair and should be rejected on that basis alone. Moreover, contrary to PO's implicit assertion, the encryption scheme identifier described by the '817 patent would also be unable to protect against such a scenario. If the UE of the '817 patent set the indicator to 1 but used a different scheme other than ECIES, decryption would also obviously fail for the exact same reason.

Nevertheless, PO attempts to distinguish Nair's privacy indicator as being limited to use in conjunction with a "single trial or error test." POR at 21. But Nair's "trial or error test" is expressly described as a disfavored *alternative* to the privacy indicator:

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]. Thus, Nair teaches to use the privacy indicator to avoid such inefficient trial and error, as shown in the excerpt above, the same attribute that PO ascribes to the '817 patent. Ex. 1004, [0043].

PO also argues that Nair cannot implement multiple encryption schemes because it only has a single SLF. POR at 21. PO's reasoning is unsupported since nothing in Nair suggests an SLF couldn't use multiple encryption schemes. Regardless, the POR expressly admits Nair has "multiple SLFs," POR at 26; Ex. 1021, as it must because Nair clearly discloses multiple SLFs as discussed above.

Finally, the POR contends that Dr. Bims and Petitioner concede that Nair does not disclose an encryption scheme identifier. POR at 23. In doing so, however, PO resorts to nothing more than semantics. As Dr. Bims explained, Nair does not "expressly" use the term "encryption scheme identifier," but Nair does teach "subject matter of an encryption scheme identifier" through its "privacy indicator." Ex. 2007 at 31:14-19, 59:5-14. As the Board recognized in the ID, the relevant question is what "Nair *teaches or suggests*" not what it "expressly discloses." Paper 7 at 25. Neither Dr. Bims, nor Respondents in the ITC hearing, have ever suggested Nair does not teach the subject matter of the encryption scheme identifier. Nair clearly does. *See* Section II.B.

C. The Combination of Nair and Forsberg Teaches a “Public Key Identifier”

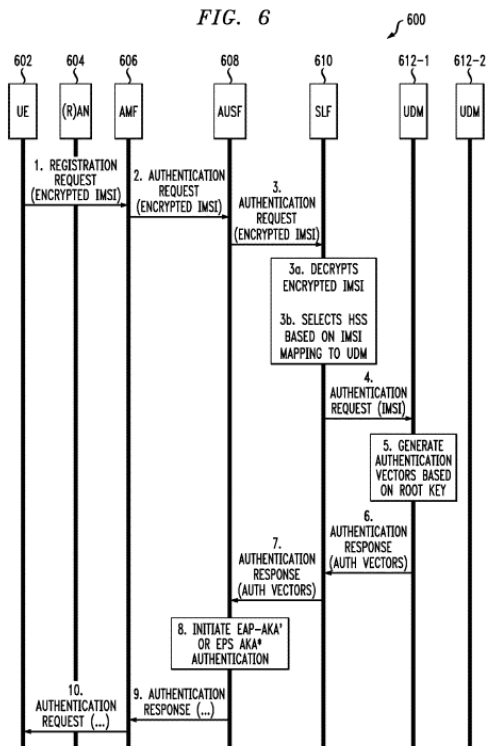
As the Petition explains, the combination of Nair and Forsberg teaches “a public key identifier for a public key of the home network,” as recited by claims 1, 9, 10, and 15. Pet. at 31. Although PO does not dispute that Forsberg discloses a “public key identifier” (Ex. 1020 at 1540:18-22), PO nevertheless disputes that the combination of Nair and Forsberg discloses that identifier. POR at 24-25. At bottom, PO's argument collapses to a repetition of its argument that a POSITA would not be motivated to combine Nair and Forsberg. POR at 24-25. For the reasons discussed in Section II.A, above, PO's arguments fail.

Dr. Mahon's argument (Ex. 2005, ¶ 112) that the public key identifier is superfluous because Nair allegedly has a “(single) private key” that is already indicated by the privacy indicator fails for the same reasons. *See* Section II.A. Namely Dr. Mahon fails to consider that a POSITA would have been motivated to use multiple keys (as disclosed by Forsberg) in Nair's system due to the benefits described by Forsberg, including enhanced security and protection against one key being compromised. Ex. 1002, ¶¶ 48-49, 87; Ex. 1019, ¶¶ 29, 36. Accordingly, the proposed combination of Nair and Forsberg has the capability of implementing multiple keys (regardless of whether unmodified Nair does), which means a public key indicator is not superfluous. *See* Ex. 1002, ¶ 87.

Additionally, PO argues that Forsberg's public key identifier "render[s] Nair's privacy indicator superfluous," which gets Dr. Mahon's argument backwards and is thus unsupported by expert testimony. POR at 24-25 (misrelying on Ex. 2005, ¶ 112 (opining the "privacy indicator alone is enough" and the public key identifier is superfluous). But as Dr. Bim's explains, Forsberg's public key indicators aren't used to show null encryption. Ex. 1019, ¶ 38. There is no indicator value that indicates no key is being provided. *Id.* Accordingly, a privacy indicator is still required. *Id.* And the efficiency gains by potentially omitting a single bit would not motivate a POSITA to avoid using the privacy indicator in any case. *Id.*, ¶ 39.

D. The Combination of Nair and Forsberg Renders Obvious Claim 2

PO disputes Nair and Forsberg teach the additional limitation of claim 2 because Nair discloses that the SLF (*i.e.*, the deconcealing server) selects an HSS based on the MCC + MNC rather than on UE information, as required by claim 2. POR at 25-26. But the MCC + MNC *is* UE information and Nair discloses that **both** the SLF and HSS are selected based on this information. As Dr. Mahon explained on cross-examination, the AMF in Nair (*e.g.*, Ex. 1004 at Fig. 6) sends an authentication request to the AUSF, which sends the authentication request to the SLF for decryption.



Ex. 1004, Fig. 6. In the 5G network disclosed by Nair, there is more than one SLF, at least one for each operator. Ex. 1021, 88:25-89:13. As Dr. Mahon explained, the AMF uses the MCC and MNC to determine the home network for the UE. Ex. 1021, 88:1-89:1. For these reasons, Dr. Mahon agreed that information from the UE is used to determine which SLF receives the authentication request in Nair. Ex. 1021, 9:14-20. Nothing more is required.

E. Nair in view of Forsberg Renders Obvious Claims 8 and 14 Through Nair's Express Incorporation of TR 33.899

As detailed in the Petition, Nair teaches “the encryption scheme is an Elliptic Curve Integrated Encryption Scheme (ECIES),” as recited in claims 8 and 14. Pet. at 51 and 58. Nair teaches this element because Nair incorporates by reference “in

its entirety” 3GPP TR 33.899 V1.1.0 (Ex. 1004, [0007]; Ex. 1008, 2:4-9), which expressly discloses concealment of the MSIN portion of a UE's IMSI using an Elliptic Curve Integrated Encryption Scheme (ECIES) to address the same problem addressed by Nair, Ex. 1004, [0007], namely securing permanent subscriber identifiers using public key encryption. Ex. 1007, §§5.7.4.15 at 376-77, 5.7.4.3.2.2 at 344; Ex. 1002, ¶ 111.

PO argues Nair's incorporation is insufficient under Federal Circuit law because Nair “only includes a bare reference to TR 33.899.” POR at 27-28. But PO's argument is factually and legally baseless. Nair includes far more than a bare reference to TR 33.899. Ex. 1004, [0007]; Ex. 1008, 2:4-9. Nair broadly and unequivocally incorporates *the entirety* of TR 33.899's disclosure directed to UE privacy:

Privacy is an important consideration in any communication system. Privacy is broadly addressed in 5G Technical Report (TR) 33.899, V 1.1.0, entitled “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14),” **the disclosure of which is incorporated by reference herein in its entirety**. In particular, TR 33.899 identifies subscription (UE) privacy as one of the most important security areas to be addressed in 5G networks.

Ex. 1004, [0007]; Ex. 1008, 2:4-9. Nair explains that TR 33.899's solutions to privacy include encryption of the permanent subscription identifier (SUPI) of the UE. Ex. 1004, [0028]-[0031]. ECIES is one of those solutions proposed in the

section of TR 33.899 dealing with the “key issue” of “[c]oncealing permanent or long-term subscription identifier. Ex. 1007, §§5.7.4.15 at 376-77, 5.7.4.3.2.2 at 344; Ex. 1002, ¶ 111; Ex. 1021 at 82:24-84:7.

Such “broad and unambiguous” incorporation of TR 33.899 (Ex. 1007) is “plainly sufficient to incorporate” TR 33.899's disclosures in their entirety under Federal Circuit law. *See Paice LLC v. Ford Motor Co.*, 881 F.3d 894, 907 (Fed. Cir. 2018); *Harari v. Lee*, 656 F.3d 1331, 1335 (Fed. Cir. 2011) (incorporated in their entirety based on “broad and unequivocal language”); *see also NeuMoDx Molecular, Inc. v. HandyLab, Inc.*, IPR2020-01133, Paper 23 (P.T.A.B. 2021) (finding err in refusal to find anticipation where “language indicating that another patent ‘is incorporated herein by this reference’ was broad and unambiguous, and plainly sufficient to incorporate the referenced patent in its entirety.”). For these reasons, all of TR 33.899, and in particular its disclosure of ECIES, is incorporated into Nair.

Further, Dr. Mahon agrees that ECIES was “a known technique that would be considered as part of any encryption scheme being implemented.” Ex. 1021, 84:21-85:2. Nor does Dr. Mahon dispute “that the 5G standard developers knew that ECIES was a good choice for the mobile devices before the invention of the ’817 patent.” Ex. 1021, 84:21-85:2.

F. Nair in view of Forsberg Renders Obvious Claim 12

PO repeats its argument that Nair does not incorporate TR 33.899 by reference. POR at 28. But, as discussed above in Section II.E, Nair broadly and unambiguously incorporates the entirety of TR 33.899. *See Paice LLC*, 881 F.3d at 907. Further, Nair discloses a temper resistant USIM (*e.g.*, “USIM securely stores the [IMSI]”) and renders obvious generating the SUCI with said USIM even without relying on TR 33.899. Pet. at 55; Ex. 1004, [0051]; Ex. 1008, 9:2-4; Ex. 1002, ¶ 121.

G. Nair in view of Forsberg Renders Obvious Claims 3, 4, 5, 6, 9, 10, 11, 13 and 15

PO does not dispute that the additional limitations of claims 3, 4, 5, 6, 9, 10, 11, 13, or 15 are rendered obvious by Nair in view of Forsberg, resting its argument on these claims on its contention that claim 1 is not invalid. POR at 27-28. But as shown above, Nair, in view of Forsberg, renders obvious claim 1.

III. GROUND 2: NAIR IN COMBINATION WITH FORSBERG AND TOGAWA

A. A POSITA Would be Motivated to Combine Nair with Forsberg and Togawa

PO's primary counterargument for Ground 2 is that a POSITA would allegedly not be motivated to combine Nair and Togawa because Nair does not disclose (and is not compatible with) multiple encryption schemes. POR at 30. As an initial matter, PO's premise is not true. Nair teaches at least two encryption schemes: the null scheme and its public/private key encryption scheme, as discussed

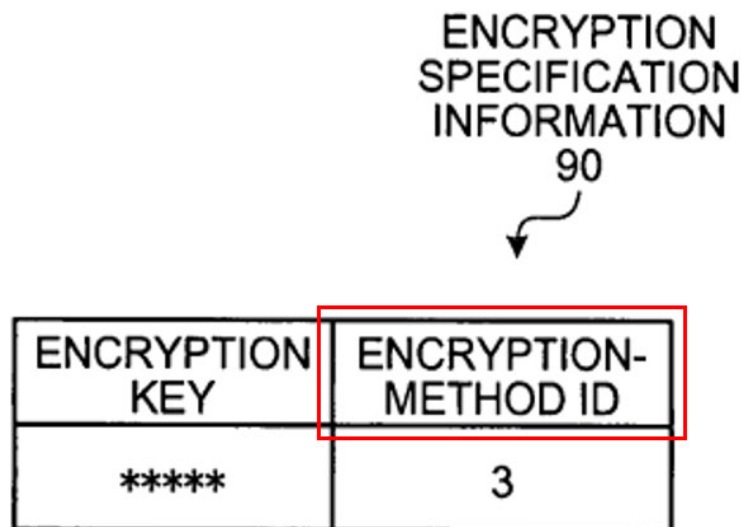
above. *See* Section II.B. Moreover, PO's attempt to construe "encryption scheme identifier" to require more than one *non*-null encryption scheme is improper. *See* Section I. Accordingly, PO's argument fails.

To the extent the Board construes the claims to require more than one non-null encryption scheme, a POSITA would be motivated to use Togawa's scheme in Nair system to enable multiple non-null schemes. Pet. at 60-62. Indeed, as explained in the Petition, a POSITA would be motivated to replace Nair's privacy indicator with Togawa's encryption method ID to achieve Togawa's capability to indicate more than two encryption schemes. Pet. at 62, 60-61; Ex. 1019, ¶¶ 43, 46, 47–50; Ex. 1002 ¶¶ 139, 136.

PO contends there is no motivation to combine because Nair does not teach multiple non-null encryption schemes (POR at 30) and because Nair and Togawa are in different fields (*id.* at 31). Both arguments fail.

First, PO's argument that Nair does not teach multiple non-null encryption schemes falls flat because Togawa teaches multiple encryption schemes and thus Petitioner does not need to rely on Nair to teach multiple non-null encryption schemes. Indeed, Togawa's recognition of the benefits of multiple non-null encryption schemes stands independently and does not rely on Nair's teachings. Ex. 1002, ¶¶ 136, 139; Ex. 1019, ¶ 47. As Dr. Bim explains, Togawa teaches the

inclusion of encryption-method ID to identify of multiple encryption schemes. Ex. 1002, ¶ 142; Ex. 1006 at Fig. 13; 23:19-25.



Id., Fig. 13 (annotated).

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. Ex. 1006, 23:1-4 (noting the encryption method changes over time), 23:17-39; Ex. 1002, ¶ 142; Ex. 1019, ¶ 50. Togawa teaches 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, 23:36-39; Ex. 1002, ¶ 142; Ex. 1019, ¶¶ 49-50. Dr. Mahon does not dispute a POSITA would be motivated to achieve secure and efficient data exchange or that Togawa teaches the same. Ex. 2021, 24:8-13, 52:23-1.

Petitioner's Reply to Patent Owner's Response

Although Togawa alone teaches the benefits of multiple non-null encryption schemes, Nair's teaching regarding the manual (or trial-and-error) deciphering technique further supports the proposed combination regardless of how many encryption schemes Nair discloses. Ex. 1019, ¶ 51. As explained above, Nair explains that the purpose of its explicit privacy indicator is to avoid having to do an inefficient trial-and-error process. Ex. 1004, [0043] ("But one key reason to have such an indication specified is that this saves processing time and fewer resources are needed."). Based on this teaching, a POSITA would recognize the benefits of an explicit indicator regardless of the number of non-null schemes it supports. Ex. 1019, ¶ 51. If trial-and-error is inefficient when there are only two options (null and non-null), as taught by Nair, a POSITA would of course understand that trial-and-error would even less efficient when there more options to try, as Dr. Bims explains. Ex. 1019, ¶ 51. As such, Petitioners argument is *not* "susceptible to Patent Owner's contention that '[t]here is no disclosure of supporting multiple encryption schemes in Nair.'" *Contra*. Paper 7 at 33.

Further, contrary to PO's arguments (POR at 30-32), nothing in Nair would preclude the use of additional non-null schemes, and as a result, Nair and Togawa are not incompatible. Ex. 1019, ¶¶ 53-56. PO's argument that Nair and Togawa are incompatible because they teach a different number of schemes (POR at 30-32) fails to address the Petitioner's proposed combination, which would replace Nair's

privacy indicator with Togawa's encryption method ID to allow Nair's system to implement two or more non-null encryption methods. Ex. 1019, ¶ 55; Pet. at 60-62. That Nair does not already have the capability to use two or more non-null schemes is irrelevant because Togawa's functionality is replacing it in the proposed combination. Ex. 1019, ¶ 56. And the use of additional non-null schemes, as taught by Togawa, is an obvious, predictable variation of Nair. *Id.* Supporting more than two possible schemes is not a significant or inventive modification to Nair's system, which clearly discloses supporting two possible schemes (one which is null). *Id.*

PO's second argument that Togawa is directed to an "entirely different technology" than either Nair or Forsberg (POR at 31-32) lacks credibility and is not supported by expert testimony. As Dr. Bim's explained, all three references are specifically directed towards the encryption of user data in wireless systems, such as IMSI in Nair and Forsberg and Togawa's "user data." Ex. 1004, [0035]; Ex. 1005, [1035]; Ex. 1006, 4:43-45; Ex. 1002 ¶¶ 134-36. As explained below, Dr. Mahon does not dispute that "Togawa, discloses an encryption scheme identifier within the meaning of the '817 patent." Ex. 1020, 1542:18-1543:7.

PO's rebuttals to the Petitioner's other three obviousness rationales fall flat. POR at 29-30. Contrary to the PO's arguments (POR at 29-30), Petitioner does not have to show that replacing Nair's privacy indicator with Togawa's encryption method ID was an "improvement in a categorical sense." *Intel Corp. v. PACT XPP*

Schweiz AG, 61 F.4th 1373, 1380-81 (Fed. Cir. 2023) (finding that both prior art references “address the same problem and that [the secondary reference’s] cache was a known way to address that problem is precisely the reason that there's a motivation to combine under KSR and our precedent.”). Here, Togawa and Nair are in the same field and address the same problem. Ex. 1002, ¶¶ 134-35. And a POSITA would have been capable of applying Togawa’s known method of enhancement (an encryption scheme identifier that allows more than two non-null schemes) to Nair’s system, which was in the prior art, and the results would have been predictable to one of ordinary skill in the art, as Dr. Bims explains. Ex. 1002, ¶¶ 134-35.

B. The Combination of Nair, Forsberg, and Togawa Teaches an Encryption Scheme Indicator

PO’s sole basis for disputing that Nair in view of Forsberg and Togawa teaches “encryption scheme indicator” is its argument that a POSITA would not be motivated to make the combination. POR at 32-33. Indeed, at trial in the ITC, Dr. Mahon conceded that “Togawa, discloses an encryption scheme identifier within the meaning of the ’817 patent.” Ex. 1020, 1542:18-1543:7. As explained above, a POSTIA would motivated to combine Nair, Forsberg, and Togawa. *See* Section III.A.

C. Claims 2-6, 8-17 are Rendered Obvious by Nair in view of Forsberg and Togawa

PO does not dispute that the additional limitations of claims 2-6, 8-17 are rendered obvious by Nair in view of Forsberg and Togawa beyond incorporating its arguments regarding Ground 1. POR 33. But as shown above Ground 1 renders obvious these claims. Section II.

IV. GROUNDS 3 AND 4: GROUNDS 1-2 IN FURTHER COMBINATION WITH 5G-ENSURE

As explained in the Petition, Nair, in combination with Forsberg and 5G-Ensure D3.1 (and optionally in combination with Togawa), renders claims 8 and 14 obvious. 5G-Ensure D3.1 teaches the benefits of practicality and inherent message randomization provided by attribute-based encryption schemes such as those based on elliptic curve pairings. Ex. 1010, §3.1.5.1 at 33; Ex. 1002, ¶¶ 145-47.

PO and Dr. Mahon argue that the ABE encryption scheme teaches away from ECIES because ABCE schemes allegedly differ from public key encryption. POR at 34; Ex. 2005, ¶¶ 137-38. However, Dr. Mahon's opinions are unsupported by corroborating evidence and should thus be ignored. Ex. 2005, ¶¶ 136-42. Prior art literature flatly contradicts Dr. Mahon's unsupported claim that ABE excludes public key encryption and ECIES (*id.*). Ex. 1019, ¶ 58. For example, two prior art articles disclose ABE "based on Elliptic Curve Integrated Encryption Scheme (ECIES)." Ex. 1023 at 3, Ex. 1024 at Abstract, 7; Ex. 1019, ¶ 58. Also, Exhibit 1023

expressly discloses an ABE scheme using both public and private keys, contrary to Dr. Mahon's unsupported argument that ABE is incompatible with public and private keys. Ex. 1023 at 6; Ex. 1019, ¶ 58.

Further, Dr. Bims's testimony confirms a POSITA would have understood that 5G-Ensure D3.1 teaches ECIES because "[t]he best known encryption scheme based on ECC [elliptic curve cryptography] is the Elliptic Curve Integrated Encryption Scheme (ECIES)." Ex. 1011, 7; Ex. 1002, ¶ 144. Dr. Mahon does not disagree that ECIES was a known and obvious choice for 5G. Ex. 1021, 84:21-85:2.

V. THERE ARE NO SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS

Ericsson argued there is objective evidence of the '817 patent solving a long-felt need, receiving industry praise, and commercial success. POR at 36-37. PO's secondary considerations arguments fail because there is no nexus between the arguments presented and the claims of the '817 patent.

For industry praise, Ericsson cites a single paper, Ex. 2002. Ex. 2005 ¶ 59. While this document calls the SUCI a key feature, on the very next line the document clarifies that the key feature of the SUCI is that the "IMSI of the UE is never sent in plaintext at any time during the initial registration with the network." Ex. 2002 at 4; Ex. 1019, ¶ 66. But encrypting the IMSI in a 5G network is applicant-admitted prior art. Ex. 1001 at 1:39-40. Nor does PO dispute that both Nair and Forsberg disclose encrypting an IMSI. Ex. 1021, 94:6-12, 67:18-23. Praise of the prior art is not

evidence of secondary considerations. *In re Kao*, 639 F.3d 1057, 1068-69 (Fed. Cir. 2011). Nothing about Ex. 2002 praises the purported novel features of the '817 Patent, the encryption scheme identifier or public key identifier. Ex. 2002 at 4. While that document describes those features, it stops far short of praising them.

For similar reasons, PO has not identified any long-felt but ***unsolved*** need. The problem of IMSI catching in 3G and 4G systems was well known and, as Dr. Bims explains, it was widely expected that the 5G standard would address this issue by encrypting the IMSI with the public key of the UE's home network. Ex. 1019, ¶ 67. Because the key element of encrypting the IMSI was well-known, there was no problem left to be solved by Ericsson. *See, e.g.*, Ex. 1001, 1:37–44. 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. Ex. 1019, ¶ 67.

PO also argues that incorporation into the 5G standard shows industry praise and commercial success. POR at 36-37. But PO does not provide any evidence the technology of the '817 patent is incorporated into the 5G standard or that such standard is successful. Ex. 1019, ¶ 61-65. Versions of the 5G standard, like 5G Non-Standalone (NSA) cannot use a SUCI, for example. *Id.*, ¶ 63. And even if it were, there have been around 350,000 patents grouped into more than 67,000 patent families found to be relevant to 5G and no evidence exists tying the success of 5G

to the invention of the '817 patent. Ex. 1019, ¶ 62; Ex. 1022 at 4. Indeed, PO admits that any success of 5G is due to “numerous contributions to the standard.” POR at 37.

Accordingly, POs alleged evidence of secondary considerations do not overcome the strong prima facie case of obviousness shown in the Petition. *See Wyers v. Master Lock Co.*, 616 F.3d 1231, 1246 (Fed. Cir. 2010).

VI. CONCLUSION

For the reasons explained above, the Board should find that the Challenged Claims are unpatentable.

DATED: February 24, 2025

Respectfully submitted,

/s/ Robert A. Appleby

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

CERTIFICATE OF COMPLIANCE

This Petition complies with the type-volume limitations as mandated in 37 C.F.R. § 42.24, totaling 5553 words. Counsel has relied upon the word count feature provided by Microsoft Word.

/s/ Robert A. Appleby
Robert A. Appleby

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a complete copy of the foregoing document as served on February 24, 2025 on counsel of record for the Patent Owner via email to the following address:

Scott W. Hejny
Christian J. Hurt
Joseph Micheli
McKool Smith, P.C.
300 Crescent Court, Suite 1500
Dallas, TX 75201
Telephone: 214-978-4000
Facsimile: 214-978-4044
Emails:
shejny@McKoolSmith.com
churt@McKoolSmith.com
jmicheli@McKoolSmith.com
Ericsson_Lenovo_IPRs@mckoolsmith.com

/s/ Robert A. Appleby
Robert A. Appleby