

**UNITED STATES INTERNATIONAL TRADE COMMISSION
WASHINGTON, D.C.**

**Before the Honorable MaryJoan McNamara
Administrative Law Judge**

**In the Matter of
CERTAIN MOBILE PHONES,
COMPONENTS THEREOF, AND
PRODUCTS CONTAINING SAME**

Investigation No. 337-TA-1375

RESPONDENTS' POST-HEARING BRIEF

TABLE OF CONTENTS

	<u>Page</u>
I. Summary Of Argument.....	1
II. Background	4
A. Procedural History	4
B. The Parties	6
1. Complainant.....	6
2. Respondents	6
C. The Products at Issue	7
III. The '817 Patent	7
A. The '817 Patent's Asserted Claims.....	7
B. Level Of Ordinary Skill In The Art	10
C. The '817 Patent's Asserted Claims Are Invalid Under 35 U.S.C. § 103.....	10
1. Overview Of The Prior Art.....	11
a. Nair	11
b. Forsberg	11
c. Togawa.....	12
d. 5G-Ensure	13
2. Ground 1: Nair In Combination With Forsberg, Togawa, and 5G-Ensure Invalidates All '817 Patent Asserted Claims	13
a. Nair, Forsberg, and Togawa Invalidates Claims 10, 13, and 15.....	13
i. Independent Claims 10 and 15.....	13
ii. Dependent Claim 13	22
b. Nair, Forsberg, Togawa, and 5G-Ensure Invalidates Claim 14.....	22
i. Dependent Claim 14	22
3. Ground 2: Forsberg In Combination With Togawa And 5G-Ensure Invalidates All '817 Patent Asserted Claims	24
a. Forsberg and Togawa Invalidates Claims 10, 13, and 15.....	24
i. Independent Claims 10 and 15.....	24
ii. Dependent Claim 13	31
b. Forsberg, Togawa, and 5G-Ensure Invalidates Claim 14.....	32
i. Dependent Claim 14	32
4. There Are No Secondary Considerations Of Non-Obviousness.....	33
D. The '817 Patent's Asserted Claims Are Invalid Under 35 U.S.C. § 101.....	34
IV. The '669 Patent	36
A. Introduction and Background	36
B. Asserted Claims	39

[REDACTED]

economic activity in North Carolina. Lenovo delivers a full portfolio of PCs, tablets, monitors, accessories, and many other electronic devices and solutions in the US. Lenovo also invests extensively in equipment, labor, capital, engineering, and research and development in the US.

C. The Products at Issue

The Accused Products are Motorola mobile phones that are compatible with the 5G NR standard, including the Motorola Razr 5G, Edge 5G, and other 5G smartphones. As discussed in further detail below, the accused functionality resides on either a Qualcomm or MediaTek chipset.

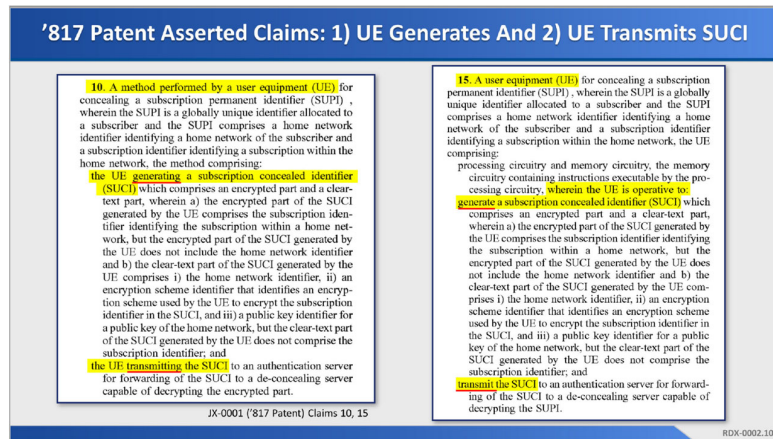
III. THE '817 PATENT

Each of the '817 patent's asserted claims (10, 13, 14, and 15) is invalid as obvious under 35 U.S.C. § 103 and as claiming patent-ineligible subject matter under § 101.

A. The '817 Patent's Asserted Claims

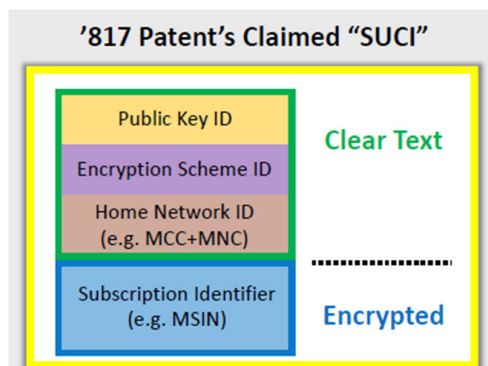
Ericsson asserts two independent claims (10 and 15) and two dependent claims (13 and 14). Hr'g Tr. at 179:16-18. The claims are directed to a user equipment (UE) and a method performed by a UE "for concealing a subscription permanent identifier (SUPI)." JX-0001 at claims 10, 15. The '817 patent itself acknowledges that this concept was known at the time of the alleged invention. As Dr. Bims explained, "encryption of user's personal information" "was known long before the '817 patent," and, in fact, "the '817 patent acknowledges that engineers developing the 5G standard already knew that the long-term subscription identifier, or SUPI, could be encrypted, and, in particular, encrypted using a public key." Hr'g Tr. at 1224:17-24, 1292:16-20; RDX-2.9; JX-0001 ('817 patent) at 1:39-43. And as Ericsson's expert Dr. Mahon admitted, "the concept" of "protecting a user's subscriber identifier" "was known." Hr'g Tr. at 1531-6.

The asserted independent claims generally include two aspects: (1) the UE "generate[s] a subscription concealed identifier (SUCI)" that includes a list of parts, and (2) the UE "transmit[s] the SUCI" along a particular path of network elements:



RDX-2.10; JX-0001 at claims 10, 15; Hr’g Tr. at 267:24-268:8 (Dr. Mahon agreeing “method claim 10 has two method steps,” “the first step is the UE generating a Subscription Concealed Identifier or SUCI,” and “the second step is the UE transmitting that SUCI”); RDX-0016.5-8.

The first aspect (generating a SUCI) involves simply compiling four parts, one of which (“subscription identifier,” an undisputed example of which is an MSIN or Mobile Subscription Identification Number) is encrypted, and the remaining parts (“home network identifier,” an undisputed example of which is a MCC+MNC (Mobile Country Code and Mobile Network Code), “encryption scheme identifier,” and “public key identifier”) are in “clear-text” (unencrypted). Hr’g Tr. at 268:9-271:20 (Dr. Mahon testifying as to these components); RDX-0016.9-18. Both parties’ experts agree that the below image accurately illustrates the components of the claimed SUCI:

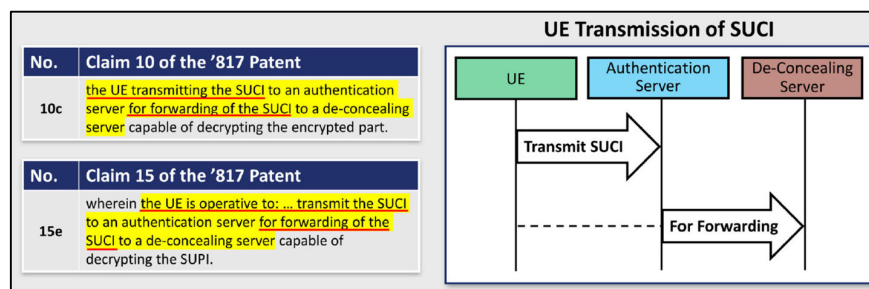


RDX-0016.9-19; RDX-0027.4; Hr’g Tr. at 268:9-271:20, 1533:9-1534:13 (Dr. Mahon); RDX-

2.11-12; Hr’g Tr. at 1225:7-1226:13 (Dr. Bims).

Each of the four parts of the claimed SUCI was known in the art before the ’817 patent. As to the first two parts, Dr. Mahon admitted that “encrypting the MSIN ... was known before the ’817 patent,” and further admitted that “the home network ID, the MCC and MNC, those were known,” they “have been around for a long time,” and they likewise “were transmitted in clear-text in the prior art.” Hr’g Tr. at 1534:14-24; *see also id.* at 1531:1-6, 269:18-22 (Dr. Mahon agreeing that “it was known before the ’817 patent that you could encrypt this MSIN”). As to the third part, Dr. Mahon testified that the prior-art reference Togawa discloses a clear-text encryption scheme identifier within the meaning of the ’817 patent. Hr’g Tr. at 1542:18-1543:7. And as to the fourth and final part, Dr. Mahon admitted that the prior-art reference “Forsberg does disclose sending a public key identifier along with the encrypted IMSI,” and it further discloses the public key identifier being sent in clear-text. Hr’g Tr. at 1540:18-1541:9. As Dr. Bims explained, and as described in more detail below, these SUCI parts were indeed well-known in the prior art. Hr’g Tr. at 1278:21-1283:7 (Ground 1), 1286:14-1289:12 (Ground 2); RDX-2.33-38; RDX-2.43-48.

The second aspect (transmitting the SUCI) requires the UE transmit the SUCI “to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the encrypted part.” JX-0001, claims 10, 15; Hr’g Tr. at 272:1-13 (Dr. Mahon testifying as to SUCI transmission); RDX-0016.19. Dr. Bims testified (and Dr. Mahon did not dispute) that the image below accurately represents the claimed SUCI transmission path for all asserted claims:



[REDACTED]

RDX-2.13; Hr’g Tr. at 122:16-1227:6; JX-0001 at claims 10, 15. As explained further below, *under Ericsson’s infringement theory*, the claimed transmission path was disclosed in the prior art, including by the Nair reference. RX-0828.19; RX-0006.36; RDX-2.39; Hr’g Tr. at 1283:8-24. Separate from Ericsson’s infringement read, the Forsberg reference also discloses the claimed transmission path. Hr’g Tr. at 1289:13-1290:16; RX-0830.3, .5, .9, .10; RDX-2.49.

Asserted claim 13 depends from claim 10 and additionally recites “wherein the transmitting the SUCI to the authentication server comprises transmitting the SUCI to the authentication server in response to an identifier request message received from an Authentication and Mobility management Function, AMF, as part of a procedure for registering the UE with a wireless communication network.” JX-0001 at claim 13; Hr’g Tr. at 1284:5-12; RDX-2.41. It is undisputed that the prior art, including the Nair reference, discloses claim 13’s additional limitation. Hr’g Tr. at 1284:5-1285:5; RX-0828.22, .29; RX-0826.119; RDX-2.41 (Nair); JSUI § III.D.

Asserted claim 14 depends from claim 10 and additionally recites “wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme.” JX-0001 at claim 14; Hr’g Tr. at 1285:6-12; RDX-2.42. It is undisputed that the prior art, including 5G-Ensure, discloses claim 14’s additional limitation. Hr’g Tr. at 1285:6-1286:13; RX-0806.32-33; RDX-2.42; JSUI § III.F.

B. Level Of Ordinary Skill In The Art

There is no material dispute over the level of ordinary skill in the art. Lenovo contends a POSA would have had a master’s degree in electrical engineering, computer engineering, or computer science, or equivalent and at least three years of experience in the field of telecommunications or wireless systems. RDX-2.27; Hr’g Tr. at 1275:23-1276:4; RDX-2.27. Ericsson contends a POSA would have had a bachelor’s, rather than a master’s, degree. CDX-21.3; Hr’g Tr. at 1487:19-24 (Dr. Mahon testifying that “for the most part it’s the same”).

C. The ’817 Patent’s Asserted Claims Are Invalid Under 35 U.S.C. § 103

1. Overview Of The Prior Art

a. Nair

U.S. Pat. App. Publ. No. 2018/0324585 (“Nair Publication”), filed on 10/26/2017 and published on 11/08/2018, claims priority to U.S. Provisional App. No. 62/502,266 (“Nair Provisional”), filed on 05/05/2017. RX-0832 (Nair Publ.) at Cover; RX-0828 (Nair Prov.) at 1; RDX-2.32; Hr’g Tr. at 1278:2-20. Nair is prior art under 35 U.S.C. § 102(a)(2).

Ericsson disputed Nair’s prior-art status in its pre-hearing brief (E’s PHB at 43), but did not do so at the Hearing. The Nair Provisional, filed on 5/5/2017 (Hr’g Tr. at 1278:10-12; RX-0828), pre-dates the ’817 patent’s earliest-claimed priority date (07/25/2017, *id.* at 1546:7-10). As Dr. Bims explained, while he “consider[ed] both the Nair provisional, RX-828, and the RX-832, Nair [publication] document in forming [his] opinion,” “*all* of [Dr. Bims’s Ground 1] invalidity opinions in this case [are] based on the Nair provisional,” and the Nair disclosure he discussed was from the Nair provisional. Hr’g Tr. at 1276:20-23, 1278:13-16.

Nair, titled “Privacy Indicators for Controlling Authentication Requests,” is directed to 5G. RX-0828; RX-0832; Hr’g Tr. at 1549:15-18. As Dr. Bims explained, Nair is “about improving the security of communication systems and, in particular, the subscription privacy of 5G networks.” Hr’g Tr. at 1276:16-19. Nair describes a process for concealing a UE’s SUPI during a UE authentication process by encrypting the user-specific information of a UE’s IMSI (i.e., the MSIN), while keeping the remaining IMSI information (e.g., the Mobile Network Code (MNC) and Mobile Country Code (MCC)) in clear-text. RX-0828.24-.25; *see also* RX-0832.10. Dr. Mahon agrees that Nair “is directed to privacy in cellular systems” and it “discloses in particular a system in which the MSIN of the IMSI is encrypted to protect subscriber privacy.” Hr’g Tr. at 1546:3-1547:4.

b. Forsberg

U.S. Pat. Appl. Publ. No. 2013/003971 (“Forsberg”) was filed on 09/13/2012 and

[REDACTED]

published on 01/03/2013. RX-0830 (Forsberg) at Cover; Hr’g Tr. at 1278:2-20. Forsberg is undisputed prior art under 35 U.S.C. §§ 102(a)(1) and (a)(2). *Id.* at 1535:5-7; JSUI § III.C.

Forsberg, titled “Identifiers in a Communication System,” describes a process for concealing a UE’s SUPI during a UE authentication process by encrypting the user-specific information of a UE’s IMSI, while keeping the remaining IMSI information in clear-text. RX-0830.1, .9; Hr’g Tr. at 1276:24-1277:6; RDX-2.29; RX-0830. As Dr. Bims explained, Forsberg is “about improving the security in communication networks by encrypting an identifier that is decrypted in the network.” Hr’g Tr. at 1277:3-6; RDX-2.29; RX-0830.9. Forsberg discloses a UE transmitting its encrypted MSIN and a clear-text home network identifier (MCC+MNC) and public key identifier to an authentication server, which uses the clear-text information to contact the UE’s home network to decrypt the UE’s identity. RX-0830.10-.11. The home network uses the key identifier to identify the secret key that is paired with the public key that was used to encrypt the MSIN portion of the IMSI and uses that secret key to decrypt the encrypted MSIN. RX-0830.10. Dr. Mahon agrees that “Forsberg concerns a cellular wireless system,” it is “directed to protecting subscriber information in such a system,” and “it discloses a technique ... of encrypting an identifier and sending it to the network.” Hr’g Tr. at 1535:14-1536:3.

c. Togawa

U.S. Pat. No. 8,005,219 (“Togawa”) was filed on 06/23/2007 and issued on 08/23/2011. RX-0834 (Togawa) at Cover; Hr’g Tr. at 1278:2-20. Togawa is undisputed prior art under 35 U.S.C. §§ 102(a)(1) and 102(a)(2). *Id.* at 1535:11-13; JSUI § III.C.

Togawa, titled “Data Decryption Apparatus and Data Encryption Apparatus,” describes an encryption apparatus and a decryption apparatus for encrypting and decrypting transmitted UE data, whereby encryption information, including an “encryption-method ID” that identifies the encryption scheme used to encrypt the data, is embedded within transmitted data. RX-0834.1, .14,

[REDACTED]

.26-.27; Hr’g Tr. at 1277:7-14; RDX-2.30. As Dr. Bims explained, Togawa is “about improving the security of communication networks, just the like ’817 patent.” Hr’g Tr. at 1277:12-14. Dr. Mahon agrees that “Togawa discloses encrypting data and transmitting encrypted data in the context of phone calls.” Hr’g Tr. at 1543:15-18.

d. 5G-Ensure

5G-Ensure Deliverable D3.1, “5G-PPP security enablers technical roadmap” (early version) (“5G-Ensure”) published on 11/03/2016. RX-0806 (5G-Ensure) at 1; Hr’g Tr. at 1278:2-20. 5G-Ensure is undisputed prior art under 35 U.S.C. §§ 102(a)(1) and 102(a)(2). JSUI § III.C.

As Dr. Bims explained, “[t]he 5G-Ensure reference is a document generated by a consortium of companies to describe the improvements to security in 5G networks by using an encryption scheme for user identifiers.” Hr’g Tr. at 1277:15-23; RDX-2.31; RX-0806. 5G-Ensure describes a method of protecting user identifiers (e.g., IMSIs) using encryption, describes the benefits of encryption schemes based on elliptic curve parings, and further describes that other information, including the associated MNC and MCC, would need to be left unencrypted within the identifier to aid the serving network in locating the home network. RX-0806.32-33.

2. Ground 1: Nair In Combination With Forsberg, Togawa, and 5G-Ensure Invalidates All ’817 Patent Asserted Claims

a. Nair, Forsberg, and Togawa Invalidates Claims 10, 13, and 15

i. Independent Claims 10 and 15

(A) [10.A]/[15.A]

To the extent the preambles are limiting, Nair indisputably discloses them. JSUI § III.D. Nair discloses a UE and a method performed by a UE. Dr. Mahon admits “Nair discloses a UE ... sending a registration request that includes an encrypted IMSI.” Hr’g Tr. at 1548:2-6; RX-0828.19.

Nair discloses the UE concealing a SUPI, wherein the SUPI is a globally unique identifier

[REDACTED]

allocated to a subscriber and the SUPI comprises a home network identifier identifying a home network of the subscriber and a subscription identifier identifying a subscription within the home network. Dr. Mahon admits Nair discloses “a system in which the MSIN of the IMSI is encrypted to protect subscriber privacy”; he admits an encrypted IMSI “is a globally unique identifier allocated to a subscriber”; and he admits he “is relying on an IMSI-based SUPI,” which “ha[s] the same contents” as an IMSI, including “a home network identifier that identifies the home network of the subscriber” and “a subscription identifier that identifies the subscription within the home network.” Hr’g Tr. at 1532:4-16, 1536:6-9, 1546:11-16; *see also* Hr’g Tr. at 181:18-182:11; (Dr. Mahon testifying that an IMSI-based SUPI “meet[s] this element”); Hr’g Tr. at 182:12-183:10 (same); Hr’g Tr. at 186:8-22 (same); Hr’g Tr. at 265:22-266:1 (same); Hr’g Tr. at 264:8-20 (Dr. Mahon testifying that an IMSI is “an example of a long-term subscription identifier” as claimed, and admitting, “IMSI’s were known long-term subscriber identifiers before the ’817 patent”).

(B) [15.B]

Nair indisputably discloses this limitation. JSUS § III.D. As Dr. Mahon admits, “Nair discloses a UE ... sending a registration request that includes an encrypted IMSI.” Hr’g Tr. at 1548:2-6; *see* RX-0828.19 (Nair Fig. 6 discloses a UE transmitting an encrypted IMSI); Hr’g Tr. at 1549:15-18 (Mahon admitting Nair is directed to 5G). As Dr. Mahon also admits, “the UE ... is your phone, user equipment,” and “it’s uncontroversial that [user equipment] processors contain circuitry and that there is also memory chips on the processor, so it’s uncontroversial there’s memory circuitry there,” and “it’s reasonable to conclude that [the UE] contains processing circuitry and memory circuitry from the perspective of a POSITA.” Hr’g Tr. at 172:24-173:7, 183:11-184:7 (Dr. Mahon testifying as to CDX-8.21-22); *id.* at 184:14-19 (Dr. Mahon testifying, “it’s uncontroversial that ... the Samsung DI products contain processing circuitry and memory circuitry” because they are UE); *id.* at 272:25-273:5 (Dr. Mahon agreeing that “mobile phones”

[REDACTED]

are “what the [’817] patent ... would call a UE”); *id.* at 276:9-18 (same).

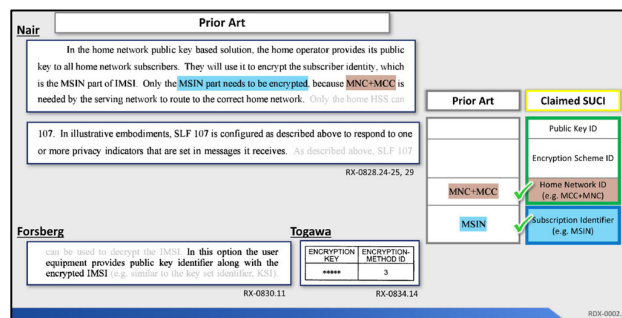
(C) [10.B]/[15.C]

Nair in combination with Forsberg and Togawa teaches these limitations. Nair discloses a UE generating an identity response message that contains an encrypted subscription identifier (MSIN) and a clear-text home network identifier (MNC+MCC). RDX-2.35. While Nair does not explicitly disclose a clear-text encryption scheme identifier, a POSA would have understood that Nair suggests or contemplates one by disclosing “one or more privacy indicators,” RX-0828.29; Togawa explicitly discloses one by disclosing a clear-text “encryption method ID,” RX-0834.14; and Nair’s one or more privacy indicators disclosure provides a motivation to a POSA to combine Togawa’s encryption scheme identifier with Nair with a reasonable expectation of success. Hr’g Tr. at 1279:23-1281:11; RDX-2.36. And, while Nair does not explicitly disclose a clear-text public key identifier, a POSA would have understood that Nair suggests or contemplates one by disclosing a “public key based solution” in which “the home operator provides its public key to all home network subscribers,” RX-0828.24-25; Forsberg explicitly discloses one by disclosing a “public key identifier,” RX-0830.11; and Nair’s public key based solution disclosure provides a POSA a motivation to combine Forsberg’s public key identifier with Nair with a reasonable expectation of success. Hr’g Tr. at 1281:12-1282:19; RDX-2.37.

(1) UE generating a subscription concealed identifier (SUCI) which comprises an encrypted part and a clear-text part wherein a) the encrypted part comprises the subscription identifier and b) the clear-text part comprises i) the home network identifier

Nair discloses a UE generating an identity response message that comprises an encrypted part and a clear-text part wherein a) the encrypted part comprises the subscription identifier and b) the clear-text part comprises i) the home network identifier. Dr. Mahon admits that Nair “discloses ... a system in which the MSIN of the IMSI is encrypted to protect subscriber privacy,” and, in

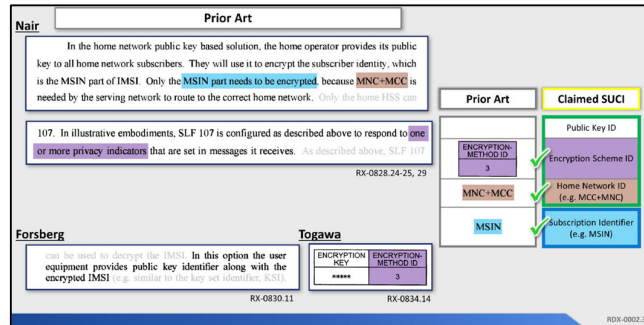
particular, in which the UE identity message includes “an encrypted part with an MSIN and a clear-text part with a home network identifier.” Hr’g Tr. at 1546:11-16, 1548:2-22; RX-0828.24-25 (“Only the MSIN part needs to be encrypted, because MNC+MCC is needed by the serving network to route to the correct home network.”). An encrypted MSIN is an encrypted subscription identifier as claimed. Hr’g Tr. at 269:2-17; RDX-0016.13. As Dr. Bims explained, Nair therefore discloses the UE generating an identity response message that contains an encrypted part comprising a subscription identifier and a clear-text part comprising a home network identifier:



Hr’g Tr. at 1279:9-22; RDX-2.34-35; RX-0828.24-25, 29.

(2) ii) an encryption scheme identifier

Nair in combination with Togawa teaches the clear-text part comprises ii) an encryption scheme identifier. While Nair does not explicitly disclose a clear-text encryption scheme identifier, incorporating one would have been obvious in view of Togawa. As Dr. Mahon admits, “Nair ... discloses one or more privacy indicators” or “privacy flag[s],” which “indicate[] whether or not encryption is turned on.” Hr’g Tr. at 1548:23-1549:10. As Dr. Bims explained, Nair’s disclosure of “multiple privacy indicators imply to a [POSA] that an encryption scheme is being used when privacy is enabled,” but “Nair does not disclose what [type of] encryption scheme is used when privacy is enabled. And that’s why a [POSA] would look to Togawa to bring an express description of the encryption scheme that is used”:



Hr’g Tr. at 1278:23-1280:14; RDX-2.36; RX-0828.24-25, 29.

Togawa discloses a clear-text encryption scheme identifier within the meaning of the ’817 patent. As Dr. Bims explained, “Togawa discloses an encryption method ID, which is the encryption scheme ID [in] the claimed SUCI.” Hr’g Tr. at 1280:15-18; RDX-2.36; RX-0834.14. Likewise, Dr. Mahon testified that “Togawa, discloses an encryption scheme identifier within the meaning of the ’817 patent.” Hr’g Tr. at 1542:18-1543:7.

A POSA would have been motivated to incorporate Togawa’s clear-text encryption scheme identifier into Nair. As Dr. Bims explained, both Nair and Togawa are directed to the same field and problem: Nair is “about improving the security of communication systems and, in particular, the subscription privacy of 5G networks,” Hr’g Tr. at 1276:16-19, and Togawa is “about improving the security of communication networks, just the like ’817 patent,” Hr’g Tr. at 1277:12-14. As Dr. Bims explained, “because Nair does not expressly disclose the [type of] encryption scheme that is associated with [its] privacy indicators, it means that the de-concealing server would not know what encryption scheme [type] is being used and would have to do an exhaustive search to determine what encryption scheme is associated with a privacy indicator. And because of this, a [POSA] would look to address this issue by combining Nair with Togawa so that the network can know what [type of] encryption scheme is associated with what privacy indicator.” Hr’g Tr. at 1280:19-1281:7. Dr. Bims further testified that a POSA would have had a reasonable expectation

[REDACTED]

of success combining Togawa's encryption scheme identifier with Nair. Hr'g Tr. at 1281:8-11.

Ericsson disagrees because, according to Dr. Mahon, Togawa is different in that it concerns encrypted user data embedded in a voice signal. Hr'g Tr. at 1497:7-22, 1503:15-1505:3. But as Dr. Bims explained, "[u]ser data can be transmitted through a voice signal, but it's still user data," *id.* at 1321:10-22, and as Dr. Mahon admits, Nair is directed to 5G and "Togawa discloses encrypting data and transmitting encrypted data in the context of phone calls," *id.* at 1543:15-18, 1549:15-18. Indeed, Dr. Mahon's testimony supports adding Togawa's encryption method ID to Nair's encrypted identity response message. As Dr. Mahon testified, if an identity response message contains an encrypted subscriber ID, a POSA would have understood that a clear-text encryption scheme ID is needed for the network to know how to decrypt it:

[I]f I just chose an encryption scheme, there's lots of them out there, and encrypted my permanent identifier with it and sent it on its merry way to the network, ***the network is going to have no idea how to decrypt it, because, again, these are typically symmetric, you need to know what algorithm was used to encrypt it in order to decrypt it.***

Hr'g Tr. at 187:18-188:1. Togawa's disclosure solves the problem above. Dr. Bims also agrees, and testified that a POSA would have understood that Nair's disclosure of providing "one or more privacy indicators" with an encrypted subscription ID suggests to a POSA that Nair is using an encryption scheme ID and, to the extent there was any uncertainty about its use, a POSA would have been motivated to allow the network to efficiently decrypt Nair's encrypted subscription ID by incorporating Togawa's encryption scheme ID. Hr'g Tr. at 1280:19-1281:7.

(3) iii) a public key identifier

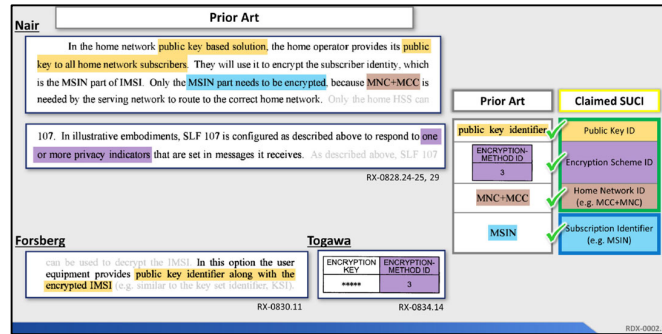
Nair in combination with Forsberg teaches the clear-text part comprises iii) a public key identifier. While Nair does not explicitly disclose a clear-text public key ID, as Dr. Bims explained, "Nair discloses a public-key-based solution in which a home operator provides its public key to all home network subscribers." Hr'g Tr. at 1281:12-17; RX-0828.24-25. Forsberg discloses a

[REDACTED]

clear-text public key ID as claimed. As Dr. Bims explained, “Forsberg expressly discloses a public key identifier that is provided by user equipment along with an encrypted IMSI.” Hr’g Tr. at 1281:21-25. Dr. Mahon likewise admitted that “Forsberg does disclose sending a [clear-text] public key identifier along with the encrypted IMSI.” Hr’g Tr. at 1540:18-1541:6; *see also id.* at 1539:9-13 (Dr. Mahon admitting Forsberg “certainly discloses the public key ID”).

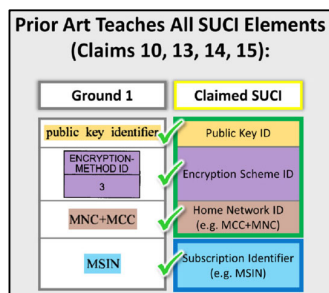
A POSA would have been motivated to add Forsberg’s clear-text public key ID to Nair. As Dr. Bims explained, Nair and Forsberg are directed to the same field and problem. Nair is “about improving the security of communication systems and, in particular, the subscription privacy of 5G networks,” Hr’g Tr. at 1276:16-19, and Forsberg is likewise “about improving the security in communication networks by encrypting an identifier that is decrypted in the network,” Hr’g Tr. at 1277:3-6; RDX-2.29; RX-0830.9.

Ericsson disagrees because, according to Dr. Mahon, Nair and Forsberg are different. Hr’g Tr. at 1496:8-1497:14. But, Dr. Mahon’s dispute lacks credibility. Indeed, Dr. Mahon agrees that Nair and Forsberg are both “directed to privacy in cellular systems” and are therefore both “in in the same field.” Hr’g Tr. at 1547:2-19. As Dr. Bims explained, “a [POSA] reading Nair would understand that, when a home operator is providing its public key to all of its home network subscribers, ... a public key ID would be involved. But a [POSA] would have to consider multiple ways of involving a public key ID. Forsberg solves that problem by expressly disclosing a public key identifier that is provided along with the encrypted IMSI as a solution to that problem”:



Hr’g Tr. at 1282:1-13; RDX-2.37; RX-0828.24-25, 29; RX-0830.11. Dr. Bims further testified that a POSA would have had a reasonable expectation of success. Hr’g Tr. at 1282:14-17.

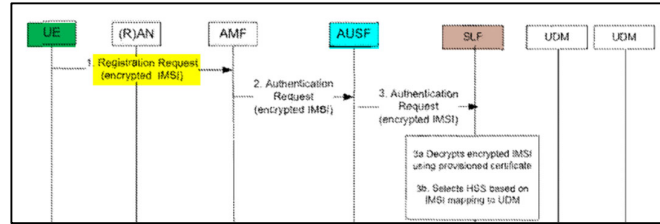
The Nair-Forsberg-Togawa combination teaches a UE generating the claimed SUCI:



RDX-2.38. As Dr. Bims testified, “[a]s you can see from this side-by-side comparison,” the prior-art disclosures and the claimed SUCI components “are word for word almost identical.” Hr’g Tr. at 1282:25-1283:3; RDX-2.37-38.

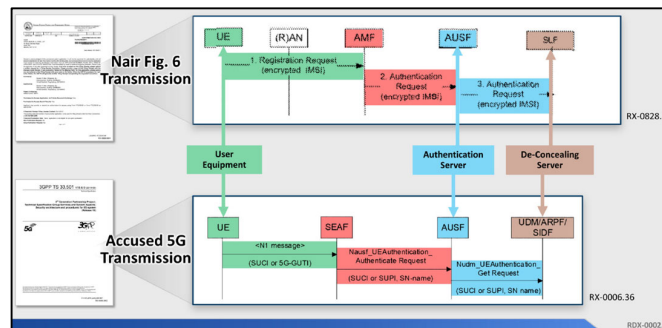
(D) [10.C]/[15.D]

Nair discloses the claimed transmission path *under Ericsson’s infringement theory*. As shown in Nair Figure 6, below, and as Dr. Mahon admits, Nair discloses a UE (green) transmitting a registration request message containing the encrypted IMSI (yellow), “[a]nd Nair discloses that the authentication server AUSF [(blue)] in Nair receives the encrypted IMSI”:



RX-0828 at Fig. 6; RDX-0027.19; Hr’g Tr. at 1549:19-1550:9. Nair’s disclosed AUSF is an authentication server as claimed. As Dr. Mahon testified, “there is not” “any dispute here that the AUSF [in] 5G is an authentication server,” Hr’g Tr. at 189:9-11, “for the purposes of infringement, [Dr. Mahon is] reading the authentication server on the 5G AUSF authentication server function,” Nair Figure 6 “is directed to the 5G nodes,” Nair “does have the AUSF listed,” and “Nair’s AUSF is an authentication server function.” Hr’g Tr. at 1549:11-1550:1. Further, as shown in Nair Figure 6, above, and as Dr. Mahon admits, “Nair discloses that the authentication server AUSF [(blue)] in Nair receives the encrypted IMSI and forwards that encrypted IMSI to an SLF [(brown)],” and “the SLF will decrypt the encrypted MSIN.” Hr’g Tr. at 1550:5-12.

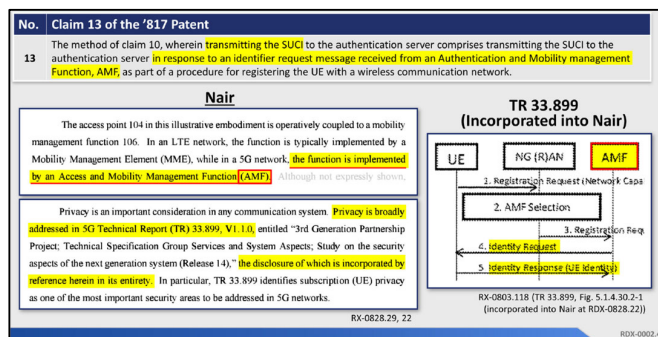
As Dr. Bims explained, the “accused 5G transmission is mimicking a disclosure in Nair Fig. 6,” such that “Nair disclose[s] the claimed SUCI transmission under Ericsson’s infringement theory” and therefore “[if] the accused products meet the SUCI transmission path,” then “Nair discloses that limitation”:



RX-0828.19; RX-0006.36; RDX-2.39; Hr’g Tr. at 1283:8-24.

ii. Dependent Claim 13

The Nair-Forsberg-Togawa combination renders claim 10 obvious, and Nair indisputably discloses the additional claim 13 limitation: the UE transmission is “in response to an identifier request message received from an Authentication and Mobility management Function, AMF, as part of a procedure for registering the UE with a wireless communication network.” JX-0001 at claim 13; JSUI § III.D. As Dr. Bims testified, “Nair discloses an access and mobility management function, or AMF, and goes into further details about [it],” including by discussing 5G Technical Report (TR) 33.899, V1.1.0 (RX-0826)², “the disclosure of which [Nair] ... incorporate[s] by reference ... in its entirety”:



Hr’g Tr. at 1284:5-23; RX-0828.29, 22; RDX-2.41. Dr. Bims further testified that TR 33.899 V1.1.0 discloses in Fig. 5.1.4.30.2-1 that “the AMF transmits an identity request to the UE prior to the UE responding by transmitting the SUCI,” which teaches the additional claim 13 limitation. Hr’g Tr. at 1284:24-1285:5; RX-0826.119.

b. Nair, Forsberg, Togawa, and 5G-Ensure Invalidates Claim 14

i. Dependent Claim 14

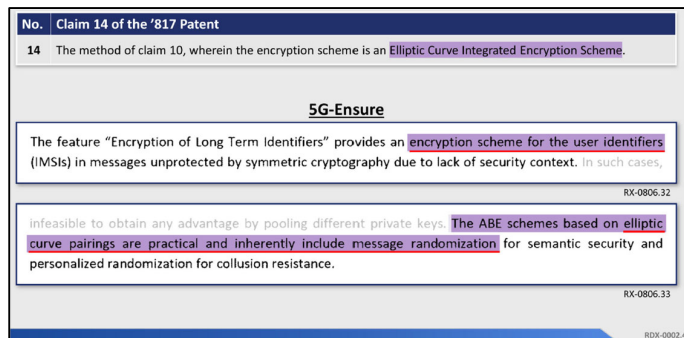
The Nair-Forsberg-Togawa combination renders claim 10 obvious, and 5G-Ensure

² RDX-2.41 inadvertently cites RX-0803 (TR 33.899, V1.2.0), rather than RX-0826 (TR 33.899, V1.1.0). Dr. Bims clarified during his testimony that his opinions are based on RX-0826.119 (TR 33.899, V1.1.0), which is incorporated in the Nair reference. Hr’g Tr. at 1284:13-1285:5, 1321:23-1323:24.

[REDACTED]

indisputably discloses the additional limitation of claim 14—namely, “wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme” (ECIES). JX-0001 at claim 14; JSUI § III.F; Hr’g Tr. at 1508:1-4 (Dr. Mahon testifying that 5G-Ensure is “that ECIES encryption algorithm that [Dr. Bims] uses” in his invalidity opinions). As Dr. Bims testified, “5G-Ensure discloses an encryption scheme for user identifiers that is based on elliptic curve pairings,” which teaches the additional limitation of claim 14. Hr’g Tr. at 1285:6-16; RX-0806.32-33; RDX-2.42.

A POSA would have been motivated to incorporate 5G-Ensure’s ECIES teachings with the combined teachings of Nair, Forsberg, and Togawa and would have had a reasonable expectation of success. As Dr. Bims testified, “in Nair it describes encrypting an MSIN, but Nair does not disclose the particular encryption scheme to encrypt the MSIN. So a [POSA] would look to 5G-Ensure for its teachings of a specific encryption scheme that is based on elliptic curve parings.” Hr’g Tr. at 1285:17-24. Dr. Bims further testified that 5G-Ensure discloses that elliptic curve parings are “practical” and “inherently include[] ... message randomization,” which “are two reasons, among others, such as the smaller size of the key, that would motivate a [POSA] to apply these elliptic curve pairings” with a reasonable expectation of success:



Hr’g Tr. at 1285:25-1286:9; RDX-2.42; RX-0806.32-33.

Ericsson disagrees, but Dr. Mahon’s arguments are conclusory and unexplained. He opines that 5G-Ensure “doesn’t provide, for example, a nice architecture where you can grab the different

[REDACTED]

structures and integrate them all in together for a person of ordinary skill in the art to understand and say, oh, yeah, if we put it together this way, it's going to work, and also it would achieve the same results, for example." Hr'g Tr. at 1508:5-12. Dr. Mahon's opinion is not tied to any claim limitation and it fails to rebut Dr. Bims's showing that using 5G-Ensure's teachings would have been logical and straightforward: Nair teaches encrypting the MSIN but doesn't teach which encryption scheme to use, which would have motivated a POSA to look for references, such as 5G-Ensure, which teaches a well-known encryption scheme (ECIES) and further teaches well-known benefits of that encryption scheme, including practicality, inherent message randomization, and a smaller key size, all of which would have given a POSA a reason to make the combination and a reasonable expectation of success. Hr'g Tr. at 1285:17-1286:9; RX-0806.32-33; RDX-2.42.

3. Ground 2: Forsberg In Combination With Togawa And 5G-Ensure Invalidates All '817 Patent Asserted Claims

a. Forsberg and Togawa Invalidates Claims 10, 13, and 15

i. Independent Claims 10 and 15

(A) [10.A]/[15.A]

To the extent the preambles are limiting, Forsberg indisputably discloses them. JSUI § III.E. As, Dr. Mahon admits, "Forsberg discloses that a UE ... generates a user identity response" and Dr. Mahon further admits that "Forsberg discloses that the UE transmits this user identity response." Hr'g Tr. at 1536:18-21, 1544:11-17; RX-0830.3, .5, .9, .10.

Forsberg discloses the UE concealing a SUPI, wherein the SUPI is a globally unique identifier allocated to a subscriber and the SUPI comprises a home network identifier identifying a home network of the subscriber and a subscription identifier identifying a subscription within the home network. As Dr. Mahon admits, Forsberg "discloses a technique ... of encrypting an identifier and sending it to the network," the identifier being "[a]n encrypted IMSI," which "is a

[REDACTED]

globally unique identifier allocated to a subscriber,” and, in particular, “Forsberg discloses ... encrypting the MSIN of the IMSI.” Hr’g Tr. at 1535:14-1536:13; *id.* at 1536:10-21 (Dr. Mahon agreeing that, as shown on RDX-27.5, RX-0830, Fig. 4, “Forsberg discloses that a UE ... generates a user identity response”); *see also id.* at. 181:18-182:11, 182:12-183:10, 186:8-22, 264:8-20.

(B) [15.B]

Forsberg indisputably discloses this limitation. JSUI § III.E. As Dr. Mahon admits, Forsberg “discloses a technique ... of encrypting an identifier and sending it to the network,” the identifier being “[a]n encrypted IMSI,” which “is a globally unique identifier allocated to a subscriber,” and, in particular, “Forsberg discloses ... encrypting the MSIN of the IMSI.” Hr’g Tr. at 1535:14-1536:13. Forsberg discloses that a UE performs the encryption and transmission. RX-0830, Fig. 4. And, as Dr. Mahon also admits, “it’s uncontroversial that [UE] processors contain circuitry and that there is also memory chips on the processor, so it’s uncontroversial there’s memory circuitry there,” and “it’s reasonable to conclude that it contains processing circuitry and memory circuitry from the perspective of a POSITA.” Hr’g Tr. at 172:24-173:7, 183:11-184:7 (Mahon testifying regarding CDX-8.21-22); *see also id.* at 184:14-19, 272:25-273:5, 276:9-18.

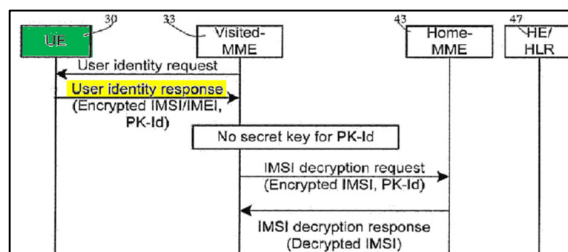
(C) [10.B]/[15.C]

Forsberg in combination with Togawa teaches these limitations. Forsberg discloses a UE generating an identity response message that contains three of the four claimed SUCI components: an encrypted subscription ID (MSIN), a clear-text home network ID (MNC+MCC), and a clear-text public key ID. RDX-2.46 (citing RX-0830.10-.11). While Forsberg does not explicitly disclose a clear-text encryption scheme ID, a POSA would have understood Forsberg suggests or contemplates one by disclosing an “encrypted IMSI,” RX-0830.10-11; and Togawa explicitly discloses one: a clear-text “encryption method ID,” RX-0834.14. Forsberg’s encrypted IMSI disclosure would have motivated a POSA to combine Togawa’s encryption scheme ID disclosure

with Forsberg with a reasonable expectation of success. Hr’g Tr. at 1287:15-1288:24; RDX-2.47.

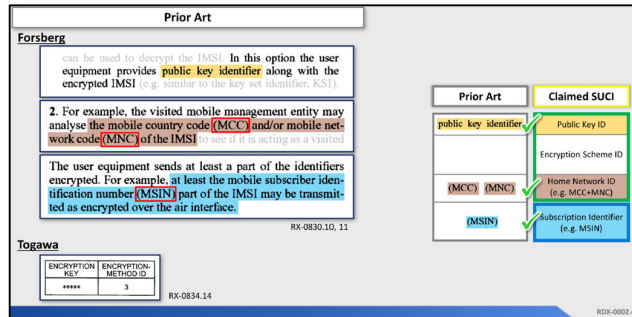
(1) UE generating a subscription concealed identifier (SUCI) which comprises an encrypted part and a clear-text part, wherein a) the encrypted part comprises the subscription identifier and b) the clear-text part comprises i) the home network identifier and iii) a public key identifier

Forsberg discloses a UE generating an identity response message that comprises an encrypted part and a clear-text part wherein a) the encrypted part comprises the subscription ID and b) the clear-text part comprises i) the home network ID and iii) a public key ID. As Dr. Mahon agreed, and as Forsberg Fig. 4 below shows, “Forsberg discloses that a UE, which we see in green, generates a user identity response, which we have colored in yellow” and “Forsberg discloses that that user identity response comprises an encrypted part and a clear-text part”:



Hr’g Tr. at 1536:10-1537:5; RDX-0027.5; Hr’g Tr. at 1536:10-1537:5 (Dr. Mahon admitting, “certainly the [Forsberg] IMSI is encrypted and the public key identifier is not encrypted”).

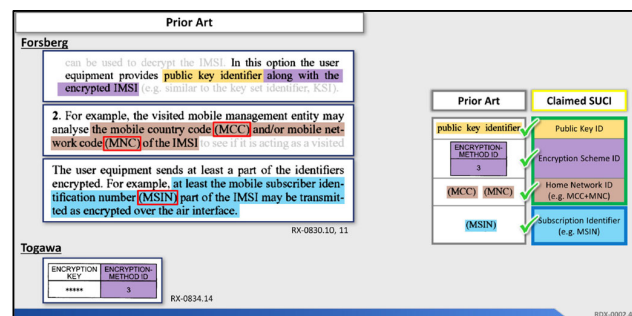
As Dr. Mahon also admitted, “Forsberg does disclose sending a public key identifier along with the encrypted IMSI,” and the public key ID is “not encrypted” but is “in the clear-text part of the user identity response.” *Id.* at 1540:18-1541:6; *see also* RDX-0027.10. And as Dr. Bims explained, “Forsberg discloses that the MSIN is transmitted in an encrypted form, and that matches up to the subscription identifier in the encrypted part of the claimed SUCI,” “Forsberg discloses and MCC and MNC combination, which is the home network ID in the claimed SUCI,” and “Forsberg discloses that the user equipment will provide a public key identifier along with the encrypted IMSI. So Forsberg is disclosing the public key ID in the claimed SUCI”:



Hr'g Tr. at 1286:19-1287:14; RDX-2.44-46; RX-0830.10-11.

(2) ii) an encryption scheme identifier

Forsberg in combination with Togawa teaches the clear-text part comprises an encryption scheme ID. While Forsberg does not explicitly disclose a clear-text encryption scheme ID, one would have been obvious in view of Togawa. As Dr. Bims explained, “Forsberg discloses that there is an encrypted IMSI that is provided along with the public key identifier,” and “Togawa describes an encryption scheme identifier that can identify the particular encryption scheme ... that can be incorporated into Forsberg”:



Hr'g Tr. at 1287:15-25; RDX-2.47; RX-0830.10-11; RX-0834.14. As explained above, and as Dr. Mahon testified, Togawa discloses an encryption scheme ID within the meaning of the '817 patent. Hr'g Tr. at 1542:18-1543:7; *see also* RDX-0027.11.

A POSA would have been motivated to add Togawa's clear-text encryption scheme ID to Forsberg. As Dr. Bims explained, Forsberg and Togawa are directed to the same field and problem:

[REDACTED]

Forsberg is “about improving the security in communication networks by encrypting an identifier that is decrypted in the network,” Hr’g Tr. at 1277:3-6; RDX-2.29; RX-0830.9, and Togawa is “about improving the security of communication networks, just the like ’817 patent,” Hr’g Tr. at 1277:12-14. Further, Dr. Mahon agrees that “Togawa discloses encrypting data and transmitting encrypted data in the context of phone calls.” Hr’g Tr. at 1543:15-18. As Dr. Bims explained, “Forsberg teaches that there is an encrypted IMSI, but Forsberg does not teach what [type of] encryption scheme is used. And so a [POSA] would not know what encryption scheme [type] to apply so that the network will know what encryption scheme to decrypt.” Hr’g Tr. at 1288:1-9. As Dr. Bims further explained, this would have caused a POSA to look to Togawa:

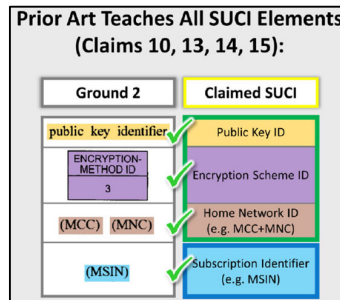
[W]ith the Togawa reference, it teaches the use of an encryption scheme ID that can identify in particular the encryption scheme used within the Forsberg teaching, which then allows for a couple of advantages. One is that, if an encryption scheme is compromised, then the combined system can then move to a different encryption scheme. And it also provides for the de-concealing server to be able to expressly know what encryption scheme is used so it does not have to do an exhaustive search to determine what that encryption scheme is.

Hr’g Tr. at 1288:10-20. As Dr. Bims explained, a POSA would have been successful incorporating Togawa’s encryption scheme identifier teachings into Forsberg. Hr’g Tr. at 1288:21-24.

Ericsson disagrees because, according to Dr. Mahon, Togawa is different in that it concerns encrypted user data embedded in a voice signal. Hr’g Tr. at 1497:7-22, 1503:15-1505:3. But as Dr. Bims explained, “[u]ser data can be transmitted through a voice signal, but it’s still user data.” *Id.* at 1321:10-22. As Dr. Mahon admits, “Forsberg concerns a cellular wireless system” and is “directed to protecting subscriber information in such a system,” *id.* at 1535:14-1536:3, and “Togawa discloses encrypting data and transmitting encrypted data in the context of phone calls,” *id.* at 1543:15-18, 1549:15-18. And, as explained above, Dr. Mahon’s testimony that sending an encrypted subscriber ID to the network without an encryption scheme ID would not work (without “know[ing] what algorithm was used to encrypt it,” “the network is going to have no idea how to

decrypt it,” *id.* at 187:18-188:1) supports this combination. As Dr. Bims explained, a POSA would have been motivated to incorporate Togawa to address this problem in Forsberg. *Id.* at 1288:1-24.

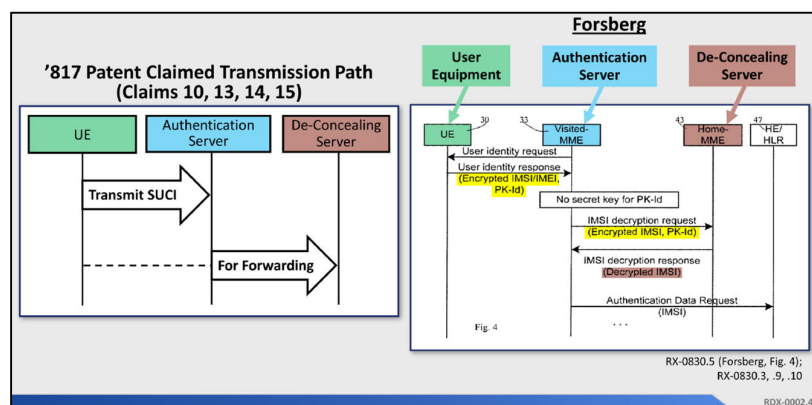
The Forsberg-Togawa combination teaches these limitations:



RDX-2.48. As Dr. Bims explained, the teachings of Forsberg and Togawa “match up with the claimed SUCI almost word for word.” Hr’g Tr. at 1288:25-1289:12; RDX-2.47-48.

(D) [10.C]/[15.D]

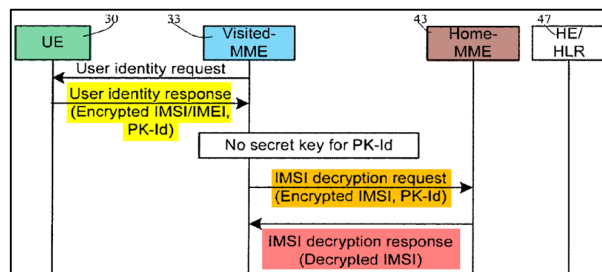
Forsberg discloses these limitations and Ericsson cannot credibly argue otherwise. As shown in RDX-2.49 below, Forsberg discloses a “UE” (green) transmitting the user identity response message containing the “Encrypted IMSI” (yellow) to a “Visited-MME” (blue), and that encrypted IMSI is then forwarded to a “Home-MME” (brown), which “Decrypt[s]” it (brown):



RDX-2.49 (annotating RX-0830.5 and further citing RX-0830.3, .9, .10). As Dr. Bims explained, “in Forsberg ... the Visited-MME is playing the role of the authentication server” and as shown in

Forsberg Fig. 4, depicted above, the UE “transmits an encrypted IMSI to the Visited-MME, which is an authentication server.” Hr’g Tr. at 1289:13-1290:7. “[T]he encrypted IMSI that is transmitted to the Visited-MME is then forwarded to the de-concealing server, which is labeled Home-MME in the Forsberg figure.” *Id.* at 1290:7-13. As shown above, Forsberg’s Home-MME can decrypt the encrypted part: the Home-MME “Decrypt[s]” the MSIN part of the IMSI. RX-0830.5.

Dr. Mahon does not dispute that Forsberg Fig. 4 discloses this transmission and forwarding of the encrypted IMSI and public key ID. He does not dispute that “the user identity response as shown in Fig. 4 of Forsberg includes a home network identifier” in addition to the encrypted IMSI (i.e., an encrypted subscription ID and a clear-text home network ID). Hr’g Tr. at 1539:5-1541:6. Dr. Mahon also does not dispute that, as shown in Fig. 4, depicted in RDX-002.13 below, “Forsberg discloses that the UE [(green)] transmits this user identity response [(yellow)],” and “the UE transmits the user identity response to a server that’s called the Visited-MME [(blue)]”:



RDX-0027.13 (annotating RX-0830.5); Hr’g Tr. at 1544:3-19. Further, Dr. Mahon agrees that, “[a]s shown in Figure 4 of Forsberg, that server, the Visited-MME, forwards the encrypted IMSI and public key identifier to another server called the Home-MME.” Hr’g Tr. at 1545:7-15. The Home-MME disclosed in Forsberg Figure 4 above is highlighted in brown, and the Visited-MME’s forwarding of the encrypted IMSI and public key identifier to the Home-MME is highlighted in orange. RDX-0027.13. Dr. Mahon further admitted that “if [the Home-MME] is contacted by the Visted-MME, ... it will do the decryption” of the encrypted IMSI, and Dr. Mahon agreed that

[REDACTED]

“Forsberg discloses that the Home-MME decrypts the MSIN portion of the IMSI” and sends the decrypted IMSI “back to the Visited-MME,” highlighted in red. Hr’g Tr. at 1545:16-1546:2.

Ericsson disagrees, and Dr. Mahon testified that he did not agree with Dr. Bims’s opinion that Forsberg’s Visited-MME and Home-MME are an authentication server and a de-concealing server as claimed, Hr’g Tr. at 1502:18-21, but Dr. Mahon did not explain why. Instead, his rebuttal of these limitations simply concluded that “[t]he disclosed functionality is not the same”:

Well, again, you’re comparing this, from my view, a muddled and I believe a person of ordinary skill in the art’s view of a muddled interpretation of how 4G worked and trying to apply it to a 5G system with the terminologies that the ’817 discloses -- the authentication server and de-concealing server. The disclosed functionality is not the same as disclosed on this slide [RDX-2.49].

Hr’g Tr. at 1502:18-1503:3. Dr. Mahon’s unexplained disagreement does not credibly rebut Dr. Bims’s showing that Forsberg discloses these limitations.

ii. Dependent Claim 13

The Forsberg-Togawa combination renders claim 10 obvious, and Forsberg discloses the additional claim 13 limitation. Dr. Mahon testified that “claim 13 require[s]” “transmitting the SUCI in response to an identifier request,” and he contends that the accused products infringe claim 13 because the 5G standard depicts a “[n]etwork node [that] sends an identity request to the phone” and “[t]he phone then responds by encrypting the permanent identifier and sending the SUCI back up to the network in response to that identifier request.” Hr’g Tr. at 192:17-193:6.

Forsberg provides the disclosure of claim 13 that Ericsson contends infringes. Forsberg discloses that, as “shown in detail in the flowcharts of FIGS. 4 and 5,” “a user equipment indicates its willingness to use communication services provided by a network,” “[t]he MME of the network then sends a message 1 to the user equipment to request for a user identity,” and “[t]he user equipment responds by returning a message 2 including an IMSI ... associated with the user equipment.” RX-0830.10; RDX-2.50. Forsberg further discloses that “[o]ther information, such as

[REDACTED]

information about public key identifiers may also be included in the response,” and “[t]he user equipment sends at least a part of the identifiers encrypted,” “[f]or example, at least the mobile subscriber identification number (MSIN) part of the IMSI may be transmitted as encrypted over the air interface.” *Id.* As Dr. Bims explained, Forsberg discloses the additional limitation of claim 13 in these paragraphs because “Forsberg teaches that the MME of the network will send a message to the user equipment requesting its user identity,” and “[i]n response, the user equipment will then transmit the SUCI back to the MME.” Hr’g Tr. at 1290:17-25; RDX-2.50.

Ericsson cannot credibly dispute these disclosures. While Dr. Mahon disagreed, he did not explain why. Instead, Dr. Mahon testified that Dr. Bims “call[ed] the Visited-MME both an AMF, which is what’s disclosed in the ’817 [patent], and the authentication server as disclosed in the ’817 [patent],” which Dr. Mahon concludes—without explanation—is not “possible.” Hr’g Tr. at 1503:4-14. Again, Dr. Mahon’s conclusory disagreement does not rebut Dr. Bims’s showing that Forsberg discloses the additional limitation of this claim.

b. Forsberg, Togawa, and 5G-Ensure Invalidates Claim 14

i. Dependent Claim 14

The Forsberg-Togawa combination renders claim 10 obvious, and 5G-Ensure indisputably discloses the additional claim 14 limitation: “wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme” (ECIES). JX-0001 at claim 14; JSUI § III.F; Hr’g Tr. at 1508:1-4 (Dr. Mahon testifying 5G-Ensure is “that ECIES encryption algorithm that [Dr. Bims] uses” in his invalidity opinions). As Dr. Bims testified, 5G-Ensure discloses the additional claim 14 limitation by disclosing “[t]he encryption scheme user identifier, which is based on elliptic curve pairings.” Hr’g Tr. at 1291:1-6; RX-0806.32-33; RDX-2.51; Hr’g Tr. at 1285:6-16.

A POSA would have been motivated to incorporate 5G-Ensure’s ECIES teachings with Forsberg and Togawa and would have reasonably expected success. As Dr. Bims testified, “the

[REDACTED]

Forsberg reference discloses an encrypted MSIN, but does not disclose what type of encryption to use,” and “[i]n 5G-Ensure, it expressly discloses elliptic curve pairings can be used.” Hr’g Tr. at 1291:7-17; RDX-2.51; *see also* Hr’g Tr. at 1285:6-13; RX-0806.32-33. Further, 5G-Ensure teaches that elliptic curve parings are “practical” and “inherently include[] ... message randomization,” which “are two reasons, among others, such as the smaller size of the key, that would motivate a [POSA] to apply these elliptic curve pairings” and would have provided a reasonable expectation of success. Hr’g Tr. at 1285:25-1286:6; RDX-2.51; RX-0806.32-33.

Dr. Mahon’s arguments against combining 5G-Ensure’s ECIES teachings with Forsberg and Togawa are the same conclusory and unexplained opinions he provided for Ground 1. Hr’g Tr. at 1508:5-12. As explained above, these opinions are not tied to any claim limitation and fail to rebut Dr. Bims’s showing that using 5G-Ensure’s teachings would have been logical and straightforward: Forsberg teaches encrypting the MSIN but doesn’t teach which encryption scheme to use, which would have caused a POSA to look for references, such as 5G-Ensure, which teaches a well-known encryption scheme (ECIES) and teaches its well-known benefits, including practicality, inherent message randomization, and a smaller key size, which would have given a POSA a reasonable expectation of success. *Id.* at 1285:25-1286:6; RDX-2.51; RX-0806.32-33.

4. There Are No Secondary Considerations Of Non-Obviousness

Ericsson’s secondary considerations arguments fail because there is no nexus between the evidence Ericsson presented and the claims of the ’817 patent. In its pre-hearing brief, Ericsson argued there is objective evidence of the ’817 patent solving a long-felt need, overcoming the failure of others, receiving industry praise, being copied, and being commercially successful. E’s PHB at 48-49. At trial, Dr. Mahon testified as to a single paper titled, “Security in 5G Networks – How 5G networks help Mitigate Location Tracking Vulnerability” (CX-2313), which he contended shows, in a single paragraph highlighted on CDX-21.6, that “people who work in the

[REDACTED]

security area[] identified [the SUCI] as a key feature” because it states that “the SUCI was adopted ... as a key feature of modern 5G networks in a new model.” Hr’g Tr. at 1508:13-22. Yet, the very next sentence explains that the paper’s focus is on prior-disclosed technology, including: “the UE will encrypt the MSIN of the IMSI, which is the most critical aspect of the IMSI, while leaving the MCC and the MNC in plaintext to allow for easier routing through the 5G network.” CDX-21.6 (quoting CX2131, § IV). Praise of the prior art is not secondary considerations evidence.

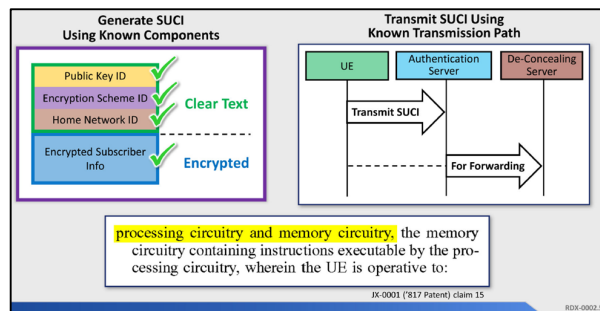
As Dr. Bims explained, this paper does not demonstrate secondary considerations of non-obviousness, nor is there any evidence of commercial success, long-felt-but-unsolved need, copying, or industry praise tied to the ’817 patent. Particularly, there is no evidence that the ’817 patent’s claims are incorporated in the 5G standard, and even if they were, Dr. Bims presented evidence showing that “there were around 350,000 patents grouped into more than 67,000 patent families found to be relevant to 5G,” and there is no evidence tying the success of 5G or the accused products to the one ’817 patent. Hr’g Tr. at 1291:18-1293:6; RDX-2.52; RX-1310.4.

D. The ’817 Patent’s Asserted Claims Are Invalid Under 35 U.S.C. § 101

The evidence shows that the ’817 patent’s asserted claims are invalid under 35 U.S.C. § 101 as claiming patent-ineligible subject matter. As Dr. Bims explained, the asserted claims “start out by describing concealing a subscription permanent identifier, and a [POSA] would know that concealing, as a general matter, is an intangible action and not related to anything other than an abstract idea.” Hr’g Tr. at 1293:7-16; RDX-2.53. These claims are thus directed to an abstract idea under step one of *Alice Corp. Pty. Ltd. v. CLS Bank Int’l.*, 573 U.S. 208, 217-18 (2014). Dr. Bims further explained that the asserted claims do not add anything inventive to this abstract idea because “the two parts of the claims are generating the SUCI and transmitting the SUCI. And as we’ve shown before, generating the SUCI uses known components and transmitting the SUCI uses a known transmission path. And on top of that, both generating the SUCI and transmitting the

SUCI can be implemented using common processing circuitry and memory circuitry.” Hr’g Tr. at 1293:17-1294:4; RDX-2.55. Thus, the asserted claims also fail *Alice* step two. 573 U.S. at 218.

Ericsson’s responsive arguments mischaracterize the facts and contravene long-established Supreme Court and Federal Circuit precedent. First, Ericsson and Dr. Mahon argued that Dr. Bims points to the preambles, but “ignore[s] the rest of the claims” which, according to Dr. Mahon, “disclose[] a particular structure and the SUCI is transmitted in a particular way.” Hr’g Tr. at 1495:1-25. Not so. Dr. Bims opined that the asserted claims are directed to the abstract idea of encrypted data *and* that what Dr. Mahon opined is the “particular structure” of the claimed SUCI is, in fact, a simple list of “known components” generated “using common processing circuitry and memory circuitry,” and the “particular way” the claimed SUCI is transmitted is, in fact, along a “known transmission path”:



Hr’g Tr. at 1293:17-1294:4; RDX-2.55.

Moreover, the Federal Circuit rejected this argument in *Yu v. Apple Inc.*, 1 F.4th 1040, 1043-44 (Fed. Cir. 2021). In *Yu*, the patent owner argued that the at-issue claim, which was directed to producing an “enhanced” digital image by taking two images and comparing them, was patent eligible because it provided “a specific solution” to certain problems. *Id.* The Federal Circuit rejected this argument and affirmed a judgment that the claim was patent-ineligible because the claimed “solution to those problems [was] the abstract idea itself—to take one image and ‘enhance’

[REDACTED]

it with another.” *Id.* So, too, here. The ’817 patent’s asserted claims’ purported solution to the identified problem of unencrypted subscriber information being “expose[d],” is the abstract idea itself: “concealing a subscription permanent identifier (SUPI).” JX-0001 at 1:31-36, 2:57-65, claims 10, 13-14, 15; Hr’g Tr. at 1223:24-1224:16; RDX-2.7-8.

Second, Ericsson and Dr. Mahon argue that the asserted claims could not have been “implemented on then existing UEs” because, according to Dr. Mahon, “[t]he UE wouldn’t know how to calculate it” and “the network certainly wouldn’t know how to handle it.” Hr’g Tr. at 1496:1-7. But the ’817 patent does not purport to have invented novel processing circuitry that enables a UE to “calculate” the claimed SUCI. Instead, the asserted claims simply recite generic “processing circuitry and memory circuitry.” JX-0001 at claims 10, 15. This is precisely what the Supreme Court held insufficient in *Alice*, where the Court affirmed a judgment that method and system claims directed to computer-implemented intermediated settlement were invalid for claiming an abstract idea because “[t]he method claims recite[d] the abstract idea implemented on a generic computer,” and “the system claims recite[d] a handful of generic computer components configured to implement the same idea.” 573 U.S. at 226. So, too, here.

IV. THE ’669 PATENT

A. Introduction and Background

As in 4G and other predecessor technologies, 5G base stations and UEs communicate with each other over uplink (UE to base station) and downlink (base station to UE) channels. Hr’g Tr. (7/15/24) (Rangan), 1051:24-1053:23; RDX-6.36-37. The base station sends UEs information regarding the location and format of downlink data on the Physical Downlink Control Channel (PDCCH). *Id.* The downlink data itself is sent over the Physical Downlink Shared Channel (PDSCH), which is called “shared” because it may be used by multiple UEs. *Id.* The UE decodes the downlink data received over the PDSCH. *Id.* Generally, if the UE decodes the sent data without

Dated: August 16, 2024

Respectfully Submitted,

/s/ Paul F. Brinkman

Paul F. Brinkman, P.C.
Ed Donovan, P.C.
F. Christopher Mizzo, P.C.
Michael A. Pearson, Jr.
Abigail Lauer Litow
John R. Rhine
Nichole DeJulio
Diva Hollis
Karthik Ravishankar
Stephen DeSalvo
Patrick Arnett
Eric Speckhard
Kirkland & Ellis LLP
1301 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
Telephone: (202) 389-5000
Facsimile: (202) 389-5200

Greg S. Arovas, P.C.
Robert A. Appleby, P.C.
Todd M. Friedman, P.C.
Leslie M. Schmidt, P.C.
Alex Henriques, P.C.
Christopher DeCoro
Christopher T. Ilardi
Stephen C. DeSalvo
Peter Evangelatos
Zhikun (David) Jiang
Michael DelRossi
Robert Endrizzi
Andrew Lee
Kirkland & Ellis LLP
601 Lexington Avenue
New York, NY 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

Eric D. Hayes, P.C.
David Rokach
Adam Janes
Kirkland & Ellis LLP
333 West Wolf Point Plaza
Chicago, IL 60654



Telephone: (312) 862-2000
Facsimile: (312) 862-2200

Bao Nguyen
Kirkland & Ellis LLP
555 California Street
San Francisco, CA 94104
Telephone: (415) 439-1400
Facsimile: (415) 439-1500

Tiffany M. Knapp
Kirkland & Ellis LLP
200 Clarendon Street
Boston, MA 02116
Telephone: (617) 385-7500
Facsimile: (617) 385-7501

Ryan James Melde
Kirkland & Ellis LLP
401 Congress Avenue, Suite 2500
Austin, TX 78701
Telephone: (512) 678-9050
Facsimile: (512) 678-9101

*Counsel for Respondents Motorola Mobility
LLC, Lenovo (United States) Inc. and
Motorola (Wuhan) Mobility Technologies
Communication Co., Ltd.*

**UNITED STATES INTERNATIONAL TRADE COMMISSION
WASHINGTON, DC**

**Before The Honorable MaryJoan McNamara
Administrative Law Judge**

**In the Matter of Certain Mobile Phones, Components Thereof, and Products
Containing Same
Inv. No. 337-TA-1375**

CERTIFICATE OF SERVICE

I, Robert Leonard, hereby certify that on August 16, 2024, copies of the foregoing document were filed and served upon the following parties as indicated:

The Honorable Lisa R. Barton, Secretary U.S. International Trade Commission 500 E Street, S.W., Room 112 Washington, DC 20436	☒ Via Electronic Filing (EDIS) ☐ Via Hand Delivery ☐ Via Federal Express ☐ Via Electronic Mail
The Honorable MaryJohn McNamara Administrative Law Judge U.S. International Trade Commission 500 E Street, S.W. Washington, DC 20436 Email: McNamara337@usitc.gov	☒ Via Electronic Filing (EDIS) ☐ Via Hand Delivery ☐ Via Federal Express ☒ Via Electronic Mail
Linda Chang Office of Unfair Import Investigations U.S. International Trade Commission 500 E Street, S.W., Room 401 Washington, D.C. 20436 Email: Linda.chang@usitc.gov	☐ Via Electronic Filing (EDIS) ☐ Via Hand Delivery ☐ Via Federal Express ☒ Via Electronic Mail ☒ Via Box.com
Adam D. Swain Alston & Bird LLP 950 F Street NW Washington, D.C. 20004 Email: EricssonLenovo@alston.com Email: Ericsson_Lenovo@mckoolsmith.com Email: Ericsson.ITC1375@fisherbroyles.com <i>Counsel for Complainant Telefonaktiebolaget LM Ericsson</i>	☐ Via Electronic Filing (EDIS) ☐ Via Hand Delivery ☐ Via Federal Express ☒ Via Electronic Mail

Brian R. Nester COVINGTON & BURLING LLP One City Center 850 Tenth Street, N.W. Washington, DC 20001 Telephone: 202-662-6000 Email: Lenovo-1375-1376-Cov@cov.com <i>Counsel for Motorola Mobility LLC, Lenovo (United States) Inc., and Motorola (Wuhan) Mobility Technologies Communications Co., Ltd.</i>	☐ Via Electronic Filing (EDIS) ☐ Via Hand Delivery ☐ Via Federal Express ☒ Via Electronic Mail
Gregory F. Corbett WOLF, GREENFIELD & SACKS, P.C. 600 Atlantic Avenue Boston, MA 02210 Telephone: 617.646.8000 Fax: 617.646.8646 Email: WGS-LenovoITC1375@WolfGreenfield.com <i>Counsel for Motorola Mobility LLC, Lenovo (United States) Inc., and Motorola (Wuhan) Mobility Technologies Communication Co., Ltd.</i>	☐ Via Electronic Filing (EDIS) ☐ Via Hand Delivery ☐ Via Federal Express ☒ Via Electronic Mail

/s/ Robert Leonard
Robert Leonard