

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

SAMSUNG ELECTRONICS CO. LTD., and  
SAMSUNG ELECTRONICS, AMERICA, INC.,  
Petitioners,

v.

NETWORK-1 TECHNOLOGIES, INC.,  
Patent Owner.

---

IPR2026-00117  
Patent 12,166,869

**DECLARATION OF DR. KONSTANTINOS PSOUNIS**

Signed: \_\_\_\_\_



Dr. Konstantinos Psounis

March 2, 2026

## **I. Introduction**

1. My name is Konstantinos Psounis. I am over eighteen years of age, of sound mind, and qualified to make the statements set forth in this Declaration. With the exception of the legal principles counsel has supplied to me, all the facts and statements contained herein are within my personal knowledge and are in all respects true and correct.

2. I have been asked by Network-1 Technologies, Inc. (“Network-1” or “Patent Owner”) to submit this declaration in response to a Petition in IPR2026-00117 from Samsung Electronics Co. Ltd., and Samsung Electronics, America, Inc., (“Samsung” or “Petitioner”) regarding U.S. Patent No. 12,166,869 (“the ’869 Patent”).

3. I am being compensated for my time at my current standard rate of \$950 per hour for the services that I provide in connection with this case. That compensation is not contingent upon my performance, the outcome of the case, or any issues involved in or related to this case.

4. I declare under penalty of perjury that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true. I further understand that willful false statements and the like are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code.

## II. Qualifications

5. I have summarized in this section my educational background, career history, publications, and other relevant qualifications. My full *curriculum vita* is available at Exhibit 2025.

6. I am a Professor and prior Associate Chair of Electrical and Computer Engineering and Professor of Computer Science at the University of Southern California. I joined the University of Southern California in 2003, after completing my PhD at Stanford University as a Stanford Graduate Fellow.

7. My professional career spans more than 20 years. As set forth in my CV, I have extensive experience in the field of networked distributed systems, including the Internet and the web, Wi-Fi and cellular wireless systems, spectrum sharing wireless systems, sensor and IoT wireless systems, mobile ad hoc and delay tolerant wireless systems, data centers and cloud systems, peer to peer systems, and autonomous vehicles/drones systems.

8. I have published more than 100 technical papers in these fields, which have been cited tens of thousands of times. I have also been awarded numerous grants and significant funding from the government and industry leaders to advance these fields. As a result, I have been named an Institute of Electrical and Electronics Engineers (IEEE) Fellow, the highest grade of membership, for “fundamental

contributions in the theory and practice of wireless networks,” and a Distinguished Member of the Association of Computing Machinery (ACM).

9. Throughout my career, I have analyzed, designed, and developed efficient networked distributed systems for the Internet and the Web, Wi-Fi and cellular wireless systems, spectrum sharing wireless systems, sensor and IoT wireless systems, mobile ad hoc and delay tolerant wireless networks, data centers and cloud systems, peer to peer systems, and autonomous vehicles/drones systems. As such, I have acquired extensive expertise in the analysis and development of those systems and associated products.

10. I have extensive experience with and made contributions specifically towards analyzing and designing efficient Wi-Fi, cellular and other wireless systems. In particular, I have received multiple funding awards from the National Science Foundation (NSF), the leading governmental agency for funding computer engineering and computer science research, to work on wireless systems, including Wi-Fi systems. I have also received multiple funding awards from industry leaders in the area of networking and in particular wireless networking, to work on these systems. I have published several papers in the most selective academic journals and conferences on wireless systems. I have also been the faculty in charge of the entire networking curriculum at the Electrical and Computer Engineering department at

USC for more than a decade and teach networking classes and in particular the graduate wireless networking class yearly.

11. I also have extensive practical experience with networked distributed systems. For example, I was a co-founder of SpaceMUX, Inc. (whose IP was later acquired by Quantenna Communications, Inc.), where I designed and developed systems to increase the speed of wireless networked systems using modern wireless networking technologies and techniques. Also, I was the Technology Architect for Fineground Networks (later acquired by Cisco Systems, Inc.), where I designed and developed systems to accelerate the delivery of content over the World Wide Web. In addition, for over 20 years both at Stanford University and at the University of Southern California I have designed and implemented efficient algorithms, protocols, and systems for a variety of distributed networked systems, and I have consulted for industrial leaders, and produced prototype systems. I have also applied for and been granted numerous patents, which are owned by network industry leaders and prestigious academic institutions.

12. In sum, I have extensive experience in and familiarity with the fields of networked distributed systems and in particular with wireless networking systems including Wi-Fi and cellular wireless systems, and extensive experience and contributions towards the analysis, design, and implementation of such systems.

### **III. Materials Considered**

13. Among the materials I have reviewed in forming my opinions are the '869 Patent, its prosecution history, as well as the patents, references, and other materials cited in this expert declaration.

14. I have also reviewed the Petition and its exhibits, including the declaration of Dr. Sundeeep Rangan, Ph.D. (Exhibit 1002).

### **IV. Legal Principles**

15. I am not a lawyer. In forming my opinions as set forth in this Declaration, I have relied upon legal principles supplied to me by attorneys for Network-1. In forming my opinions, I have not relied upon Patent Owner's attorneys for any purpose other than the following legal principles.

#### **A. Claim Construction**

16. I understand that determining whether a patent claim is valid requires a two-step analysis. First, the claim must be construed. Second, the properly construed claim must be compared to the prior art.

17. With respect to the first step, I understand that claims are construed from the perspective of a person of ordinary skill in the art ("POSITA") at the time of the invention. I understand that, absent a disclaimer or express definition, claim terms are given their plain and ordinary meaning to a POSITA in view of the specification and file history and the knowledge of a POSITA. Unless otherwise

noted, I have applied what I consider to be the plain and ordinary meaning of all terms as understood by a POSITA at the time of the invention.

### **B. Anticipation**

18. I understand that, although not expressly disclosed, subject matter may be inherently disclosed in a prior art reference where that subject matter is necessarily present in the subject matter disclosed and would be understood to be so by those of ordinary skill in the art. I understand that the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic.

19. I understand that a claim is invalid if each and every element of the claim is disclosed in a single prior art reference with the elements arranged as specified in the claim, either expressly or inherently. I understand that invalidity based on the disclosure of a single prior art reference in this manner is called anticipation.

### **C. Obviousness**

20. I understand that a claim would have been obvious under 35 U.S.C. § 103 if one or more prior art references disclose every claim limitation in such a way so as to render the claim, as a whole, obvious to a person of ordinary skill in the art at the time the purported invention was made.

21. In determining whether or not a patented invention would have been obvious, the following factors should be considered: (a) the scope and content of the prior art; (b) the differences between the prior art and the claims at issue; (c) the level of ordinary skill in the art; and (d) whatever “secondary considerations” may be present.

22. I understand that certain “secondary considerations” may be relevant in determining whether or not an invention would have been obvious, and that these secondary considerations may include commercial success of a product using the invention, if that commercial success is due to the invention; long-felt but unsolved need for the invention; evidence of copying of the claimed invention by others; industry acceptance; initial skepticism of the invention; failure of others to solve the problem; praise of the invention by others; the taking of licenses under the patents by others; and simultaneous invention by others (which may be an indication that the claimed invention was the result of ordinary skill in the art).

23. I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. While multiple prior art references or elements may, in some circumstances, be combined to render a patent claim obvious, I understand that I should consider whether there is an apparent reason to combine the prior art references or elements in the way the patent claims. To determine whether such an

apparent reason exists to combine the prior art references or elements in the way a patent claims, it will often be necessary to look to the interrelated teachings of multiple patents, to the effects of demands known to the design community or present in the marketplace, and to the background knowledge possessed by a person having ordinary skill in the art.

24. I also understand that when the prior art teaches away from combining prior art references or certain known elements, discovery of a successful means of combining them is more likely to be non-obvious. A prior art reference may be said to teach away from a patent when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the patent or would be led in a direction divergent from the path that was taken by the patent.

25. I also understand that it is not permissible to use hindsight in assessing whether a claimed invention is obvious. Rather, I understand that, to assess obviousness, you must place yourself in the shoes of a person having ordinary skill in the relevant field of technology at the time the inventions were made who is trying to address the issues or solve the problems faced by the inventor and ignore the knowledge you currently now have of the inventions.

26. I also understand that there are numerous ways in which to articulate the legal standard for obviousness, including: (1) combining prior art elements according to known methods to yield predictable results, (2) simple substitution of

one known element for another to obtain predictable results, (3) use of a known technique to improve similar devices (methods, or products) in the same way, (4) applying a known technique to a known device, method, or product ready for improvement to yield predictable results, (5) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success, (6) known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art, and (7) some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

**D. Person of Ordinary Skill in the Art**

27. I understand that the meaning of claim terms and a patent's validity are to be determined from the vantage point of one of ordinary skill in the art at the time of the invention (a "POSITA"). In determining who would be one of such ordinary skill, I understand it is appropriate to consider criteria such as: (a) the type of problems encountered in the art; (b) prior art solutions to those problems; (c) the rapidity with which innovations are made; (d) the sophistication of the technology; and (e) the education level of active workers in the field.

## **V. The Level of Ordinary Skill in the Art**

28. For the purposes of this declaration supporting the Patent Owner's Preliminary Response, I have been asked to apply the same POSITA definition as the Petition and assume that a POSITA "would have had at least a bachelor's degree in electrical engineering, computer engineering, computer science, or a similar field, and 2-3 years of experience with cellular/WLAN security and mobile devices." Pet. at 8. I understand that if trial is instituted, I will have the opportunity to propose my own definition of a POSITA.

## **VI. Claim 1 of the '869 Patent**

29. Claim 1 of the '869 Patent recites a method for a mobile device with an embedded universal integrated circuit card (eUICC) to securely communicate with a wireless network:

1. A method for a mobile device with an embedded universal integrated circuit card (eUICC) to securely communicate with a wireless network, the method performed by the mobile device, the method comprising:
  - a) storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key;
  - b) receiving, from a first server associated with the wireless network, an encrypted profile for the eUICC comprising cryptographic parameters, a module identity, and a key K;
  - c) generating a shared secret key using a first elliptic curve Diffie-Hellman (ECDH) key exchange with the first module private key and the network public key;
  - d) decrypting, with the shared secret key, at least a portion of the encrypted profile for the eUICC;
  - e) generating, by the eUICC, a second module public key and a corresponding second module private key;

- f) sending, to a second server associated with the wireless network, the second module public key;
- g) generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;
- h) generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity; and
- i) sending, to the second server, the module encrypted data.

EX1001 at 148:4-31. The claim provides a cryptographically connected, two-stage approach by which a mobile device with an eUICC can securely communicate with a wireless network, such as a cellular network. It details the use of both asymmetric keys and symmetric keys in a particular way to ensure safe delivery of an eUICC profile that contains important data, which is used to enable subsequent cryptographic exchanges for authenticating to a wireless network. The first stage—limitations 1(a)-(d)—details steps for securely receiving an eUICC profile for the mobile device from a first server. The second stage—limitations 1(e)-(i)—details steps for using that received profile information to then securely identify the mobile device to a second server of the network (*e.g.*, for authentication purposes).<sup>1</sup>

30. In the first stage, the eUICC of the mobile device stores a first module private key, a corresponding first module public key, and a network public key. *See* EX1001 at 148:8-10; *see also id.* at Fig. 1a, 1c, 23:22-24, 15:24-26.

---

<sup>1</sup> The Petition also describes and illustrates claim 1 as a two-phase approach. However, this analysis never acknowledges that those two phases are cryptographically connected. This oversight in the analysis of claim 1 permeates the Petition's entire proposed mapping of the references to the claim limitation.

31. The mobile device receives, from a first server associated with the wireless network an encrypted eUICC profile containing cryptographic parameters, a module identity (*e.g.*, an IMSI), and a key K. *See* EX1001 at 148:11-14; *see also id.* at Fig. 3b (illustrating a received eUICC profile), 61:53-57 (describing key K), 62:22-28 (describing cryptographic parameters and module identity).

32. The mobile device then generates a shared secret key with a first elliptic curve Diffie-Hellman (ECDH) key exchange using the stored first module private key and network public key. *See* EX1001 at 148:15-17; *see also id.* at 61:14-25 (describing generation of a shared secret key). The shared secret key is then used to decrypt at least a portion of the received profile. *See* EX1001 at 148:18-19; *see also id.* at 61:25-32 (describing profile decryption).

33. In the second stage, the eUICC generates a second module public key and corresponding second module private key. *See* EX1001 at 148:20-21; *see also id.* at Fig. 3b, 133:39-42 (describing derivation of new module public and private keys). Then, the mobile device sends this second public key to a second server associated with the wireless network. *See* EX1001 at 148:22-23; *see also id.* at 134:39-41.

34. The mobile device then generates a symmetric key using a second ECDH exchange with the second module private key and the cryptographic parameters from the received profile. *See* EX1001 at 148:24-26; *see also id.* at 33:24-

32 (describing ECDH key exchange for deriving symmetric key); *id.* at 123:56-62, 141:25-36 (similar). Using that symmetric key, the mobile device generates module encrypted data that includes the module identity and sends this encrypted data to the second server. *See* EX1001 at 148:27-31; *see also id.* at 138:4-7, 138:16-19 (detailing sending message including an encrypted module identity 110a).

35. Importantly, the two “stages” of the claim are not independent of each other. Nor would a POSITA understand them to be interchangeable operations. The cryptographic parameters obtained through the first exchange—the cryptographic parameters within the profile—directly enable the second exchange. And these parameters can only be obtained via proper secure delivery of the encrypted profile, which is enabled via a shared secret key generated using the stored first module private key and network public key. Because both sides (the mobile device and the first server) independently derive the same shared secret from their respective private keys and the other party’s public key, the decryption key itself (shared secret key) never needs to be transmitted—a fundamental advantage over the prior art’s dependence on encrypted channel delivery of key K. *See* EX1001 at 4:14-25.

36. And the second stage, by using a freshly generated key pair (the second module public key and corresponding second module private key), ensures that even if the initial module private key became compromised, the mobile device’s module identity transmission would remain protected by an entirely separate set of keys.

This architecture achieves the patent's core objectives: eliminating dependence on physical key distribution, avoiding transmission of key K through insecure third-party channels, enabling key rotation without replacing hardware or profiles, and maintaining full compatibility with deployed wireless networks.

## VII. Petitioner's References

37. I have summarized the subset of references relied on by the Petition that are pertinent to my opinions provided below responsive to aspects of Grounds 1 and 2 of the Petition.

### A. Nakhjiri

38. Nakhjiri, U.S. Patent No. 9,210,138, titled "Efficient Key Generator for Distribution of Sensitive Material from Multiple Application Service Providers to a Secure Element Such as a Universal Integrated Circuit Card (UICC)," was filed on April 17, 2013. EX1005 at cover page. The reference is directed to a single, discrete problem: the secure remote provisioning of profiles from application service providers, such as mobile network operators ("MNOs"), to target devices such as smartphones containing embedded UICCs. *See* EX1005 at Abstract, 2:34-42.

39. Nakhjiri describes a provisioning infrastructure that includes a source node associated with an MNO, intermediate nodes including a Subscription Manager-Data Preparation ("SM-DP") server, and the target device. *See* EX1005 at 2:37-42, 2:50-58. The profile to be securely delivered may include "security

application algorithm codes, data and cryptographic keys.” EX1005 at 2:4-6. Nakhjiri specifically identifies “MNO-specific boot codes” and “a sequence number or a timestamp” as data included in a profile. *See* EX1005 at 7:24-27, 7:49-51.

40. A central concern of Nakhjiri is the storage limitations of memory-constrained UICCs. *See* EX1005 at 4:14-16. Nakhjiri explains that prior approaches, such as assigning unique public/private key pairs to each UICC or using global MNO key pairs, suffered from scalability and storage problems. *See* EX1005 at 4:14-27. Storing pre-loaded key pairs for each MNO could quickly exhaust UICC memory, and would also exclude new MNOs for which key pairs had not been pre-loaded. *See* EX1005 at 4:20-25. Nakhjiri describes these problems and frames them as the motivation for its inventive solution. *See* EX1005 at 4:66-5:2; *id.* at 5:14-24 (explaining that requiring certificates to verify public keys “would defeat the purpose of using ECC and private seeds for storage space optimization”).

41. To address these storage problems, Nakhjiri teaches using Elliptic Curve Cryptography (“ECC”) with a private seed that is unique to each UICC and is loaded during manufacturing. *See* EX1005 at 4:38-45. Using this seed and an MNO identifier (MNO\_ID), the UICC derives a device-specific ECC private key (MNO\_ECC\_PVKDEV) on the fly through a key generation function (“KGF”):

$$MNO\_ECC\_PVKDEV = KGF(private\_seed, MNO\_ID)$$

EX1005 at 4:45-50. The corresponding ECC public key (MNO\_ECC\_PLKDEV) is then derived from the private key and the ECC curve, using the Elliptic Curve base point G:

$$MNO\_ECC\_PLKDEV = MNO\_ECC\_PVKDEV * G$$

EX1005 at 4:51-56. Nakhjiri explains that because the UICC only needs to store the seed, it saves significant storage space compared to storing multiple RSA private keys and MNO certificates. *See* EX1005 at 4:66-5:2.

42. The UICC manufacturer or vendor creates the private/public key pairs based on the private seeds and sends the public key list to the SM-DP associated with each MNO. *See* EX1005 at 5:6-8. Critically, Nakhjiri teaches that the list of device public keys should be kept secret as an authentication measure. *See* EX1005 at 5:14-17. Nakhjiri warns that if the public key list were public, any party could use a device public key to encrypt an illegitimate profile and send it to a UICC. *See id.* Avoiding this attack by requiring the MNO SM-DP to sign the encrypted profile would in turn require installation of SM-DP certificates for every MNO/SM-DP within the UICC, which Nakhjiri states, “would defeat the purpose of using ECC and private seeds for storage space optimization.” EX1005 at 5:14-22. Accordingly, Nakhjiri’s system relies on maintaining the public key list in secret to avoid the use of signatures altogether. *See* EX1005 at 5:23-24.

43. To deliver the encrypted profile, the SM-DP generates its own ECC private/public key pair (MNO\_ECC\_PVKOP and MNO\_ECC\_PLKOP). *See* EX1005 at 5:40-43. The SM-DP uses its private key and the UICC's public key (obtained from the secret public key list) to perform a local ECDH key agreement and create a profile encryption key ("PEK") from a shared ECDH secret. *See* EX1005 at 5:43-50. The SM-DP then uses the PEK to encrypt the profile via symmetric key encryption and delivers the encrypted profile along with the MNO\_ID and the MNO's public key (MNO\_ECC\_PLKOP) to the target device. *See* EX1005 at 5:53-58.

44. On the device side, once the UICC receives the encrypted profile, it uses its private seed and the MNO\_ID to generate its own ECC private key (MNO\_ECC\_PVKDEV) using the pre-configured key generator function (KGF). *See* EX1005 at 5:61-64. The UICC then uses this derived private key and the MNO's public key (MNO\_ECC\_PLKOP) to perform a local ECDH key agreement, derive the same PEK, and decrypt the profile for secure storage. *See* EX1005 at 5:64-6:2, 6:9-16.

45. Nakhjiri does not describe the UICC taking any further action with the profile, such as using it or its contents to authenticate with any network server. The reference does not address what happens after the profile is provisioned; it does not

describe any network authentication process or any subsequent use of the provisioned profile to communicate with a wireless network.

**B. Jeong**

46. Jeong, titled “A Design of Safe AKA Module for Adapted Mobile Payment on Openness Smartphone Environment,” was published in November 2010 in the Journal of Korea Multimedia Society, Vol. 13, No. 11. EX1007 at 0002. The paper addresses user authentication in mobile payment systems operating in open smartphone environments. *See* EX1007 at 0002 (Abstract). Jeong builds upon the existing 3GPP-AKA (Authentication Key Agreement) protocol, identifying several deficiencies in that protocol and proposing targeted improvements to address them. *See* EX1007 at 0008 (§3.2).

47. Jeong’s system involves three network entities: a mobile station (“MS”) equipped with a USIM card, a serving network (“SN”), and a certificate authority designated as the home network (“HN”), which includes an Authentication Center. *See* EX1007 at 0008 (Fig. 6). In the 3GPP-AKA model, the MS sends its IMSI (International Mobile Subscriber Identity) in plaintext to the HN for authentication. *See* EX1007 at 0004-05 (§2.2). Jeong identifies this as a privacy vulnerability, noting the “privacy problem due to IMSI plaintext transmission in the existing 3GPP-AKA mutual authentication.” *See* EX1007 at 0008 (§3.2).

48. To address the IMSI exposure problem, Jeong proposes encrypting the IMSI with a shared secret key  $SSK_{MS-HN}$  that is shared between the MS and the HN, and then transmitting the encrypted IMSI ( $E-IMSI_{MS}$ ) to the SN for forwarding to the HN. *See* EX1007 at 0008 (§3.2(1)). At the HN, the certificate authority decrypts  $E-IMSI_{MS}$  using the same shared secret key  $SSK_{MS-HN}$  to recover the MS's IMSI, and then checks whether the IMSI is in its database. *See* EX1007 at 0008 (§3.2(3)).

49. Jeong is explicit about how  $SSK_{MS-HN}$  is generated. Jeong explains that  $SSK_{MS-HN}$  is a static, long-term key that is derived from values established during an advance registration phase: “The shared secret key,  $SSK_{MS-HN}$ , is generated using the initial point and secret key registered in the USIM card and the certificate authority when the USIM card is first registered, and  $MAC_{MS}$  and  $XMAC_{MS}$  are generated for mutual authentication.” EX1007 at 0009 (§4.1.1(1)). This key is described as being based on the EC-DH algorithm. *See* EX1007 at 0009 (§4.1.1(1)). The inputs to the key derivation—a “secret key registered in the USIM card and the certificate authority” and the “initial point”—are established at the time of USIM registration and are already known to both the MS and HN before any authentication session begins. *See* EX1007 at 0009 (§4.1.1(1)). The paper's abstract similarly confirms that the module “prevents the exposure of IMSI by creating the SSK (Shared safe Key) through advance registration . . . .” EX1007 at 0002 (Abstract).

50. Jeong’s design makes a deliberate architectural distinction between two different categories of shared secret keys.  $SSK_{MS-HN}$  is the static, pre-registered key used to encrypt the IMSI for the MS-HN authentication relationship. *See* EX1007 at 0009 (§4.1.1(1)). By contrast,  $OT-SSK_{MS-SN}$  is a separate, one-time shared secret key generated dynamically for each session between the MS and the SN. *See* EX1007 at 0009 (§4.1.1(2)). The  $OT-SSK_{MS-SN}$  is generated through a protocol-based, interactive ECDH exchange illustrated in Figure 6 and detailed in §3.2.

51. At step (5), the SN transmits the initial point P and its own public key SNP to the MS; at step (6), the MS generates  $OT-SSK_{MS-SN}$  using its own secret key and the received public key ( $OT-SSK_{MS-SN} = EC-DH(P, MS, SNP)$ ). *See* EX1007 at 0009 (§§3.2(5)-(6)). This dynamic exchange occurs only after the HN verifies the identity of the MS at step (3). *See* EX1007 at 0009 (step (4) proceeds “After verifying the identity of the MS”). That is, the MS first sends its encrypted IMSI at step (1), the HN decrypts and verifies the MS’s identity at step (3), all before the MS-SN ECDH exchange begins. *See* EX1007 at 0008-0009 (§§3.2(1)-(5)). Jeong specifically identifies the one-time key approach as providing protection against “retransmission attacks” and uses it to “generat[e] a new OT-SSK for each connection . . . .” EX1007 at 0010 (§§4.1.3, 5).

52. This two-tier key architecture—a pre-registered static key for the MS-HN trust relationship and a dynamic ephemeral key for the MS-SN session

relationship—is a deliberate design choice driven by protocol sequencing requirements. The very first action in Jeong’s Safe AKA Procedure is for the MS to encrypt its IMSI using  $SSK_{MS-HN}$ . *See* EX1007 at 0008 (§3.2(1)). Because this is the opening message of the authentication sequence—with no prior interactive communication between the MS and any network entity—the MS must already possess the key needed to protect its IMSI before the protocol begins. A dynamically derived key would require a preliminary key exchange, which would itself require the MS to identify itself to the network, potentially re-introducing the IMSI exposure problem that  $SSK_{MS-HN}$  was designed to eliminate.

53. In addition to the IMSI privacy improvement, Jeong addresses other deficiencies in the existing 3GPP-AKA protocol, including the sequence number (SQN) synchronization problem, false base station attacks, and bandwidth consumption between the SN and certificate authority. *See* EX1007 at 0008 (§3.2). The paper also describes a mobile payment protocol with registration, authentication, and payment authorization phases, in which participants (users, merchants, payment centers, and issuing banks) register their master keys with the certificate authority and generate shared secret keys during the registration phase for use in subsequent authentication stages. *See* EX1007 at 0006-07 (§3.1.1 and §3.1.2). The Safe AKA Procedure detailed later in Jeong provides the basis of this advanced

registration phase regarding the users, merchant, payment centers, and issuing banks to support Jeong's Mobile Payment protocol design.

### **C. Ala-Laurila**

54. Ala-Laurila (U.S. Patent Publication No. 2012/0300934), titled "Arranging Data Ciphering in a Wireless Telecommunication System," was published on November 29, 2012. EX1013 at cover page. The reference is directed to a method for authenticating a mobile terminal ("MT") in a wireless local area network ("WLAN") by leveraging the subscriber identity and authentication infrastructure of a public land mobile network—in the preferred embodiment, a GSM network ("GSMNW"). *See* EX1013 ¶¶ [0005]-[0007].

55. Ala-Laurila identifies a specific problem in WLAN networks: "ciphering keys used for ciphering traffic must be stored in advance in the terminal and access point," which makes it "difficult" to "add different ciphering keys" and prevents "safe data transmission" for "terminals moving in different networks." EX1013 ¶ [0004]. Ala-Laurila states that it is "an object of the invention to provide a new method for creating the keys to be used in ciphering for a wireless local area network and for employing them so as to avoid the above problems." EX1013 ¶ [0005]. Ala-Laurila's solution avoids pre-storing ciphering keys in the terminal and access point, and instead dynamically creates them during an authentication process that leverages the existing GSM infrastructure.

56. Ala-Laurila’s system involves several distinct network entities residing in separate networks. As illustrated in Figure 1, the MT (which contains a SIM) communicates wirelessly with access points (“APs”) in the WLAN. *See* EX1013 ¶ [0016], Fig. 1. The WLAN includes a Public Access Controller (“PAC”) that controls access to the WLAN. *See* EX1013 ¶ [0021], Fig. 1. Separately, connected through the Internet, is the GSMNW—a public land mobile network—which contains a GSM Authentication and Billing Gateway (“GAGW”). *See* EX1013 ¶ [0022], Fig. 1. The GAGW is described as “an entity in the mobile network GSMNW offering authentication services of mobile subscribers to the WLAN networks . . . .” EX1013 ¶ [0022]. Critically, the PAC resides in the WLAN network, and the GAGW resides in the GSMNW—these are two distinct servers in two distinct networks, separated by the Internet. *See* EX1013 Fig. 1; *id.* ¶ [0021] (noting that the WLAN “may also offer a connection through a gateway to other networks, such as the Internet”).

57. The authentication process described in Ala-Laurila’s preferred embodiment, illustrated in Figure 2, proceeds through a multi-step GSM-based challenge-response protocol. When the MT seeks to connect to the WLAN, it retrieves the IMSI identifier from its SIM (step 202) and sends an authentication starting request (MT\_PAC\_AUTHSTART\_REQ) to the PAC. *See* EX1013 ¶ [0026]. This request contains a Network Access Identifier (“NAI”) that “comprises

the IMSI identifier obtained from the identity module SIM.” EX1013 ¶ [0026]. Ala-Laurila states that this request “is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm, for example.” EX1013 ¶ [0026]. Ala-Laurila provides no further detail regarding this Diffie-Hellman reference—there is no discussion of public or private key generation, no discussion of elliptic curve parameters, no description of key exchange mechanics, and no explanation of how a symmetric key would be derived from the exchange.

58. After the PAC receives the authentication request, it “deciphers the request 204 if needed” and sends the GAGW a request (PAC\_GAGW\_AUTHSTART\_REQ) that includes the NAI and the MT’s protection code. EX1013 ¶ [0027]. Ala-Laurila does not state or suggest that this subsequent message from the PAC to the GAGW is sent in ciphered form.

## VIII. Analysis

### A. Nakhjiri’s Design Disallows Storing Public/Private Keys for Provisioning in the eUICC

59. Nakhjiri is focused on the problem of secure remote provisioning of profiles from application service providers (*e.g.*, mobile network operators) to target devices (*e.g.*, cellphones or smartphones with UICCs). *See* EX1005 at Abstract, 2:34-42. Nakhjiri explains that, within the problem-space it is addressing, there are multiple application service providers (or MNOs), each providing its own secure data that must be maintained in “its own secure domain of the secure execution

environment” of the UICC. EX1005 at 1:60-65. And Nakhjiri identifies UICC storage space as a significant design challenge for any solution in this problem-space context: “This can present a challenge when the amount of resources and secure storage space in the secure execution environment is limited.” EX1005 at 1:65-67.

60. Importantly, the secure profiles Nakhjiri seeks to provision take space on the UICC—they must be installed. *See* EX1005 at 2:6-10 (“Such provisioning may include the transport of encrypted profiles through the network, decryption of encrypted profiles within the secure execution environment, and installation of the profiles within a secure storage for later execution within the secure execution environment.”). Accordingly, Nakhjiri highlights the importance of reducing the storage space required for its profiles.

61. Relatedly, Nakhjiri discusses the storage problems that arise from storing public and/or private keys corresponding to each application service provider (or MNO). *See* EX1005 at 4:14-16 (“Both with global MNO key pairs and unique UICC key pairs, there may be storage problems for memory-constrained UICCs, especially if RSA key pairs are used.”). Based on these identified storage problems, Nakhjiri proposes a solution in which private keys are derived as needed rather than stored. This derivation relies on a key generator function to calculate the private key for a target device (or mobile phone) using a private seed that is unique to the device. *See* EX1005 at 5:61-64 (“As shown, the UICC uses its private seed and the MNO

identifier (MN\_ID) to generate its own ECC private key (MNO\_ECC\_PVKDEV) using the pre-configured key generator function (KGF) 510.”); EX1005 at 4:38-40 (“To generate ECC private keys within the UICC, a *private seed that is unique to each UICC* can be loaded within each UICC.” (emphasis added)); *see also* EX1005 at 4:50 (private key derivation function).

62. Nakhjiri explains that a purpose of its proposed solution, including the derivation of mobile device private keys using a private seed, is to optimize storage space. *See* EX1005 at 5:21-22 (identifying a purpose of Nakhjiri’s solution as “using ECC and private seeds for storage space optimization”); EX1005 at 4:66-5:2 (“Since the UICC only needs to store the seed it is able to save significant storage space (in comparison to the amount of storage space needed to store multiple RSA PVKs for multiple MNOs as well as certificates for those MNOs).”).

63. Based on Nakhjiri’s teachings regarding space optimization in the UICC, it is my opinion that a POSITA would not have understood Nakhjiri to teach storing private keys for the target device. Furthermore, I do not agree with the Petition’s assertion that the MNO\_ECC\_PVKDEV in Nakhjiri is “stored in the eUICC at least long enough for the eUICC to derive the ‘shared ECDH Secret 540.’” Pet. at 29. A POSITA would have understood Nakhjiri’s ECDH Key Agreement 520 to represent mathematical operations on the input values. Furthermore, the KGF 510 (or key generator function) also would have been understood as mathematical

operations. Chaining together two sequences of mathematical operations, as illustrated in Nakhjiri's Figure 4, does not teach or suggest that the interim values must be stored as claim 1 of the '869 Patent requires.

64. For these reasons, it is my opinion that Nakhjiri fails to disclose "storing, in the eUICC, a first module private key" as required by Claim 1 of the '869 Patent. Rather, Nakhjiri highlights as one of its advantages that public and private keys are not stored in the UICC. *See* EX1005 at 4:66-5:2.

### **B. Nakhjiri's Design Avoids Exposing Public Keys**

65. As detailed earlier, Nakhjiri teaches the derivation of private keys (MNO\_ECC\_PVKDEV) based on pre-stored private seeds. *See supra* ¶ 41. That is how a target device (or mobile phone) derives its own private key. Nakhjiri explains that the public/private key pairs used for target device UICCs are generated by the manufacturer or vendor of the UICC. *See* EX1005 at 5:8-13 ("Accordingly, the UICC manufacturer or vendor creates a private, public key pair (MNO\_ECC\_PVKDEV, MNO\_ECC\_PLKDEV) based on the private seeds and then sends the public key list (the list of MNO\_ECC\_PLKDEV) to the SM-DP associated with that MNO.").

66. Nakhjiri then explains that the public key list provided to the SM-DP associated with an MNO should be kept secret as a security measure. *See* EX1005 at 5:14-15 ("As an authentication measure, the list of public keys may be kept

secret.”). Nakhjiri explains that, if the list is not kept private, “any party could use a public MNO\_ECC\_PLKDEV to encrypt an illegitimate profile and send it to a UICC.” EX1005 at 5:15-17. To avoid such illegitimate use of a publicly known MNO\_ECC\_PLKDEV, the “MNO SM-DP would have to sign the encrypted profile,” which would require “installation of MNO SM-DP certificates for every single MNO/SM-DP within the UICC . . . .” EX1005 at 5:17-21. However, Nakhjiri highlights that this implementation “would defeat the purpose of using ECC and private seeds for storage space optimization.” EX1005 at 5:21-22. Nakhjiri proposes that “by maintaining the public key list in secret the use of a signature can be avoided.” EX1005 at 5:23-24.

67. The Petition proposes incorporating Nakhjiri’s ECDH key exchange process into Ala-Laurila to satisfy limitations 1(e), 1(f), and 1(g). *See* Pet. at 63 (regarding limitation 1(e)), 65 (regarding limitation 1(f)), 65-66 (regarding limitation 1(g)). This proposal is problematic for multiple reasons, one of which I detail below.

68. Limitation 1(f) requires that the mobile device send its public key over a wireless connection to a second server. EX1001 at 148:22-23. However, sending the public key over a wireless network exposes it to the public—which is something that Nakhjiri specifically disallows as it requires the public key to remain a secret. *See* EX1005 at 5:14-17. Applying Nakhjiri’s reasoning in the context of the

authentication system that the Petition proposes to modify, an exposed public key would allow a party to imitate the second server (*e.g.*, a MNO authentication server) and “authenticate” the device to a false network. As a result, the false network can then intercept all remaining communications from the device during that session because the device believes it is authenticated to a proper network. The proposed combination and modifications neglect Nakhjiri’s teachings about public key security for authentication, and by doing so, exposes the system to a man-in-the-middle attack.

69. A POSITA would have recognized this problem with combining Nakhjiri’s ECDH key exchange process (which disallows sharing the public key and requires the other end to know it in advance) and Ala-Laurila’s authentication process. Based at least on Nakhjiri’s teachings regarding the problems it seeks to address (and avoid), a POSITA would not have expected Nakhjiri’s ECDH key exchange process to work for its intended purpose if implemented as the Petition proposes within the context of Ala-Laurila.

**C. The Proposed Combination of Nakhjiri and Ala-Laurila Is Internally Inconsistent**

70. The Petition proposes incorporating Nakhjiri’s ECDH key exchange process into Ala-Laurila to satisfy limitations 1(e), 1(f), and 1(g). *See* Pet. at 63 (regarding limitation 1(e)), 65 (regarding limitation 1(f)), 65-66 (regarding limitation 1(g)). For limitation 1(f), the Petition identifies both the PAC (of Ala-

Laurila's WLAN network) and the GAGW (of Ala-Laurila's GSMNW network) as the claimed "second server associated with the wireless network." *See* Pet. at 65. This same identification of both the PAC and GAGW as the claimed "second server" is confirmed in the Petition's limitation 1(e) analysis. *See* Pet. at 63 (identifying "PAC/GAGW" as "the 'second server'").

71. I disagree that a POSITA would have understood the combination of Ala-Laurila's PAC (in a WLAN network) and GAGW (in a GSM network) to teach the "second server associated with the wireless network" of claim 1 of the '869 Patent. Based on Ala-Laurila's teachings, these are separate servers in separate networks. *See* EX1013 ¶ [0016] (describing WLAN as "a WLAN network WLAN according to IEEE802.11 standard" and describing "GSMNW" as "a public land mobile network, in this embodiment a GSM network GSMNW").

72. Claim 1 of the '869 Patent requires "a second server associated with the wireless network." EX1001 at 148:22-23. The Petition never specifically identifies the "wireless network" of the claims. However, the Petition identifies Nakhjiri's SM-DP server as the "first server associated with the wireless network," which Nakhjiri explains is associated with a mobile network operator. *See, e.g.*, EX1005 at 3:60-61 ("the SM-DP associated with the given ASP"); *id.* at 2:45-46 (identifying a mobile network operator as an example of an ASP, or application service provider).

73. The Petition identifies only the PAC as the “second server” in its analysis of limitation 1(i). *See* Pet. at 67-68. However, one of skill in the art would not have understood Ala-Laurila’s WLAN networks to be associated with a mobile network operator’s network, which is what Nakhjiri’s SM-DP server and profile relate to. Instead, Ala-Laurila’s WLANs are networks that are separate from mobile networks, or cellular networks, such as those detailed in Nakhjiri. *See* EX1013 ¶¶ [0003], [0017] (detailing IEEE802.11 WLAN networks located in hotels, airports, etc.).

74. The Petition’s identification of the second server for two different claim limitations is inconsistent. As I explained above, a POSITA would not have understood the combination of Ala-Laurila’s PAC and GAGW (servers residing in two different, unrelated networks) to be the claimed “second server.” Furthermore, as POSITA would have not understood the PAC server in a WLAN network to be associated with the type of network Nakhjiri’s solution focused on (*e.g.*, cellular networks).

**D. Cryptographic Protocols, Algorithms, and Exchanges Are Not Plug-and-Play Components—The Proposed Combinations Are Fundamentally Inoperable**

75. Menezes, Oorschot, and Vanstone authored the Handbook of Applied Cryptography, which details the complexities and challenges associated with designing a cryptographic solution. A cryptosystem (or cryptographic solution) is a

“set of cryptographic primitives used to provide information security services.” EX2026 at 15 (page 29 of 103). These primitives include, for example, different types of symmetric-key primitives and public-key primitives. EX2026 at 5 (page 19 of 103) (Figure 1.1). The primitives used in a cryptosystem should be evaluated against criteria such as: (1) level of security; (2) functionality; (3) methods of operation; (4) performance; and (5) ease of implementation. *See* EX2026 at 5-6 (pages 19-20 of 103). “The relative importance of various criteria is very much dependent on the application and resources available.” EX2026 at 6 (page 20 of 103).

76. Specifically, regarding the methods of operation for a given primitive, Menezes et al. explains: “Primitives, when applied in various ways and with various inputs, will typically exhibit different characteristics; thus, *one primitive could provide very different functionality depending on its mode of operation or usage.*” EX2026 at 5-6 (pages 19-20 of 103) (emphasis added). Thus, a POSITA would have understood that the components (or primitives) of a cryptosystem (or cryptographic solution) could behave very differently depending on their mode of operation or how they are used.

77. Relatedly, a cryptographic protocol “is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective.” EX2026 at 33 (page 47 of 103). When designing a cryptographic protocol, it is essential to: “[1] identify *all*

assumptions in the protocol or mechanism design; and [2] for each assumption, determine the effect on the security objective if that assumption is violated.” EX2026 at 35 (page 49 of 103) (emphasis in original). Given the tight link between protocol design assumptions and the corresponding security objective, a cryptographic protocol designed for a particular use case (*e.g.*, profile provisioning) cannot simply be transplanted to a different use case (*e.g.*, authenticating with a mobile network) without potentially impacting or changing the design assumptions and security objectives. Thus, a POSITA would have understood that a cryptographic protocol designed for a particular use case should not be applied to a different use case without a rigorous analysis to verify that the underlying design assumptions remain valid and properly address the security objectives of the new use case.

78. The cryptographic protocols provided by both Jeong and Ala-Laurila relate to authentication. *See* EX1007 at 0008 (§3.2) (“Design of a safe Authentication Key Agreement (AKA) Module for Adapted Mobile Payment on Openness Smartphone Environment”); EX1013 at [0012] (describing Figure 2 as “a signaling diagram showing the authentication and calculation of a ciphering key according to a preferred embodiment”). The design of such protocols is solution-specific; any change in the protocol requires a reevaluation and verification of the modified protocol to determine whether it satisfies the underlying security objectives. Menezes et al. described the seemingly hidden complexities of

cryptographic protocols for authentication. *See* EX2026 at 401 (page 80 of 103) (“The apparent simplicity of the techniques presented below and in §10.3.3 is misleading. The design of such techniques is intricate and the security is brittle . . .”).

79. The Petition’s proposed combinations ignore the difficulties with designing secure cryptosystems or cryptographic protocols, and the Petition provides no analysis to confirm that the modified systems would have worked for their intended purposes. As detailed below, a POSITA would not have combined Nakhjiri with either Jeong or Ala-Laurila as the Petition proposes. The proposed combinations involve incompatible systems, yielding a resulting system that is fundamentally inoperable and would not work for its intended purpose.

**1. The Proposed Nakhjiri–Jeong Combination is Fundamentally Inoperable**

80. A POSITA would not have been motivated to combine Nakhjiri and Jeong as the Petition proposes. For Ground 1, the Petition proposes implementing Nakhjiri’s ECDH exchange to generate a pair of public/private keys (limitation 1(e)) to replace Jeong’s reliance on the static credentials established during an advance registration phase to generate  $SSK_{MS-HN}$ . *See* Pet. at 40-41; *see also* EX1007 at 0009 (§4.1.1(1)) (“The shared secret key,  $SSK_{MS-HN}$ , is generated using the initial point and secret key registered in the USIM card and the certificate authority when the USIM card is first registered . . .”). This proposed change affects the entirety of

Jeong's Safe AKA Procedure, which relies on  $SSK_{MS-HN}$  to encrypt the very first message of the protocol. It is not a simple "plug-and-play" change. The Petition fails to acknowledge or address any of these concerns. A POSITA would not have been motivated to make such a drastic change to Jeong's protocol, and a POSITA would not have had a reasonable expectation of success given the previously mentioned complexities of designing cryptographic protocols to satisfy particular security objectives.

81. More generally, a combination of Nakhjiri and Jeong results in a practically inoperable architecture due to redundant and conflicting credential management requirements. While Nakhjiri requires the manufacturing-level provisioning of a private seed, Jeong necessitates an independent advance registration phase to establish a Shared Safe Key (SSK). Attempting to bridge these two models—which both require the device and server to share a pre-existing secret before any secure communication may begin—forces a network operator to maintain dual, synchronized databases of secret keys for every global user. This is a logistical impossibility that cannot scale to support anonymous roaming across untrusted, third-party infrastructures and creates further security vulnerabilities. For these reasons, the proposed combination would not have worked for either reference's intended purpose.

## **2. The Proposed Nakhjiri–Ala-Laurila Combination is Fundamentally Inoperable**

82. A POSITA also would not have been motivated to combine Nakhjiri with Ala-Laurila as the Petition proposes. For Ground 2, the Petition proposes that “[a] POSITA would have applied Nakhjiri’s same ECDH mechanism to generate a second, ephemeral keypair for the authentication phase and send the second module public key to the PAC/GAGW (the ‘second server’).” Pet. at 63. Again, this proposed change affects a substantial portion of Ala-Laurila’s authentication solution, changing the very first message in the protocol sequence. The Petition fails to acknowledge or address any of these concerns. A POSITA would not have been motivated to make such a drastic change to Ala-Laurila’s protocol, and a POSITA would not have had a reasonable expectation of success given the previously mentioned complexities of designing cryptographic protocols.

83. More generally, Nakhjiri’s key derivation process, which relies on pre-shared private seeds, would be inoperable in Ala-Laurila’s network architecture that includes numerous untrusted WLANs. Nakhjiri’s private key is derived from a pre-shared seed. Ala-Laurila’s WLAN access points are not, and would not be, provisioned with the pre-shared seed, thus breaking the entire public/private key derivation process taught by Nakhjiri. Furthermore, Ala-Laurila specifically identified requiring pre-stored keys in the WLAN or terminal as a problem. *See* EX1013 ¶[0004].

84. For the above reasons, Nakhjiri and Ala-Laurila are architecturally incompatible. At a fundamental level, one cannot reconcile a security model requiring local nodes to possess a shared secret (Nakhjiri's non-exposed and thus secret public key) with a network topology where the local nodes are explicitly untrusted (Ala-Laurila's WLAN APs). Attempting to do so would necessitate exposing Nakhjiri's master seeds to the very third-party access points Ala-Laurila seeks to isolate, thereby negating the security objectives of both systems.