

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

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

v.

NETWORK-1 TECHNOLOGIES, INC.,  
Patent Owner.

---

IPR2026-00117  
Patent 12,166,869

**PATENT OWNER'S PRELIMINARY RESPONSE UNDER  
37 C.F.R. § 42.107 TO PETITION FOR INTER PARTES REVIEW**

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

## TABLE OF CONTENTS

I.	Introduction.....	1
II.	Background.....	4
	A. State of the Art .....	4
	B. Problems with the State of the Art .....	5
	C. The '869 Patented Invention .....	6
	D. Petitioners' References.....	10
	1. Nakhjiri [EX1005] .....	11
	2. Jeong [EX1007, EX1012].....	13
	3. Ala-Laurila [EX1013].....	15
III.	Legal Standards .....	16
IV.	Level of Ordinary Skill in the Art .....	18
V.	Claim Construction.....	19
VI.	Argument .....	19
	A. Nakhjiri Fails to Teach Multiple Limitations of Claim 1 (All Grounds).....	19
	1. Nakhjiri Teaches Away From Storing a Private Key in the eUICC .....	19
	2. Nakhjiri's Profile Does Not Include the Petition's Identified Parameters .....	22
	B. Jeong Fails to Teach Multiple Limitations and Would Not Have Been Modified as the Petition Proposes (Ground 1).....	25
	1. The Cryptographic Parameters Identified in Jeong Are Not Received in an Encrypted Profile .....	26
	2. Jeong's Static, Pre-Registered Keys Do Not Disclose "Generating" a Second Key Pair or Symmetric Key.....	29
	3. Because Jeong Does Not Disclose the Second Key Pair, It Cannot Disclose Sending a Second Public Key .....	40

C.	Ala-Laurila Fails to Teach Multiple Limitations and Would Not Have Been Combined with Nakhjiri as the Petition Proposes (Ground 2).....	41
1.	The Petition’s Shifting “Second Server” Identification Exposes the Internal Inconsistency of Ground 2 .....	42
2.	A POSITA Would Not Have Imported Nakhjiri’s ECDH Exchange into Ala-Laurila, and the Petition’s Proposed Modification Fails to Satisfy Limitation 1(e) .....	46
3.	Nakhjiri Teaches Away from Exposing Public Keys .....	50
4.	Nakhjiri’s Seed-based Key Derivation Is Infeasible in Ala-Laurila’s Architecture of Unrelated WLAN Access Points .....	51
5.	No Reference Teaches that Parameters Received in an Encrypted Profile From One Server Be Used for a Subsequent ECDH Exchange with a Different Server .....	52
VII.	Conclusion .....	53

## TABLE OF AUTHORITIES

### Cases

<i>Ashland Oil, Inc. v. Delta Resins &amp; Refractories, Inc.</i> , 776 F.2d 281 (Fed. Cir. 1985) .....	18
<i>Chemours Co. FC, LLC v. Daikin Indus.</i> , 4 F.4th 1370 (Fed. Cir. 2021) .....	21
<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015) .....	17
<i>Harmonic Inc. v. Avid Tech., Inc.</i> , 815 F.3d 1356 (Fed. Cir. 2016) .....	17
<i>In re Gurley</i> , 27 F.3d 551 (Fed. Cir. 1994) .....	18, 19
<i>In re Lee</i> , 277 F.3d 1338 (Fed. Cir. 2002) .....	17
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016) .....	16, 17, 24
<i>In re NuVasive, Inc.</i> , 842 F.3d 1376 (Fed. Cir. 2016) .....	17
<i>In re Van Os</i> , 844 F.3d 1359 (Fed. Cir. 2017) .....	18
<i>In re Warsaw Orthopedic, Inc.</i> , 832 F.3d 1327 (Fed. Cir. 2016) .....	17
<i>Interconnect Planning Corp. v. Feil</i> , 774 F.2d 1132 (Fed. Cir. 1985) .....	29, 53
<i>Orexo AB v. Actavis Elizabeth LLC</i> , 903 F.3d 1265 (Fed. Cir. 2018) .....	29, 53
<i>TikTok Inc. v. NTECH Props., Inc.</i> , IPR2024-01339, Paper 9 (P.T.A.B. 2025).....	23
<i>TQ Delta, LLC v. Cisco Sys.</i> , 942 F.3d 1352 (Fed. Cir. 2019) .....	18
<i>W.L. Gore &amp; Assocs. v. Garlock, Inc.</i> , 721 F.2d 1540 (Fed. Cir. 1983) .....	18
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (P.T.A.B. 2022).....	23

### Statutes

35 U.S.C. § 312 .....	17, 23
-----------------------	--------

**Regulations**

37 C.F.R. §42.104 .....23

**EXHIBIT LIST**

<b>Exhibit</b>	<b>Description</b>
EX2001	Complaint for Patent Infringement, <i>Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.</i> , EDTX-2-25-cv-00667, Dkt. 1 (June 27, 2025)
EX2002	Docket Control Order, <i>Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.</i> , EDTX-2-25-cv-00667, Dkt. 26 (Oct. 10, 2025)
EX2003	U.S. Patent No. 11,606,204
EX2004	U.S. Patent No. 11,973,864
EX2005	<i>Reserved</i>
EX2006	U.S. Patent No. 11,233,780
EX2007	U.S. Patent No. 12,207,094
EX2008	U.S. Patent No. 11,916,893
EX2009	6/28/2017 Information Disclosure by Applicant for Application No. 14/884,870
EX2010	2/9/2021 Information Disclosure by Applicant for Application No. 17/171,396
EX2011	U.S. Patent No. 10,187,206
EX2012	5/25/2017 Notice of References Cited for Application No. 14/718,619
EX2013	9/17/2019 Notice of References Cited for Application No. 16/248,090
EX2014	8/7/2019 Non-Final Office Action for Application No. 16/125,586
EX2015	Diffie, W. and Hellman, M. E., "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT.22, No. 6 (Nov. 1976)
EX2016	Defendants' Patent Local Rule 3-3 Disclosure of Invalidity Contentions, <i>Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.</i> , EDTX-2-25-cv-00667 (December 9, 2025)
EX2017	U.S. Patent No. 8,761,390
EX2018	Declaration of R. Allan Bullwinkel in Support of Patent Owner's Discretionary Denial Brief
EX2019	Declaration of John Nix in Support of Patent Owner's Discretionary Denial Brief
EX2020	Email chain dated September 27, 2016, produced with Bates

	Nos. NWO SAM 00013288–90
EX2021	Email chain dated December 21, 2016, produced with Bates No. NWO SAM 00013295
EX2022	“Patent Portfolio for ‘Embedded SIMs’ and the ‘Internet of Things,’” produced with Bates Nos. NWO_SAM_00013436–37
EX2023	Email chain dated January 3, 2017, produced with Bates Nos. NWO SAM 00013296–97
EX2024	Declaration of Dr. Konstantinos Psounis
EX2025	CV for Dr. Konstantinos Psounis
EX2026	Excerpts from A. Menezes , P. Oorschot, & S. Vanstone, <i>Handbook of Applied Cryptography</i> (1997)

## I. Introduction

The '869 Patent invention enables a mobile device to securely connect to a wireless network using two sequential cryptographic exchanges. First, the device receives an encrypted profile—containing its network identity and security credentials—from a provisioning server and decrypts it. Second, the mobile device generates a fresh set of keys using parameters from that decrypted profile and transmits its identity in encrypted form to a different server to authenticate with a mobile network. The two exchanges are linked: the cryptographic parameters delivered during provisioning are reused in the authentication phase. This linkage is an architectural core of the invention, cryptographically connecting provisioning with authentication and providing heightened security in both phases.

The Petition stitches together three references for each of its two principal Grounds, yet the resulting combinations fail to replicate this architecture.

Nakhjiri fails to teach a private key be *stored* in the device's embedded secure element (the eUICC). Nakhjiri's design *avoids* private key storage—it identifies key storage as a problem for memory-constrained devices and solves it by deriving keys on the fly from a pre-loaded seed so the device “only needs to store the seed.” The Petition asks the Board to modify Nakhjiri to do precisely what it was designed not to do—a textbook case of teaching away. Furthermore, the Petition fails to show that Nakhjiri's profiles include the identified “cryptographic parameters.”

Regarding Jeong, the Petition fails to show that its “cryptographic parameters” are received in an encrypted profile. The Petition ignores the claim’s requirement that the cryptographic parameters used in the second exchange are *the same* parameters received in the encrypted profile during the first exchange. The Petition identifies parameters from one reference for the first exchange, and different parameters from a different reference for the second exchange—delivered through different mechanisms, at different times, by different entities—and simply ignores the requirement that they must be the same.

Jeong also fails to teach generating the new public/private key pair required for the second exchange of the claim. Instead, Jeong’s authentication protocol encrypts the device’s identity using a shared secret key derived from *static, pre-registered* keys that are established when the device is registered—not from dynamically generated keys as claimed. Jeong designed its protocol this way for a specific reason: the device must encrypt its identity in the very first message of the authentication sequence, before any interactive key exchange can occur. Replacing that static key with a dynamic exchange, as the Petition proposes, would fundamentally break Jeong’s protocol by leaving the device’s identity unprotected at the moment it is most vulnerable.

In Ground 2, the Petition substitutes Ala-Laurila for Jeong, but Ala-Laurila is no better and falls far short of the claimed invention. The Petition fails to consistently

identify a “second server” in Ala-Laurila: it points to two servers in two different networks to satisfy the “second server” requirement for one limitation and a single server to satisfy that “second server” requirement in another limitation, exposing an internal inconsistency that the Petition never reconciles. And the Petition relies on a single sentence referencing “the Diffie-Hellman algorithm”—with no discussion of public keys, private keys, key generation, or exchange mechanics—to satisfy multiple limitations of the independent claim. The Petition attempts to fill this gap by importing Nakhjiri’s key derivation process, but that process—which relies on a pre-shared seed and a deterministic key generator function—would produce the *same* private key as the first exchange, not the *second* private key required by the claims. Importing Nakhjiri poses additional problems, including teaching away from exposing public keys and requiring seed storage that directly counters Ala-Laurila’s stated goals.

In short, the Petition does not present a coherent theory of obviousness. It relies on a primary reference that teaches away from a threshold requirement, ignores the claim’s structural linkage between its two cryptographic phases, and depends on secondary references that either lack the required teachings or would require modifications that conflict with their own designs. The Board should deny institution.

## **II. Background**

### **A. State of the Art**

At the time of the invention (November 2013), wireless wide-area networks such as 3GPP's 3G UMTS and 4G LTE relied on a security architecture built around a pre-shared secret key K. This key K, along with a subscriber identity (such as an International Mobile Subscriber Identity, or IMSI) and network parameters, was physically recorded on a universal integrated circuit card ("UICC")—the familiar SIM card—and distributed to end users for insertion into mobile phones and modules. EX1001 at 2:54-65. Both the network operator and the UICC stored matching copies of key K, and this shared secret key served as the root of trust for authentication and session-key derivation under ETSI and 3GPP standards. EX1001 at 3:57-65.

This physical-SIM model worked tolerably for consumer handsets, where users could manually swap cards and the secret key was embedded in a physical SIM card. But the rapid growth of "machine-to-machine" (M2M) communications—remote sensors, vehicle telematics, shipping-container trackers, health monitors, and the broader "Internet of Things"—created a significant new class of problems that required more flexibility in the manner in which key information was exchanged and heightened security measures. EX1001 at 1:63-2:10 (detailing M2M applications);

*id.* at 2:44-4:48 (detailing new problems related to remote provisioning of network credentials).

**B. Problems with the State of the Art**

The physical distribution of UICCs became increasingly impractical as M2M modules proliferated. These modules are often deployed in remote, sealed, or mobile locations—shipping containers traversing the globe, industrial sensors in the field, medical monitors on patients—where physically replacing a SIM card is difficult, expensive, or impossible. EX1001 at 3:13-31. The industry recognized this challenge and began developing the embedded UICC (eUICC), which virtualizes the SIM so that profiles containing key K, an IMSI, and network parameters can be delivered to mobile devices and M2M modules electronically rather than on a physical card. EX1001 at 3:33-36.

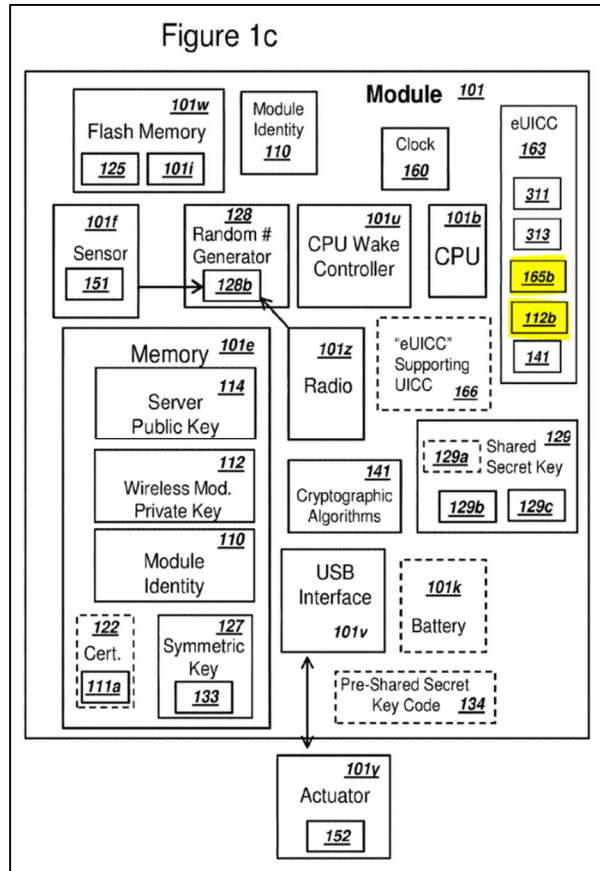
Although the eUICC eliminated the need for physical card swaps, it did not solve the deeper security problems introduced by the eUICC model. This new model required key K to be transmitted electronically to the eUICC, typically through third-party subscription managers in encrypted form. EX1001 at 4:4-25. The security of electronically transferred key K was therefore only as strong as the delivery channel's encryption and the trustworthiness of the intermediaries—entities potentially outside the network operator's control. EX1001 at 4:15-25. Moreover, with conventional technology a single key K remained in use for the lifetime of the

mobile device. Extended use of one key over years of encrypted data transmissions creates exposure to cryptanalytic attack, especially as data volumes grow. With conventional physical SIM technology, the only way to change key K was to physically distribute a new UICC, which was costly and complex. EX1001 at 4:26-46. Compounding these security challenges, any proposed solution had to remain compatible with the massive installed base of PLMN infrastructure that uses a pre-shared secret key K as the foundation for authentication and ciphering. EX1001 at 3:57-65.

### **C. The '869 Patented Invention**

The '869 Patent claims solve these problems through a cryptographically connected, two-phase approach in which a mobile device with an eUICC securely establishes communication with a wireless network. *See* EX2024 ¶¶ 29, 35-36. The solution uses two distinct elliptic curve Diffie-Hellman (ECDH) key exchanges that work in concert: the first secures delivery of the eUICC profile from a first server, and the second—using freshly generated keys and parameters obtained from that profile—secures the module's transmission of its identity to the mobile network via a second server for authentication. *See* EX1001 at 148:4-31 (claim 1). The claim 1 solution provided by the '869 Patent is detailed below with reference to disclosed specification embodiments.

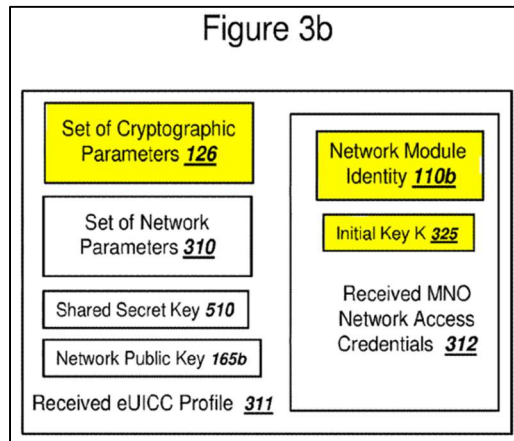
In the first phase, the eUICC stores an initial module private key, a corresponding module public key, and a network public key. EX1001 at 148:8-10. Figure 1c illustrates the components of a module, which can be a mobile device, such as a cellular phone. See EX1001 at 13:5-11.



EX1001 at Fig. 1c (annotated). The network public key 165b and module private key 112b (both highlighted in yellow) are stored in an eUICC that forms part of the mobile device module. See EX1001 at 23:22-24. The module also stores a module private key 111b. See EX1001 at Fig. 1a, 15:24-26.

The module receives, from a first server associated with the wireless network—which according to the preferred embodiment may be operated by an

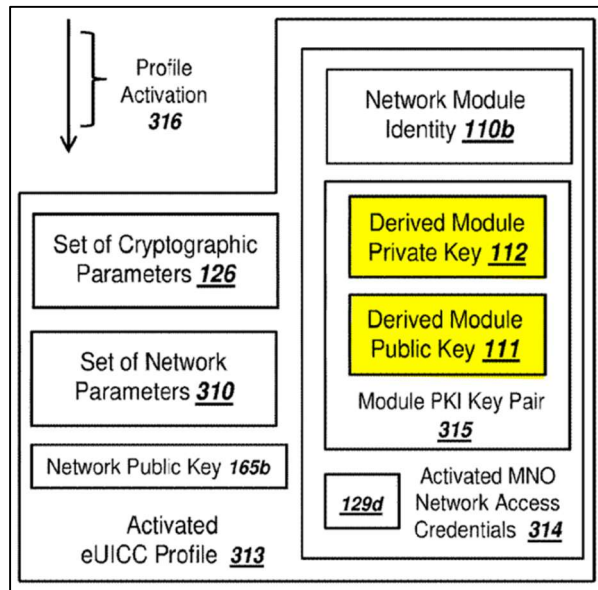
eUICC subscription manager—an encrypted eUICC profile containing cryptographic parameters, a module identity such as an IMSI, and a key K. EX1001 at 148:11-14. Figure 3b illustrates an exemplary received eUICC profile:



EX1001 at Fig. 3b (excerpted and annotated); *see id.* at 61:53-57 (describing key K); *id.* at 62:22-28 (describing cryptographic parameters and module identity).

The module then performs a first ECDH key exchange using its stored module private key and the network public key to generate a shared secret key. EX1001 at 148:15-17; *see also id.* at 61:14-25 (describing generation of a shared secret key). This shared secret key is used to decrypt a portion of the received profile. EX1001 at 148:18-19; *see also id.* at 61:25-32 (describing profile decryption). Because both sides (the module 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.

In the second phase, the eUICC generates a second module public key and corresponding second module private key. EX1001 at 148:20-21. These keys are illustrated in the activated eUICC profile of Figure 3b:



EX1001 at Fig. 3b (excerpted and annotated); *see also id.* at 133:39-42 (describing derivation of new module public and private keys using the cryptographic parameters). The module sends this newly generated second public key to a second server associated with the wireless network. EX1001 at 148:22-23; *see also id.* at 134:39-41.

The module then performs a second ECDH key exchange, using the second module private key and the cryptographic parameters from the profile, to generate a symmetric key. 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 module encrypts data that includes the module

identity and sends this encrypted data to the second server. EX1001 at 148:27-31; *see also id.* at 138:4-7, 138:16-19 (detailing sending message including an encrypted module identity 110a). This allows the module to authenticate itself to the network using keys that did not exist until the module generated them from the decrypted profile.

The two phases are interdependent: the cryptographic parameters within the decrypted profile directly enable the second exchange, and the freshly generated key pair ensures that compromise of the initial private key would not expose the module's identity transmission. 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.

#### **D. Petitioners' References**

The Petition relies on seven references to support its eight Grounds. This Preliminary Response focuses on Grounds 1 and 2—the only Grounds addressing

the only independent claim of the '869 Patent.<sup>1</sup> Accordingly, only the references relevant to Patent Owner's Preliminary Response arguments are addressed below.

**1. Nakhjiri [EX1005]**

Nakhjiri, 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)," is directed to the secure remote provisioning of profiles from application service providers to target devices such as smartphones containing embedded UICCs. The reference addresses the challenge of securely transmitting profiles through a provisioning infrastructure that includes a source node associated with a mobile network operator (MNO), intermediate nodes including a Subscription Manager-Data Preparation (SM-DP), and the target device. *See* EX1005 at Abstract, 2:34-42, 2:50-58.

To provide end-to-end protection, the SM-DP server encrypts the profile and delivers the encrypted profile and the MNO's public key (MNO\_ECC\_PLKOP) to the target device. EX1005 at 5:53-58. The target device's UICC then derives a

---

<sup>1</sup> For the purposes of this Preliminary Response, Patent Owner has focused on independent Claim 1. If trial is instituted, then Patent Owner reserves the right to further address additional deficiencies in the Petition's theories, including deficiencies regarding the dependent claims.

private key from its pre-stored private seed and a mobile network operator ID (MNO\_ID). EX1005 at 5:61-64. Next, the device uses the derived private key and the MNO's public key to perform its own ECDH key agreement, derive the same PEK, and decrypt the profile for secure storage. EX1005 at 5:61-6:2.

Nakhjiri relies on a key generator function to derive private keys based on a private seed stored in the target device and mobile network operator ID. *See* EX1005 at 4:45-50. Nakhjiri explains that *storing* keys in the UICC creates storage problems. *See id.* at 4:14-16 (“Both with global MNO key pairs and unique UICC key pairs, there may be *storage problems for memory-constrained UICCs . . .*”). Thus, Nakhjiri implemented its key derivation solution (based on a key generator function and private seed) to avoid such problems. *See id.* 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 [private keys] for multiple MNOs as well as certificates for those MNOs[]).”); *id.* at 5:21-22 (identifying “the purpose of using ECC and *private seeds* for storage space optimization”); *see also* EX2024 ¶¶ 40-41.

Nakhjiri's disclosure is expressly confined to the profile provisioning process—that is, the secure delivery of sensitive data from a provisioning server (e.g., the MNO's SM-DP) to the target device's UICC. The ECDH key exchange it teaches takes place between the SM-DP server and the UICC, using elliptic curve

cryptography (ECC) parameters including the ECC curve and base point. EX1005 at 4:51-56. These parameters exist in the context of that provisioning relationship.

Nakhjiri does not address any step of network authentication after provisioning. It does not describe the UICC using the profile or its cryptographic parameters to authenticate with another server. The reference's scope begins with the SM-DP server's preparation of the encrypted profile and ends with the UICC's decryption and storage of that profile.

## **2. Jeong [EX1007, EX1012]**

Jeong, a 2010 academic paper published in the Journal of Korea Multimedia Society, is titled "A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment." The paper describes a modified Authentication Key Agreement ("AKA") module for a mobile payment system suited to smartphones that operate in an "open" environment. EX1007 at Abstract, 0003 (§1 Introduction). The system involves a mobile station (MS), a serving network (SN), and a certificate authority designated as the home network (HN). *See* EX1007 at 0008 (Fig. 6). Jeong identifies several problems with the existing 3GPP-AKA protocol, including the sequence number synchronization problem, false base station attacks, bandwidth consumption between the SN and certificate authority, and—most relevant here—the "privacy problem due to IMSI plaintext transmission in the existing 3GPP-AKA mutual authentication." EX1007 at 0008 (§3.2). To

address the IMSI exposure problem, Jeong proposes encrypting the IMSI using a shared secret key between the MS and the HN ( $SSK_{MS-HN}$ ) derived via the EC-DH algorithm. EX1007 at 0008 (§3.2(1)). Then, the encrypted IMSI ( $E-IMSI_{MS}$ ) is transmitted to the SN and forwarded to the HN for decryption and identity verification. EX1007 at 0008 (§§3.2(1)-(3)); *id.* at 0009 (§4.1.2).

Jeong's design makes a deliberate architectural distinction between two categories of shared secret keys.  $SSK_{MS-HN}$ —the key between the MS and the certificate authority (HN) used to encrypt the IMSI—is a static, long-term key. Jeong explains that this key “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 . . . .” EX1007 at 0009 (§4.1.1(1)). This key is established once during the USIM registration phase and persists for the life of that registration—*i.e.*, it is a static key.

By contrast, Jeong's  $OT-SSK_{MS-SN}$ —the one-time shared secret key between the MS and the SN—is generated dynamically for each session through a protocol-based ECDH exchange. *See* EX1007 at 0008 (lower portion of Fig. 6). For the protocol-based ECDH exchange, the SN transmits its public key SNP and the initial point P to the MS; the MS generates  $OT-SSK_{MS-SN}$  using its own secret key; and the parties derive session encryption and integrity keys CK and IK from that one-time key. EX1007 at 0009 (§§3.2(5)–(8)). Jeong specifically identifies this 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). This two-tier 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 core feature of Jeong’s design.

### 3. Ala-Laurila [EX1013]

Ala-Laurila, titled “Arranging Data Ciphering in a Wireless Telecommunication System,” 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 such as a GSM network (GSMNW). The system involves the MT, which contains a subscriber identity module (SIM), communicating with a Public Access Controller (PAC) that controls access to the WLAN, and a GSM/GPRS Authentication and Billing Gateway (GAGW) that is “an entity in the mobile network GSMNW offering authentication services of mobile subscribers to the WLAN networks . . . .” EX1013 ¶ [0022].

Ala-Laurila recognized the problem of needing to store in advance the ciphering keys needed for encrypting traffic. *See* EX1013 ¶ [0004] (“However, a problem in some wireless telecommunication networks, such as IEEE802.11 WLAN networks, is that the ciphering keys used for ciphering traffic must be stored in

advance in the terminal and access point.”). And it sought to address these problems with its solution: “*[i]t 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.*” *Id.* ¶ [0005] (emphases added).

Referring to Figure 2, an MT seeking to connect to the WLAN first retrieves the IMSI identifier from its SIM (step 202) and sends an authentication starting request (MT\_PAC\_AUTHSTART\_REQ, step 204) to the PAC containing a Network Access Identifier (“NAI”) that “comprises the IMSI identifier obtained from the identity module SIM.” EX1013 ¶ [0026], Fig. 2. Ala-Laurila states that this request “is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm, for example.” EX1013 ¶ [0026]. Notably, Ala-Laurila provides no further detail regarding this Diffie-Hellman algorithm—there is no discussion of public/private keypair generation, elliptic curve parameters, key exchange mechanics, or how a symmetric key is derived from the exchange.

### III. Legal Standards

An IPR should not be instituted unless Petitioner has shown a likelihood of success on the invalidity grounds *presented in the petition*. See *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016) (“[T]he Board must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond.”).

“In an IPR, the petitioner has the burden from the onset to show *with particularity* why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016); *see also* 35 U.S.C. § 312(a)(3) (requiring petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”). This burden of persuasion never shifts to the patent owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l*, 829 F.3d at 1380. The obviousness inquiry requires considering whether one of skill in the art “would have been motivated to combine the prior art to achieve the claimed invention.” *In re NuVasive, Inc.*, 842 F.3d 1376, 1381 (Fed. Cir. 2016) (quoting *In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016)). “[T]he factual inquiry whether to combine references must be thorough and searching...” *Id.* at 1382-82 (quoting *In re Lee*, 277 F.3d 1338, 1343 (Fed. Cir. 2002)).

“A reference, however, must have been considered for all it taught, disclosures that diverged and taught away from the invention at hand as well as disclosures that pointed towards and taught the invention at hand.” *Ashland Oil, Inc. v. Delta Resins*

*& Refractories, Inc.*, 776 F.2d 281, 296 (Fed. Cir. 1985) (citing *W.L. Gore & Assocs. v. Garlock, Inc.*, 721 F.2d 1540, 1550 (Fed. Cir. 1983)). “A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant.” *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994).

“[C]onclusory expert testimony is inadequate to support an obviousness determination . . . .” *TQ Delta, LLC v. Cisco Sys.*, 942 F.3d 1352, 1359 (Fed. Cir. 2019). “[C]rediting such testimony risks allowing the challenger to use the challenged patent as a roadmap to reconstruct the claimed invention using disparate elements from the prior art—i.e., the impermissible *ex post* reasoning and hindsight bias that *KSR* warned against.” *Id.* at 1361 (citing *In re Van Os*, 844 F.3d 1359, 1361 (Fed. Cir. 2017)).

#### **IV. Level of Ordinary Skill in the Art**

For purposes of this Preliminary Response, Patent Owner does not contest the Petition’s recitation of the level of skill in the art, because even under that proposed level of skill (Pet. at 8), the Petition fails to demonstrate a reasonable likelihood of success. Patent Owner reserves the right to propose its own definition of a person of ordinary skill in the art in the future if necessary.

## V. Claim Construction

Petitioner contends that no terms require construction. Pet. at 9. For the purpose of this Preliminary Response, Patent Owner agrees.

## VI. Argument

The Board should deny institution because each of Nakhjiri, Jeong, and Ala-Laurila fails to teach multiple limitations of independent claim 1.

### A. Nakhjiri Fails to Teach Multiple Limitations of Claim 1 (All Grounds)

First, Nakhjiri teaches away from storing private keys as required by Limitation 1(a). The Petition incorrectly alleges that Nakhjiri teaches storing private keys. However, Nakhjiri promotes its *seed-based* solution for deriving private keys as an improvement that avoids the problems caused by storing keys in memory-constrained UICCs. Second, the Petition has failed to show that Nakhjiri's profiles include the cryptographic parameters required by Limitation 1(b). Nakhjiri does not say the required cryptographic parameters are included in its profile, and the Petition fails to show that the parameters are necessarily included in Nakhjiri's profile.

#### 1. Nakhjiri Teaches Away From Storing a Private Key in the eUICC

*Limitation 1(a): "storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key;"*

Nakhjiri fails to teach storing a first module private key in the eUICC as required by Limitation 1(a) and instead teaches away from such retention. *See In re Gurley*, 27 F.3d at 552.

In Nakhjiri, the private key identified by the Petition—MNO\_ECC\_PVKDEV—is derived on-the-fly by a key generator function (KGF) using a private seed and a mobile network operator id (MNO\_ID). *See* EX1005 at 5:61-64, 4:45-50. Nakhjiri teaches this approach for generating the private key to **avoid** storing public/private keys in the UICC. The reference identifies problems with storing public or private keys in the UICC. *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 . . .**”); EX2024 ¶ 59.

Nakhjiri explains that requiring stored key pairs for each mobile network operator (MNO) could quickly exhaust the limited memory of a UICC. *See* EX1005 at 4:14-20. Additionally, storing keys in this manner would have eliminated support for new MNOs that came into existence after the key pairs had “been pre-loaded in the UICC.” *See id.* at 4:20-23. Nakhjiri’s solution—using a pre-stored private seed and key generator function to generate keys—avoids these specifically identified key storage problems. *See* 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 [private keys] for multiple MNOs as well as certificates for those MNOs[)].”); *id.* at 5:21-22 (identifying “the purpose of using ECC and **private seeds** for storage space optimization”). The Petition

proposes a modification of Nakhjiri—*i.e.*, storage of private keys or PVKs—that contradicts its explicit teachings. *See* EX2024 ¶¶ 61-64

In *Chemours Co. FC, LLC v. Daikin Indus.*, the Federal Circuit reversed the PTAB’s obviousness decision when the proposed modification or combination would involve altering the inventive concept or teaching of the underlying reference. *See Chemours Co. FC, LLC v. Daikin Indus.*, 4 F.4th 1370, 1373 (Fed. Cir. 2021). The reference taught the importance of a narrow molecular weight distribution for the polymer at issue. *See id.* at 1375 (“Kaulbach highlights that the polymer of the invention has a ‘very narrow molecular weight distribution.’”). However, the Board adopted a modification or combination based on that reference in which the molecular weight distribution would be broadened, contrary to the teachings of the reference. *See id.* at 1376 (quoting the Board’s reasoning at J.A. 51). The Federal Circuit reversed, finding that the Board failed to articulate an adequate evidentiary basis “for why a POSA would have been motivated to increase Kaulbach’s melt flow rate to the claimed range, when doing so would necessarily involve altering the inventive concept of a narrow molecular weight distribution polymer.” *Id.* at 1377.

Here, the Petition invites similar error with its proposed modification of Nakhjiri to store private keys in the UICC despite Nakhjiri’s warnings about space problems with UICCs and key storage. Nakhjiri’s solution avoids such space problems by using a key generator function to generate private keys based on a pre-

stored private seed and a MNO ID (per mobile network operator), thus allowing keys to be generated for each mobile network operator without imposing onerous storage requirements. Because Nakhjiri teaches away from storing private keys in the UICC, which is required by all claims, the Petition fails to show a reasonable likelihood that Petitioners would prevail on any asserted Ground.

## **2. Nakhjiri's Profile Does Not Include the Petition's Identified Parameters**

*Limitation 1(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;"*

The Petition maps the Limitation 1(b) "cryptographic parameters" to ECC parameters such as the curve identifier and base point G. *See* Pet. at 32. However, the Petition fails to show that the identified parameters are included in Nakhjiri's profile that is transmitted to a mobile device. Nakhjiri explains that the profile may include "security application algorithm codes, data and cryptographic keys." EX1005 at 2:4-6 (cited by Pet. at 32). The Petition summarily asserts that a POSITA would have understood these items to be "cryptographic parameters," then takes *another* inferential leap and asserts that they would include "ECC parameters (curve ID and base point G) used later by [Nakhjiri's] eUICC." *See* Pet. at 32.

First, the Petition never explains why a POSITA would have understood "security application algorithm codes, data and cryptographic keys" to be "cryptographic parameters." Rather, it only provides a conclusory allegation. The

Petition cites to testimony by Dr. Rangan to support the chain of inference relied on to map Nakhjiri's disclosure to "cryptographic parameters." *See* Pet. at 32 (citing EX1002 ¶¶94). However, the cited expert testimony is verbatim what is included in the Petition and thus provides no probative value.<sup>2</sup> *See Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15-16 (P.T.A.B. 2022) (precedential); *TikTok Inc. v. NTECH Props., Inc.*, IPR2024-01339, Paper 9 at 16 (P.T.A.B. 2025) (finding that "verbatim" testimony mimicking the Petition is "entitled to little weight"). In a footnote, the Petition (and expert declaration) asserts that cryptographic parameters are "conventionally the curve identifier and base point G used in key agreement." Pet. at 32. n.7. For support, the Petition cites two Sections (spanning over 30 pages) of a document regarding elliptic curve cryptography (*see id.*); however, the Petition fails to identify any particular passages in those 30 pages supporting its conclusory assertions about cryptographic parameters being provided in Nakhjiri. *See* 35 U.S.C. §312(a)(3) (requiring that "the petition identifies, in writing and with particularity . . . the evidence that supports the grounds"); 37 C.F.R. §42.104(b)(5) (requiring "identifying specific portions of the evidence that support the challenge"). The cited pages are highly technical, and the Petition makes no attempt to explain

---

<sup>2</sup> Aside from the Introductory material and Technological Background (EX1002 ¶¶ 1-52), Dr. Rangan's testimony is a near-identical copy of the Petition.

how the exhibit relates to Petitioners' conclusory statement about conventional cryptographic parameters.

Nakhjiri explains that its profile can include "an MNO-specific boot code," "a sequence number or a timestamp." EX1005 at 7:24-25, 7:49-51. Nakhjiri never states that the curve identifier and base point G are included in the profile transmitted from the subscription manager server. And, it never states that the curve identifier and base point G are "security application algorithm codes, data and cryptographic keys." Therefore, the Petition merely alleges, without support from Nakhjiri, that the curve and base point G would have been included in Nakhjiri's received encrypted profile. Conclusory assertions without factual support are insufficient to carry Petitioners' burden to show a reasonable likelihood that Nakhjiri's profiles include "cryptographic parameters." *See In re Magnum Oil Tools Int'l*, 829 F.3d at 1380.

Furthermore, the Petition fails to show that Nakhjiri inherently discloses that the profiles include the required cryptographic parameters. *See In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) ("Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." (internal citations omitted)). This deficiency provides an independent basis to reject all Grounds, which rely on Nakhjiri's teachings for the Limitation 1(b) cryptographic parameters.

**B. Jeong Fails to Teach Multiple Limitations and Would Not Have Been Modified as the Petition Proposes (Ground 1)**

For Ground 1, the Petition relies on Jeong to purportedly teach or disclose the latter limitations of Claim 1 (Limitations 1(e)-1(i)). However, the Petition's mapping of Jeong to these limitations ignores claim requirements, ignores Jeong's teachings, and proposes modifications to Jeong that would change its principle of operation.

First, the Petition fails to link the cryptographic parameters it identifies in Jeong for Limitation 1(g) to those it identifies in Nakhjiri for Limitation 1(b)—completely ignoring the claim's required link between those parameters. Second, Jeong does not disclose generating a second module public/private key pair as required by Limitations 1(e) and 1(g) because its shared secret  $SSK_{MS-HN}$  is derived from static, pre-registered keys established at initial USIM registration—not from a dynamically generated key pair. The Petition's proposed modification to replace this static key with a dynamic ECDH exchange would fundamentally alter Jeong's protocol and express design choices, changing its intended mode of operation in a manner counter to Jeong's design goals. Finally, because Jeong fails to disclose generating the second module public/private key pair, it also fails to teach sending the second module public key to a second server as required by Limitation 1(f).

**1. The Cryptographic Parameters Identified in Jeong Are Not Received in an Encrypted Profile**

*Limitation 1(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;**”*

*Limitation 1(g): “generating a symmetric key using a second ECDH key exchange with the second module private key and **the cryptographic parameters;**”*

Limitation 1(g) requires that a symmetric key be generated using “the cryptographic parameters,” which refers back to Limitation 1(b)’s cryptographic parameters that are included in the received encrypted profile for the eUICC. *See* EX1001 at 148:11-14, 148:24-26, 133:39-44. The claim thus requires that the same cryptographic parameters received in the encrypted profile from the first server be used in the second ECDH key exchange with the second server. This linkage is not incidental, and the Petition has ignored it.

The Petition maps the Limitation 1(b) “cryptographic parameters” to Nakhjiri’s ECC parameters such as the curve identifier and base point G. *See* Pet. at 32. These identified parameters exist solely within the context of provisioning a profile for the UICC. However, the Petition pivots to an entirely different source for the cryptographic parameters of Limitation 1(g). It maps “**the** cryptographic parameters” to Jeong’s “initial point P,” asserting that “[a] POSITA would have understood that ‘the initial point’ P is a cryptographic parameter of the ECDH algorithm.” Pet. at 43. But Jeong’s initial point P, which is used in the derivation of

the shared secret  $SSK_{MS-HN}$ , is not received in an encrypted profile from a provisioning server—it is “registered in the USIM card and the certificate authority when the USIM card is first registered . . . .” EX1007 at 0009 (§4.1.1). It is a registration-time parameter, established during USIM manufacturing or initialization, that has no connection to any encrypted profile received from a subscription management server.

The Petition thus relies on two different sets of parameters from two different references, delivered through two entirely different mechanisms, at two different points in time, and simply assumes—without explanation—that they are the same parameters. Nakhjiri’s ECC curve ID and base point G are provisioning-context parameters *purportedly* delivered in an encrypted profile from the SM-DP server. Jeong’s initial point P is a registration-context parameter pre-installed in the USIM at the time of initial registration with the certificate authority.

The Petition asserts only that P is “*a* cryptographic parameter of the ECDH algorithm” for Limitation 1(g). Pet. at 43. While this may be true as a generic matter, it does not address the claim’s requirement that the parameter used in Limitation 1(g) overlap with the cryptographic parameters received in Limitation 1(b). The use of the indefinite article “*a*” in the Petition’s characterization of its identified Limitation 1(g) “cryptographic parameters” underscores the deficiency: the claim does not require merely that *any* cryptographic parameter be used, but that

cryptographic parameters *from the encrypted profile* be used. The Petition offers no evidence that any reference teaches this linkage.

The Petition's deficiencies here are compounded by errors addressed elsewhere: Nakhjiri does not teach that the identified parameters are included in the profile (*see supra* Section VI.A.2), and Jeong fails to teach an ECDH exchange between the MS and HN (*see infra* Section VI.B.2). But even setting those failures aside, the Petition never explains how or why the cryptographic parameters purportedly delivered in Nakhjiri's encrypted profile would be the same parameters used in a subsequent ECDH exchange between the mobile station (MS) and Jeong's Home Network (HN). This gap is particularly glaring given that Jeong's HN is not an SM-DP profile provisioning server as disclosed in Nakhjiri.

Nor does the Petition's reliance on the analogy to Jeong's MS-SN exchange cure this deficiency. *See* Pet. at 42-43 n.11. In the MS-SN exchange, the initial point P is transmitted from the Serving Network (SN) to the Mobile Station (MS) at step (5) of Jeong's protocol (EX1007 at 0009 (§3.2(5))), not received as part of an encrypted profile from a provisioning server. Even within Jeong's own system, the parameter P used for the OT-SSK<sub>MS-SN</sub> exchange is delivered through a different mechanism than the one required by the '869 claims. Finally, applying Nakhjiri's ECDH process to Jeong's MS-HN exchange, as the Petition proposes (*see* Pet. at 42-43), still does not answer the question of where the cryptographic parameters come

from—and specifically, whether they come from the encrypted profile received from a first server as the claim requires.

In short, the Petition never acknowledges that the Limitation 1(g) parameters must be the same parameters received in the Limitation 1(b) encrypted profile. This is not a minor detail—the claim structure requires that parameters flow from provisioning to authentication, and it is precisely this continuity that the Petition’s combination fails to replicate. The Petition’s proposed combination relies on the claims as a blueprint to cherry-pick components from disconnected references to purportedly satisfy the limitations. This is nothing more than hindsight bias. *See Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1138 (Fed. Cir. 1985) (“The invention must be viewed not with the blueprint drawn by the inventor, but in the state of the art that existed at the time.”); *see also Orexo AB v. Actavis Elizabeth LLC*, 903 F.3d 1265, 1271 (Fed. Cir. 2018).

Because the Petition fails to link “the cryptographic parameters” of Limitation 1(g) to the cryptographic parameters received in the encrypted profile at Limitation 1(b), it has not established that the Ground 1 combination teaches every element of Claim 1.

**2. Jeong’s Static, Pre-Registered Keys Do Not Disclose “Generating” a Second Key Pair or Symmetric Key**

*Limitation 1(e): “generating, by the eUICC, a second module public key and a corresponding second module private key;”*

*Limitation 1(g): “generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;”*

The Petition alleges that “a POSITA would have understood that Jeong’s MS would generate a public/private key pair ( $d_{MS}/Q_{MS}$ ) for the ECDH exchange with HN.” Pet. at 40. It then alleges that the “symmetric key” corresponds to  $SSK_{MS-HN}$ . See Pet. at 43-44. These arguments are wrong for at least three reasons. First, Jeong affirmatively teaches that the  $SSK_{MS-HN}$  key is generated from pre-registered, static keys at initial USIM registration. Second, Petitioners’ arguments ignore Jeong’s express teachings regarding generation of the  $SSK_{MS-HN}$ . Third, the Petition’s proposed modification fundamentally rewrites Jeong’s security protocols, changing the principle of operation for the system and its resulting benefits.

**(a) Jeong’s  $SSK_{MS-HN}$  Is Generated from Pre-registered, Static Values**

To understand the Petition’s failure regarding Limitation 1(e), it is necessary to look forward to Limitation 1(g) and the Petition’s identification of the symmetric key generated by using the Limitation 1(e) second module private key. The Petition identifies Jeong’s shared secret— $SSK_{MS-HN}$ —as the Limitation 1(g) symmetric key, which must be generated using the second module private key from Limitation 1(e). See Pet. at 43-44; see also EX1001 at 148:20-21, 148:24-26. Jeong teaches that the shared secret  $SSK_{MS-HN}$  is used to encrypt data communications between the mobile station (MS) and Home Network (HN) so the HN can authenticate the MS. Jeong’s

Figure 6 illustrates this process.

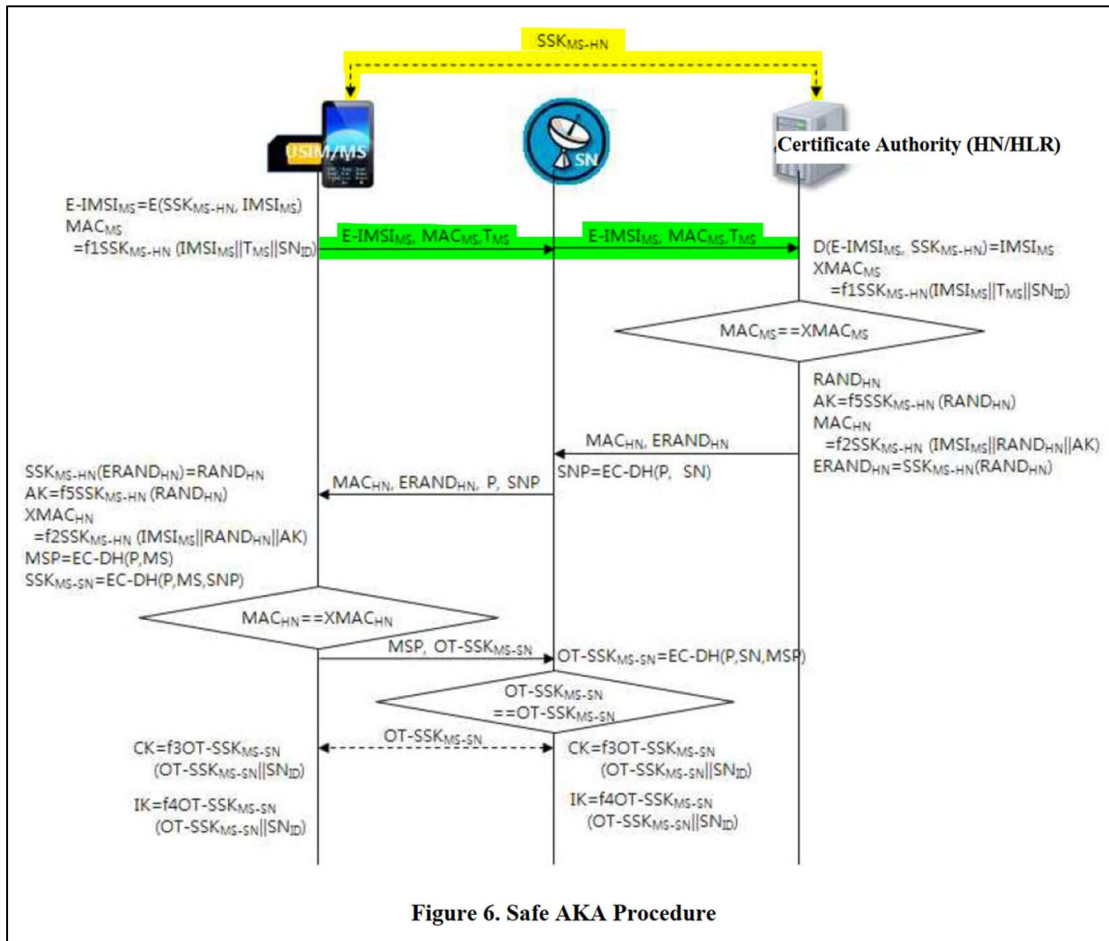


Figure 6. Safe AKA Procedure

EX1007 at 0008 (annotations added). The dotted-line at the top of this figure (highlighted yellow), labeled  $SSK_{MS-HN}$ , illustrates that communications between the USIM/MS and Certificate Authority (HN/HLR) are encrypted using the shared secret  $SSK_{MS-HN}$ . The first transmission in the Safe AKA Procedure from the MS to the HN (via the SN) is illustrated by the top line (highlighted green) and includes transmission of the  $E-IMSI_{MS}$ ,  $MAC_{MS}$ , and  $T_{MS}$  values. These values are encrypted using  $SSK_{MS-HN}$  at the MS, sent to the SN, and forwarded to the HN. See EX1007 at 0008 (§3.2(2)) (“The SN forwards the received  $E-IMSI_{MS}$ ,  $MAC_{MS}$ ,  $T_{MS}$  to the

corresponding certificate authority (HN).”). Once these values are received by the HN, it “decrypts the  $E\text{-IMSI}_{MS}$  with the shared secret key  $SSK_{MS\text{-}HN}$  between the MS and HN . . . .” *Id.* (§3.2(3)).

Claim 1 of the ’869 Patent requires that this symmetric key be generated “using a second ECDH key exchange *with the second module private key*” of Limitation 1(e). *See* EX1001 at 148:20-26. However, Jeong’s  $SSK_{MS\text{-}HN}$  is not generated based on a second module private key generated by the mobile device. Instead, Jeong explains that  $SSK_{MS\text{-}HN}$  is generated from static credentials established during an advance registration phase:

The AKA module proposed in this paper uses  $SSK_{MS\text{-}HN}$ , a shared secret key based on the EC-DH algorithm, between the MS and the certificate authority (HN) for mutual authentication. *The shared secret key,  $SSK_{MS\text{-}HN}$ , 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)) (emphases adde).

Jeong’s “secret key registered in the USIM and the certificate authority” is not the claimed “second module private key” that must be generated by the mobile device. Rather, that “secret key registered in the USIM and the certificate authority” is a *shared key* between the USIM and the certificate authority, not a *private key* for the USIM and not generated by the mobile device, as required by Limitation 1(e).

As the underlined passage in the block quote above shows, Jeong explicitly indicated which values were “generated for mutual authentication” between the MS and HN (*i.e.*, the  $MAC_{MS}$  and  $XMAC_{MS}$ ). Thus, Jeong fails to teach or disclose “generating . . . a second module public key and a corresponding second module private key” as required by Limitation 1(e).

The Petition tacitly admits as much: “Jeong does not specifically provide identifiers for the public/private key pairs used to generate the  $SSK_{MS-HN}$  key . . . .” Pet. at 40.<sup>3</sup> The reason for Jeong’s lack of identifiers is simple—those keys do not exist. As detailed above, the  $SSK_{MS-HN}$  is generated from pre-registered, static keys provisioned to the MS and certificate authority (HN) at initial USIM registration, not from a module-generated public/private key pair. And that pre-registered static key (*i.e.*, the “secret key registered in the USIM and the certificate authority”) is not a private key for the USIM; it is shared between the USIM and the certificate authority.

**(b) The Petition Ignores Jeong’s Express Teachings**

To advance its claim mappings to Jeong, the Petition ignores Jeong’s teachings about how the  $SSK_{MS-HN}$  is generated based on shared secrets determined at registration (rather than on the fly). *See* Pet. at 39 (“Although Jeong states that

---

<sup>3</sup> Nonetheless, Petitioners manufactured identifiers for these missing keys in their claim elements charts. *See* Pet. at 41 (identifying  $Q_{MS}$  and  $d_{MS}$ ).

$SSK_{MS-HN}$  is derived between MS and HN using the ECDH algorithm, it does not describe that exchange in detail.”). But Jeong explains the derivation: “The AKA module of mobile payment system based on 3GPP-AKA protocol prevents the exposure of IMSI by creating the SSK (Shared safe Key) through advance registration . . . .” EX1007 at 0002 (Abstract); *see also id.* 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 specific design choice was adopted by Jeong to avoid sending the IMSI in plaintext for authentication. *See id.* at 0009 (§4.1.2) (“The AKA module proposed in this paper solves the privacy problem of IMSI plaintext transmission by encrypting IMSI with  $SSK_{MS-HN}$  and transmitting it to the certificate authority.”).<sup>4</sup> The Petition ignores these express teachings in Jeong about how the  $SSK_{MS-HN}$  is generated and the particular reasons for that design decision.

Continuing to ignore Jeong’s teachings about how the  $SSK_{MS-HN}$  is determined, the Petition alleges that “[i]t would have been obvious to a POSITA that

---

<sup>4</sup> The certified translation of Jeong (EX1007) refers to  $SSK_{MS-SN}$ ; however, the original Jeong paper (EX1012) refers to  $SSK_{MS-HN}$  in this same paragraph, which is consistent with Jeong’s teachings regarding encryption of the IMSI. *See* EX1007 at 0008 (Figure 6 and §3.2(1)).

the ECDH key agreement between MS and HN would proceed the same way it does between MS and SN.” Pet. at 39-40 n.8; *see also* Pet. at 40 (“[A] POSITA would have understood that Jeong’s MS would generate a public/private key pair ( $d_{MS}/Q_{MS}$ ) for ECDH exchange with HN.”). However, Jeong teaches that the  $SSK_{MS-HN}$  is derived differently than the one time key OT- $SSK_{MS-SN}$ . *Compare* EX1007 at 0009 (§4.1.1(1)) (detailing  $SSK_{MS-HN}$  generation based on a “secret key registered in the USIM card and certificate authority when the USIM card is first registered”), *with id.* at 0009 (§3.2(6)) (“At this time, the MS generates OT- $SSK_{MS-SN}$  with *its own secret key* to the public key received from the SN.”). In short, Petitioners’ arguments regarding how a POSITA would have interpreted Jeong directly contradict Jeong’s express teachings, which are specific choices made to address particular design issues.

**(c) The Petition’s Proposed Modification of Jeong Changes Its Principle of Operation**

Perhaps recognizing that Jeong teaches other than what the Petition alleges regarding  $SSK_{MS-HN}$ , Petitioners conclude their analysis of Limitation 1(e) by proposing to modify Jeong to have the MS generate a public/private key pair to satisfy the limitation. *See* Pet. at 40 (“[I]t would have been obvious to a POSITA to dynamically generate the MS public/private key pair in order to remove reliance on long-term secrets that might be compromised and to achieve forward security, such that compromise of the key pair would not allow discovery of past messages.”); *see*

*also id.* at 41 n.9 (“Thus, a POSITA would have understood the security benefits of dynamically generating a public/private key pair and would have implemented Jeong’s  $SSK_{MS-HN}$  key by first generating a public/private key pair at the MS (UICC) for exchange with the HN.”). The Petition’s proposed modification is improper for at least two reasons. First, it fundamentally rewrites Jeong’s security protocols, which were designed to address the security constraints imposed by the mobile payment system problem. Second, the proposed modification is not an obvious design choice because that design was expressly rejected by Jeong.

Citing the generic benefits of “forward security,” the Petition alleges that a POSITA would have dynamically generated an MS key pair to derive  $SSK_{MS-HN}$ , reasoning by analogy to Jeong’s separate OT- $SSK_{MS-SN}$  exchange and Nakhjiri’s ECDH key generation process. *See* Pet. at 40-41. But this argument does not account for Jeong’s own protocol architecture, which demonstrates that the static, pre-registered nature of  $SSK_{MS-HN}$  is a structural necessity of the design—not an oversight or deficiency that a POSITA would have been motivated to correct.

Jeong is explicit that  $SSK_{MS-HN}$  “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 . . . .” EX1007 at 0009 (§4.1.1). Thus, both inputs to the key derivation—the secret key and the initial point P—are established during USIM registration and are already known to both the MS and the HN before any

authentication session begins.

The reason for this design choice is apparent from the structure of Jeong's authentication protocol. As detailed in §3.2(1) and shown in Figure 6, the very first action in Jeong's authentication flow (the Safe AKA Procedure) is for the MS to encrypt its IMSI using  $SSK_{MS-HN}$ , yielding an  $E-IMSI_{MS}$  value that is then transmitted to the SN. This is the opening message of the Safe AKA Procedure—no prior interactive communication between the MS and any network entity has occurred. Therefore, the MS must already possess the key needed to protect its IMSI when it initiates the authentication sequence. If  $SSK_{MS-HN}$  were instead derived through a dynamic ECDH exchange—as the Petition proposes—the MS would first need to exchange public keys with HN (or some intermediary) before it could encrypt its IMSI. But any such preliminary exchange would itself require the MS to contact the network, raising the question of how the MS identifies itself during that preliminary step without exposing the very IMSI that  $SSK_{MS-HN}$  is designed to protect. The Petition ignores this deficiency in its proposed modification.

By contrast, Jeong's  $OT-SSK_{MS-SN}$ —the one-time key to which the Petition analogizes—is generated at an entirely different point in the Safe AKA Procedure protocol. At step (5), the SN transmits the initial point P and its public key SNP to the MS, and at step (6) the MS uses those values along with its own secret key to generate  $OT-SSK_{MS-SN}$ . EX1007 at 0009 (§3.2(5)-(6)). This exchange occurs only

after the protocol has already progressed through multiple steps: the MS has transmitted its encrypted IMSI at step (1), the SN has forwarded that data to HN at step (2), HN has decrypted and *verified the MS's identity* at step (3), and HN has returned its own authentication credentials to the SN at step (4). The dynamic ECDH exchange with SN thus takes place only *after* the MS has been authenticated by the HN—not at the beginning stages of the authentication protocol. The difference in protocol sequencing is what makes a static pre-registered key necessary for the MS-HN relationship and a dynamic one-time key feasible for the MS-SN relationship.

Jeong was plainly aware of dynamic, ephemeral key generation—it implemented exactly that for OT-SSK<sub>MS-SN</sub> and specifically identified it as providing protection against retransmission attacks. *See* EX1007 at 0010-11 (§§4.1.3, 5). Yet Jeong chose not to apply this approach to SSK<sub>MS-HN</sub>. A POSITA reading Jeong's protocol would have understood this as a purposeful design decision dictated by the protocol's sequencing requirements, not as a gap inviting modification. The Petition's proposal to replace Jeong's static, pre-registered key with a dynamically generated key pair does not optimize Jeong's system—it fundamentally alters the protocol sequence in a manner that Jeong's architecture does not support and that would undermine the IMSI privacy protection that SSK<sub>MS-HN</sub> was designed to provide.

A POSITA would have recognized that there are significant complexities

associated with cryptographic solutions (or cryptosystems), including the primitives and protocols relied on to implement such systems. *See* EX2024 ¶¶ 75-77. The Petition’s proposed combinations fundamentally change cryptographic protocols without addressing the security objectives of those protocols or considering how the changes may alter the assumptions underlying the protocol’s design. This lapse can have significant consequences, and the Petition failed to address them. *See* EX2024 ¶¶ 78-79.

The Petition offers no explanation of how a dynamic ECDH exchange with HN could be inserted before step (1) of Jeong’s protocol without requiring additional message flows that Jeong does not contemplate. Nor does the Petition address the risk that such a modification could re-introduce the IMSI exposure vulnerability that Jeong’s design was specifically engineered to eliminate. And, introducing additional message flows would increase bandwidth consumption, which Jeong expressly sought to reduce. *See* EX1007 at 0008 (§3.2) (describing improvements to the “bandwidth consumption problem between SN (Serving Network) and certificate authority”); *id.* at 0010 (§4.2.1 Bandwidth Reduction). The conclusory assertion that a POSITA would have appreciated the “security benefits of dynamically generating a public/private key pair” (Pet. at 41 n.9) does not answer these questions and does not provide the reasoned, evidence-based explanation required to support a finding of obviousness. *See* EX2024 ¶¶ 80-81.

**3. Because Jeong Does Not Disclose the Second Key Pair, It Cannot Disclose Sending a Second Public Key**

*Limitation 1(f): “sending, to a second server associated with the wireless network, the second module public key;”*

For these same reasons (*i.e.*, the absence of a second public/private key pair), the Petition fails to show that Jeong meets Limitation 1(f), which requires “sending, to a second server associated with the wireless network, the second module public key.” EX1001 at 148:22-23. As detailed above, Jeong fails to disclose generating a second module public/private key pair, so it also fails to disclose sending a second module public key to the authentication center of the HN, which the Petition has identified as the “second server.” In an effort to sidestep this deficiency, the Petition points to communications between the MS and SN. *See* Pet. at 42 n.10. But Jeong explicitly teaches that the  $SSK_{MS-SN}$  is generated differently than the  $SSK_{MS-HN}$ . Core reasons for that difference were detailed above. *See supra* Section VI.B.2. Jeong’s teachings provide an additional reason for the difference: the communication channel between the MS and SN *is not* a trusted channel, and the channel between the SN and HN *is* a trusted channel. *See* EX1007 at 0008 (§3.2) (explaining that “the communication channel between the SN and H[N] is secure”). Therefore, one-time (OT) shared secrets are needed for the MS to communicate with the SN, but they are not needed for communications between the MS and HN.

For these reasons, the Petition’s Ground 1 mapping of Jeong to the claims

fails to establish a reasonable likelihood that any challenged claim is unpatentable.

**C. Ala-Laurila Fails to Teach Multiple Limitations and Would Not Have Been Combined with Nakhjiri as the Petition Proposes (Ground 2)**

Unlike the Petition’s Ground 1 analysis, which includes claim element charts for every limitation, its Ground 2 analysis includes no chart for Ala-Laurila. The reason is simple—the Petition has not identified any disclosure in Ala-Laurila sufficient to teach Limitations 1(e)-1(h), and including such a chart would highlight these deficiencies.

Instead, the Petition inconsistently identifies the claimed “second server,” pointing to two servers in two different networks for Limitation 1(f) but only one for Limitation 1(i). Additionally, a POSITA would not have imported Nakhjiri’s ECDH exchange into Ala-Laurila because Ala-Laurila never mentions public or private keys, references a different algorithm than ECDH, and teaches away from Nakhjiri’s pre-stored seed approach. Furthermore, Nakhjiri teaches away from Limitation 1(f) because its system requires the module public key to remain secret and transmitting it wirelessly to a server compromises that confidentiality. Even assuming the Petition’s proposed modification was adopted, Nakhjiri’s deterministic seed-based key generator function fails to create different private keys as required by the claim. Finally, the Petition fails to identify any teaching that cryptographic parameters for profile provisioning also would be used for device authentication.

**1. The Petition’s Shifting “Second Server” Identification Exposes the Internal Inconsistency of Ground 2**

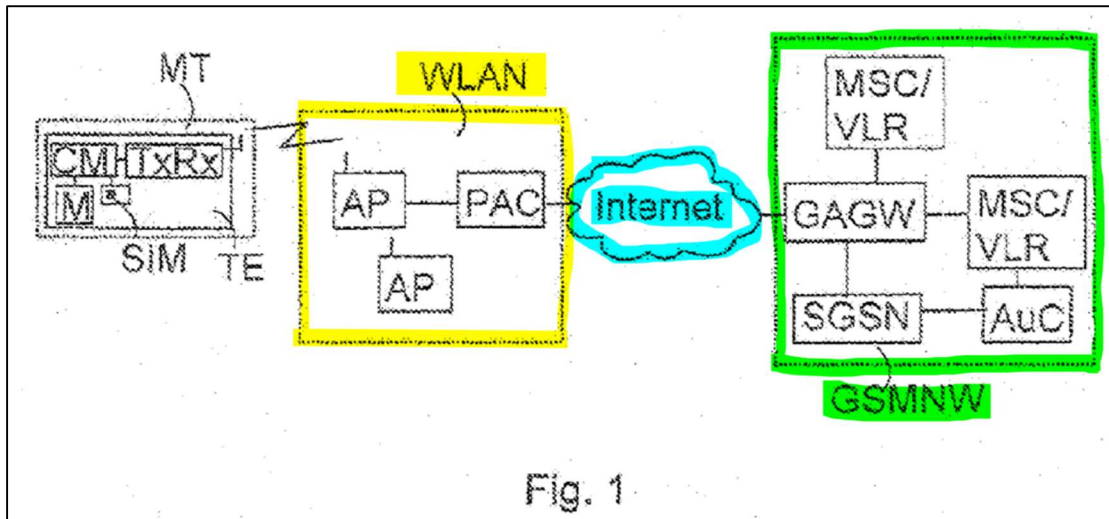
*Limitation 1(f): “sending, to a second server associated with the wireless network, the second module public key;”*

*Limitation 1(i): “sending, to the second server, the module encrypted data.”*

The Petition fails to specifically identify the claimed “second server associated with the wireless network.” Instead, its “second server” identification is ambiguous and spans two different networks. For Limitation 1(f), the Petition identifies two different servers, each in a separate network, as the second server. However, for Limitation (i), it only identifies one of the two servers previously identified. This ambiguous and shifting identification of the second server fails to show that Ala-Laurila discloses the claimed “second server.”

First for Limitation 1(f), the Petition identifies the PAC and GAGW of Ala-Laurila as the “second server.” *See* Pet. at 65 (“The PAC and GAGW performs authentication and corresponds to the recited ‘second server.’”); *see also id.* at 63 (identifying “PAC/GAGW (the ‘second server’)”). However, the Petition fails to show that the PAC and GAGW represent “a second server associated with the wireless network.” As Ala-Laurila explains, the PAC and GAGW are two different servers in two different networks.

Ala-Laurila’s Figure 1 illustrates the wireless telecommunication system of its preferred embodiment, and is shown below.



EX1013 Fig. 1 (annotated); *see id.* ¶ [0011]. Ala-Laurila describes the WLAN (highlighted in yellow) as “a *WLAN network* WLAN according to IEEE802.11 standard.” EX1013 ¶ [0016]. It describes the GSMNW (highlighted in green) as “a *public land mobile network*, in this embodiment a *GSM network* GSMNW.” *Id.* These two networks (the WLAN and GSMNW) are separated by the Internet (highlighted in blue), which Ala-Laurila describes as yet another network. *See id.* ¶ [0021] (“The WLAN network WLAN may also offer a connection through a gateway to other networks, such as the Internet.”). According to Ala-Laurila’s express teachings, the PAC and GAGW identified by the Petition as the “second server associated with *the* wireless network” each belong to different networks. *See* EX2024 ¶ 71. The Petition fails to identify *which network*<sup>5</sup> in Ala-Laurila

<sup>5</sup> The Petition never specifically identifies the network that corresponds to the “wireless network” of the claims. Had it done so, such identification would have

corresponds to “the wireless network” of the claim, and it has identified the combination to two distinct servers in two different networks as purportedly satisfying the claimed “second server.” In short, the Petition fails to properly identify a second server that corresponds to “the wireless network” for Limitation 1(f).

Turning now to Limitation 1(i), the Petition identifies *only the PAC* as the claimed “second server.” *See* Pet. at 67-68. Thus, the Petition’s identification of the “second server” for Limitation 1(f) (PAC/GAGW) is different from the second server identified for Limitation 1(i) (PAC). The different requirements between these two limitations highlight the flaws with the Petition’s Ground 2 mapping to the claim.

Limitation 1(i) requires sending the module encrypted data (which includes the module identity per Limitation 1(g)) to the second server. And the Petition relies on the PAC as the second server based on Ala-Laurila’s teaching that the MT\_PAC\_AUTHSTART 204 request between the MT and PAC can be sent in ciphered form. *See* Pet. at 66-67 (citing EX1013 ¶ [0026] and Fig. 2). Ala-Laurila then explains that the PAC then sends a PAC\_GAGW\_AUTHSTART 205 request

---

highlighted the problems stemming from the Petition’s attempt to cobble together components from multiple, unrelated networks in an effort to meet the challenged patent claim limitations.

to the GAGW, which also includes the network access identifier (NAI) comprising the IMSI identifier. *See id.* ¶ [0027]. Notably, Ala-Laurila does *not* teach that this subsequent message between the PAC and GAGW is ciphered (*i.e.*, encrypted). *See id.* (explaining that the “PAC decipheres the request 204 if needed” but never suggesting request 205 is ciphered by the PAC or deciphered by the GAGW); *see also* Pet. at 67 (pointing only to the MT\_PAC\_AUTHSTART\_REQ 204 message as “encrypted”). Thus, the Petition’s Limitation 1(i) mapping limits the claimed second server to the PAC because there is no teaching that an encrypted module identity is sent to the GAGW.

However, if the PAC is the second server, the Petition’s mapping for Limitation 1(f) breaks down. For that limitation, the Petition alleges that Nakhjiri’s key exchange process would be used for communications between the claimed mobile device and second server. *See* Pet. at 65 (“In the Nakhjiri-Bradley-Ala-Laurila combination, Nakhjiri’s Diffie-Hellman key exchange process would be used to send a second module public key to an authentication server (*i.e.*, second server) . . . .”). However, Nakhjiri’s key exchange relies on a private seed and a mobile network operator ID (MNO\_ID). *See* EX1005 at 5:61-64, 4:50. But the PAC, which is part of the WLAN network—not a mobile operator network—would not have a corresponding MNO\_ID. In fact, Ala-Laurila teaches that each of the many, unrelated WLANs is connected to the Internet and to any number of GSM networks

for mobile network operators. *See* EX1013 ¶¶ [0017], [0022]. Thus, each WLAN may communicate with numerous mobile network operator networks (GSMNWs). The Petition fails to explain how Nakhjiri’s key exchange, which relies on a MNO\_ID corresponding to a particular mobile network operator, would have been used for a WLAN that has no affiliation with any mobile network operator and may facilitate communications with numerous mobile operator networks. Furthermore, the Petition has not shown or even alleged that the PAC for a WLAN is somehow associated with the same network comprising the SM-DP servers (*i.e.*, first server of Limitation 1(b)) of Nakhjiri. *See* EX2024 ¶¶ 72-74.

The Petition’s Ground 2 mapping relies on ambiguous definitions of the “second server.” The purported server identified for Limitation 1(f) (PAC/GAGW) belongs to two different networks, and the purported server identified for Limitation 1(i) (PAC) is not affiliated with a mobile network operator and does not have a mobile network ID (or private seed) as required by Nakhjiri’s ECDH exchange for generating a public key.

**2. A POSITA Would Not Have Imported Nakhjiri’s ECDH Exchange into Ala-Laurila, and the Petition’s Proposed Modification Fails to Satisfy Limitation 1(e)**

*Limitation 1(e): “generating, by the eUICC, a second module public key and a corresponding second module private key;”*

Ala-Laurila never mentions public or private keys at all. The Petition instead relies on the following statement from Ala-Laurila to support its arguments

regarding Limitation 1(e): “The [authentication starting] request 204 is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm, for example.” EX1013 ¶ [0026]; *see* Pet. at 64. And the Petition admits that “Ala-Laurila does not describe the Diffie-Hellman exchange in detail . . . .” Pet. at 64. Nonetheless, the Petition alleges that this single passing reference to Diffie-Hellman in Ala-Laurila would have motivated a POSITA to modify Nakhjiri’s disclosure “to generate a second module public key and a corresponding second module private key for mutual authentication with the PAC/GAGW servers, as taught by Ala-Laurila.” Pet. at 64.

Petitioners are wrong for at least three reasons. First, the Diffie-Hellman reference in Ala-Laurila is to a completely different key exchange algorithm than the ECDH algorithm required by the ’869 Patent claims. Second, the Petition’s proposed use of Nakhjiri would result in the generation of the *same* public/private keys detailed earlier regarding limitation 1(a). Third, the Petition provides no basis to import Nakhjiri’s provisioning solution into the WLAN authentication context detailed by Ala-Laurila.

The “Diffie-Hellman algorithm” referred to by Ala-Laurila is the algorithm disclosed in the 1976 seminal paper by Whitfield Diffie and Martin Hellman. *See* EX2015. The Petition provides no factual support for the conclusory statement 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 . . . .” Pet. at 63. Rather, the Petition relies on hindsight and unsupported inference to allege that a single reference to “the Diffie-Hellman algorithm” purportedly discloses the particular ECDH key exchange detailed in Limitations 1(e), 1(f), and 1(g). The Petition fails to identify any factually supported reason to modify Ala-Laurila to use an algorithm other than “the Diffie-Hellman algorithm” it specifically identifies.

Furthermore, the Petition’s proposed use of Nakhjiri to satisfy Limitation 1(e) fails. Nakhjiri’s teaching regarding the generation of a module/USIM private key MNO\_ECC\_PVKDEV would not result in a second module private key. Nakhjiri relies on a private seed (shared between the USIM and network) and a mobile network operator identifier (MNO\_ID) to generate the private key MNO\_ECC\_PVKDEV. *See supra* Section II.D.1. This aspect of Nakhjiri’s design renders the Petition’s proposed modification unworkable for two reasons.

First, a POSITA would not combine the systems as proposed because Ala-Laurila teaches away from relying on pre-stored values to support authentication in its WLANs. Ala-Laurila identifies problems with WLAN networks as follows:

However, ***a problem in*** some wireless telecommunication networks, such as IEEE802.11 ***WLAN networks, is that the ciphering keys used for ciphering traffic must be stored in advance in the terminal and access point.*** If the network does not have the same key as the terminal,

then the data between the network and the terminal cannot be ciphered.

To add different ciphering keys is difficult, and a safe data transmission cannot always be offered for terminals moving in different networks.

EX1013 ¶ [0004] (emphasis added). Ala-Laurila then explains that “*[i]t 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.*” *Id.* ¶ [0005] (emphases added). Nakhjiri’s key exchange, however, requires that the private seed be stored in advance in the terminal. *See* 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.”). This requirement is counter to Ala-Laurila’s stated design goals.

Even accepting the Petition’s proposed importation of Nakhjiri’s ECDH key exchange into Ala-Laurila, the combined system still fails to generate a *second* public/private key pair. Nakhjiri’s use of the private\_seed (which is *unique* to the UICC) and MNO\_ID in the deterministic key generator function (KGF) will always result in the same value for a module private key and not a *second* module private key as required by Limitation 1(e). *See* EX1005 at 4:38-40, 5:61-64. The Petition never explains how the same deterministic inputs would yield a different output. Thus, the proposed combined system fails to satisfy the requirement of generating a second module private key.

Nakhjiri’s cryptographic system is designed specifically to support provisioning profiles from an SM-DP server to a mobile device. *See* EX1005 at 1:57-2:24. Ala-Laurila, on the other hand, is focused on creating ciphering keys for a mobile device to communicate with a wireless LAN (WLAN) access point by relying on GSM authentication in a Public Land Mobile Network (PLMN). EX1013 ¶¶ [0005]-[0007]. As detailed above, combining or modifying cryptographic protocols designed for specific purposes can significantly impact the combined system’s operation—including its ability to satisfy security objectives as well as changing the underlying assumptions providing a basis for the original design. *See* EX2024 ¶¶ 75-79.

The Petition failed to address any of these concerns, instead summarily proposing a significant modification to Ala-Laurila for the sole purpose of satisfying multiple claim limitations—*i.e.*, via hindsight. *See* EX2024 ¶ 82. The network infrastructure, assumptions, and problems addressed by these two references are different and largely unrelated. *See* EX2024 ¶¶ 83-84. The Petition provides no apparent reason to import the cryptographic solution of Nakhjiri wholesale into Ala-Laurila, and even so, the proposed modification fails to generate a new, second key pair as required by Limitation 1(e).

### **3. Nakhjiri Teaches Away from Exposing Public Keys**

*Limitation 1(f): “sending, to a second server associated with the wireless network, the second module public key;”*

An additional reason that the Petition’s reliance on Nakhjiri-Bradley-Ala-Laurila (Ground 2) fails for Limitation 1(f) is due to its reliance on Nakhjiri as purportedly disclosing “sending” the claimed second public key to a second server.

Nakhjiri depends on the module/USIM public key MNO\_ECC\_PLKDEV remaining secret. *See* EX1005 at 5:8-17; EX2024 ¶¶ 65-66. This teaches away from Limitation 1(f) since a mobile device sending that key over a public network means that Nakhjiri’s module/USIM public key MNO\_ECC\_PLKDEV becomes public and is no longer secret. A POSITA would not have been motivated to modify Nakhjiri’s system to expose public keys because it would require additional authentication measures and potentially exposes the modified system to additional security vulnerabilities, such as man-in-the-middle attacks. *See* EX2024 ¶¶ 67-69. Consequently, the proposed Nakhjiri-Bradley-Ala-Laurila combination does not teach Limitation 1(f).

**4. Nakhjiri’s Seed-based Key Derivation Is Infeasible in Ala-Laurila’s Architecture of Unrelated WLAN Access Points**

*Limitation 1(g): “generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;”*

Petitioners rely on the same arguments made for Limitations 1(e) and 1(f) to support their Limitation 1(g) analysis. *See* Pet. at 65 (“Nakhjiri-Bradley-Ala-Laurila teaches Element 1(g) for the reasons described for Elements 1(e)-1(f).”). Thus, the Petition’s support for Limitation 1(g) suffers from the same flaws detailed above for

Limitations 1(e) and 1(f). Neither Nakhjiri nor Ala-Laurila teaches the *second* set of public/private keys required by all three limitations (1(e)-1(g)).

In addition, Nakhjiri's key derivation process, which relies on pre-shared private seeds, would be inoperable in Ala-Laurila's network architecture comprised of numerous unrelated WLANs. *See* EX2024 ¶¶ 82-84. 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, because Ala-Laurila specifically identified requiring pre-stored keys in the WLAN or terminal as a problem. *See* EX1013 ¶ [0004]. Eliminating the pre-shared seed breaks the entire public/private key derivation process taught by Nakhjiri. Additionally, placing Nakhjiri's pre-stored seed on numerous untrusted WLAN networks introduces a significant security concern that the Petition fails to even acknowledge or address. Such a change in the underlying assumptions regarding Nakhjiri's protocol requires a rigorous assessment of whether the modified protocol continues to work for its intended purpose. *See* EX2024 ¶¶ 75-79. The Petition provides no such evaluation and thus fails to show that a POSITA would have modified Ala-Laurila as proposed.

**5. No Reference Teaches that Parameters Received in an Encrypted Profile From One Server Be Used for a Subsequent ECDH Exchange with a Different Server**

*Limitation 1(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;"*

*Limitation 1(g): “generating a symmetric key using a second ECDH key exchange with the second module private key and **the cryptographic parameters;**”*

The Petition’s Ground 2 allegations regarding the claimed “cryptographic parameters” suffers from a similar flaw as its Ground 1 allegations (*see supra* Section VI.B.1)—it fails to link the Limitation 1(g) parameters used for a second server exchange to those received via encrypted profile from a first server as required by Limitation 1(b). The Petition proposes injecting Nakhjiri’s ECDH exchange into Ala-Laurila’s WLAN authentication procedure. *See* Pet. at 65 (“A POSITA would have used Nakhjiri’s ECDH procedure to create the symmetric key Ala-Laurila uses to encrypt IMSI.”). But there is no teaching in *any* reference that cryptographic parameters purportedly received during profile provisioning would be reused for a subsequent authentication-phase ECDH exchange *with a different server*. Petitioners only arrive at the proposed combination through improper use of hindsight bias. *See Interconnect Planning*, 774 F.2d at 1138; *Orexo AB*, 903 F.3d at 1271.

## **VII. Conclusion**

For all of the reasons stated herein, Patent Owner respectfully requests that the Petition be denied.

Dated: March 2, 2026

Respectfully submitted,

By: /R. Allan Bullwinkel /  
R. Allan Bullwinkel (Reg. No. 77,630)  
Attorney for Patent Owner  
Network-1 Technologies, Inc.

**CERTIFICATE OF SERVICE**

The undersigned certifies that pursuant to 37 C.F.R. § 42.6(e), a copy of the foregoing **Patent Owner’s Preliminary Response Brief**, was served via email to counsel of record for Petitioners as follows:

<b>Counsel for Petitioners</b>	
<b>Lead Counsel</b>	<b>Backup Counsel</b>
William M. Fink (Reg. No. 72,332) O’Melveny & Myers LLP 1625 Eye Street, NW Washington, DC 20006 Telephone: (202) 383-5300 Fax: (202) 383-5414 Email: tfink@omm.com	Benjamin M. Haber (Reg. No. 67,129) O’Melveny & Myers LLP 400 South Hope Street, 19th Floor Los Angeles, CA 90071 Telephone: (213) 430-6000 Fax: (213) 430-6407 Email: bhaber@omm.com  Marc J. Pensabene (Reg. No. 37,416) O’Melveny & Myers LLP 1301 Avenue of the Americas, Suite 1700 New York, NY 10019 Telephone: (212) 326-2000 Fax: (212) 326-2061 Email: mpensabene@omm.com  Brian Cook (Reg. No. 59,356) O’Melveny & Myers LLP 400 South Hope Street, 19th Floor Los Angeles, CA 90071 Telephone: (213) 430-6000 Fax: (213) 430-6407 Email: bcook@omm.com  Caitlin P. Hogan (Reg. No. 61,515) O’Melveny & Myers LLP 1301 Avenue of the Americas, Suite 1700 New York, NY 10019

	Telephone: (212) 326-2000 Fax: (212) 326-2061 Email: chogan@omm.com
--	---

Dated: March 2, 2026

Respectfully submitted,

/ R. Allan Bullwinkel /  
R. Allan Bullwinkel (Reg. No. 77,630)  
Attorney for Patent Owner  
Network-1 Technologies, Inc.

**CERTIFICATE OF COMPLIANCE**

Pursuant to 37 C.F.R. § 42.24(d), the undersigned hereby certifies that this brief complies with the type-volume limitation of 37 C.F.R. § 42.24 because this brief contains 11,614 words.

Dated: March 2, 2026

Respectfully submitted,

/ R. Allan Bullwinkel /

R. Allan Bullwinkel (Reg. No. 77,630)

Attorney for Patent Owner

Network-1 Technologies, Inc.