

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

v.

NETWORK-1 TECHNOLOGIES, INC.,
Patent Owner.

Case No. IPR2026-00117
U.S. Patent No. 12,166,869

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 12,166,869**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	1
III. FEE AUTHORIZATION	3
IV. GROUNDS FOR STANDING.....	3
V. PRECISE RELIEF REQUESTED	3
VI. THE CHALLENGED PATENT	4
VII. PROSECUTION HISTORY OF THE '869 PATENT.....	8
VIII. LEVEL OF ORDINARY SKILL IN THE ART	8
IX. PRIORITY DATE	8
X. CLAIM CONSTRUCTION	9
XI. BRIEF DESCRIPTION OF THE APPLIED PRIOR ART	9
A. Nakhjiri (Ex-1005)	9
B. Bradley (Ex-1006).....	11
C. Jeong (Ex-1007)	12
D. Ala-Laurila (Ex-1013).....	13
E. ANSI X9.63-Overview (Ex-1014).....	16
F. Pierce (Ex-1009).....	17
G. GlobalPlatform (Ex-1010).....	18
XII. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS	18
A. Ground 1: Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri, Bradley, and Jeong.....	18
1. A POSITA would have been motivated to combine Nakhjiri's teachings with Bradley's teachings and Jeong's teachings and would have had a reasonable expectation of success.....	18
2. Independent Claim 1	23

TABLE OF CONTENTS
(continued)

	Page
a. Element 1[pre]: 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:.....	23
b. Element 1(a): storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key;.....	24
c. Element 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;	30
d. Element 1(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;	34
e. Element 1(d): decrypting, with the shared secret key, at least a portion of the encrypted profile for the eUICC;	37
f. Element 1(e): generating, by the eUICC, a second module public key and a corresponding second module private key;	38
g. Element 1(f): sending, to a second server associated with the wireless network, the second module public key;	42
h. Element 1(g): generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;.....	42
i. Element 1(h): generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity; and	44
j. Element 1(i): sending, to the second server, the module encrypted data.....	46

TABLE OF CONTENTS
(continued)

	Page
3. Dependent Claims 2-4, 7, 9-14, and 16-20	47
a. Claim 2: The method of claim 1, wherein the module identity comprises an international mobile subscriber identity (IMSI).	47
b. Claim 3: The method of claim 1, wherein the module identity comprises a permanent identifier for the mobile device.	47
c. Claim 4: The method of claim 1, wherein the cryptographic parameters comprise an identifier for a set of cryptographic parameters.	48
d. Claim 7: The method of claim 1, wherein the first server mutually derives the shared secret key using the first ECDH key exchange with the first module public key and a network private key corresponding to the network public key.	49
e. Claim 9: The method of claim 1, further comprising in step h) generating, with the symmetric key and an Advanced Encryption Standard (AES), the module encrypted data.	50
f. Claim 10: The method of claim 1, wherein steps g) and h) occur before step f).	51
g. Claim 11: The method of claim 1, wherein the network public key is associated with an eUICC subscription manager.	52
h. Claim 12: The method of claim 11, wherein the eUICC subscription manager comprises the first server.	52
i. Claim 13: The method of claim 1, further comprising: j) receiving, from the wireless network, a random number (RAND) and generating a response (RES) using the RAND and the key K.	53

TABLE OF CONTENTS
(continued)

	Page
j. Claim 14: The method of claim 1, further comprising before step b), authenticating the first server by (i) receiving a server digital signature and (ii) verifying the server digital signature with a server public key.....	55
k. Claim 16: The method of claim 1, wherein the first server, the second server, and the wireless network are associated with a mobile network operator.	56
l. Claim 17: The method of claim 1, wherein the eUICC comprises a processor, firmware, and protected memory.	58
m. Claim 18: The method of claim 1, wherein the cryptographic parameters include a base point G for an elliptic curve.....	59
n. Claim 19: The method of claim 1, wherein the mobile device comprises a wireless device with a radio for communicating with a plurality of base stations for the wireless network.	59
o. Claim 20: The method of claim 1, wherein the eUICC comprises a package soldered to a circuit board of the mobile device.	61
B. Ground 2: Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri in view of Bradley and Ala-Laurila.	61
1. A POSITA would have been motivated to combine Nakhjiri-Bradley with Ala-Laurila and would have had a reasonable expectation of success.....	61
2. Independent Claim 1	63
a. Elements 1[pre]; 1[a]-[d]:.....	63
b. Element 1(e): generating, by the eUICC, a second module public key and a corresponding second module private key;	63

TABLE OF CONTENTS
(continued)

	Page
c. Element 1(f): sending, to a second server associated with the wireless network, the second module public key;	65
d. Element 1(g): generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;.....	65
e. Element 1(h): generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity; and	66
f. Element 1(i): sending, to the second server, the module encrypted data.....	67
3. Dependent Claims 2-4, 7, 9-14, and 16-20	68
a. Claims 2-4, 7, 9, 11-12, 14, and 17-20.....	68
b. Claim 10: The method of claim 1, wherein steps g) and h) occur before step f).....	68
c. Claim 13: The method of claim 1, further comprising: j) receiving, from the wireless network, a random number (RAND) and generating a response (RES) using the RAND and the key K.....	69
d. Claim 16: The method of claim 1, wherein the first server, the second server, and the wireless network are associated with a mobile network operator.	70
C. Grounds 3-4: Claims 5-6 are obvious over Nakhjiri, Bradley, Jeong, and X9.63-Overview; or Nakhjiri, Bradley, Ala-Laurila, and X9.63-Overview	71
1. A POSITA would have been motivated to combine Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila with X9.63-Overview and would have had a reasonable expectation of success.....	71
2. Dependent Claims 5-6.....	73

TABLE OF CONTENTS
(continued)

	Page
a. Claim 5: The method of claim 1, further comprising in step c) deriving the shared secret key using an American National Standards Institute (ANSI) standard X-9.63 key derivation function.....	73
b. Claim 6: The method of claim 1, further comprising in step g) deriving the symmetric key using an ANSI standard X-9.63 key derivation function.....	75
D. Grounds 5-6: Claim 8 is obvious over Nakhjiri, Bradley, Jeong, and Pierce or Nakhjiri, Bradley, Ala-Laurila, and Pierce.....	75
1. Dependent Claim 8.....	75
a. Claim 8: The method of claim 1, further comprising in step e), generating, by the eUICC, the second module public key and the second module private key using a random number generator and input from a sensor.	75
E. Grounds 7-8: Claim 15 is obvious over Nakhjiri, Bradley, Jeong, and GlobalPlatform or Nakhjiri, Bradley, Ala-Laurila, and GlobalPlatform.....	77
1. Dependent Claim 15	77
a. Claim 15: The method of claim 1, further comprising (i) in step a), storing a server name for the first server and a port number in a nonvolatile memory of the eUICC, and (ii) before step b) sending the first module public key to the first server.....	77
XIII. CONCLUSION.....	80

LIST OF EXHIBITS¹

Ex. No.	Description
Ex-1001	U.S. Patent No. 12,166,869 (“the ’869 Patent”)
Ex-1002	Declaration of Dr. Sundeep Rangan
Ex-1003	Curriculum Vitae of Dr. Sundeep Rangan
Ex-1004	Prosecution History of U.S. Patent No. 12,166,869
Ex-1005	U.S. Patent No. 9,210,138 to Nakhjiri (“Nakhjiri”)
Ex-1006	U.S. Patent Publication No. 2014/0024343 to Bradley (“Bradley”)
Ex-1007	Certified Translation: Eun-Hee Jeong & Byung-kwan Lee, A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment, 13 Journal of Korea Multimedia Society 1687-97 (Nov. 2010) (“Jeong”)
Ex-1008	U.S. Patent Publication No. 2013/0012168 to Rajadurai (“Rajadurai”)
Ex-1009	U.S. Patent Publication No. 2009/0323967 to Pierce (“Pierce”)
Ex-1010	GlobalPlatform Remote Application Management over HTTP Card Specification V2.2 – Amendment B ver 1.1.1 (Mar. 2012) (“GlobalPlatform”)
Ex-1011	Certicom Research, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, v2 (May 21, 2009) (“SEC1”)
Ex-1012	Eun-Hee Jeong & Byung-kwan Lee, A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment, 13 Journal of Korea Multimedia Society 1687-97 (Nov. 2010) (“Jeong”) (original Korean)

¹ Four-digit pin citations that begin with 0 are to the branded numbers added by Samsung in the bottom right corner of the exhibits. All other pin citations are to original page, column, paragraph, or line numbers.

Ex. No.	Description
Ex-1013	U.S. Patent Publication No. 2012/0300934 to Ala-Laurila (“Ala-Laurila”)
Ex-1014	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000) (“X9.63-Overview”)
Ex-1015	Declaration of Simon Blake-Wilson, author of ANSI X9.63-Overview
Ex-1016	National Library of Korea Catalog Printout
Ex-1017	Korea Multimedia Society Webpage Printout
Ex-1018	Declaration of Tono Aspinall of GlobalPlatform, Inc.
Ex-1019	INTENTIONALLY LEFT BLANK
Ex-1020	Claim Mapping Table
Ex-1021	Prosecution History of U.S. Patent No. 10,700,856
Ex-1022	Prosecution History of U.S. Patent No. 10,187,206
Ex-1023	Prosecution History of U.S. Patent No. 9,742,562
Ex-1024	U.S. Patent Publication No. 2013/0301828 to Gouget (“Gouget”)
Ex-1025	U.S. Patent Publication No. 2010/0174907 to Semple (“Semple”)
Ex-1026	PCT Patent Publication No. WO2008/005162 to Wang (“Wang”)
Ex-1027	U.S. Patent Publication No. 2010/0135491 to Bhuyan (“Bhuyan”)
Ex-1028	CSMG, Reprogrammable SIMs: Technology, Evolution and Implications, Final Report (Sept. 25, 2012) (“CSMG”)
Ex-1029	U.S. Patent Publication No. 2007/0083766 to Farnham (“Farnham”)

Ex. No.	Description
Ex-1030	INTENTIONALLY LEFT BLANK
Ex-1031	U.S. Patent Publication No. 2014/0219443 to Brainis (“Brainis”)
Ex-1032	U.S. Patent Publication No. 2009/0068985 to Nguyen (“Nguyen”)
Ex-1033	U.S. Patent Publication No. 2012/0008775 to Natarajan (“Natarajan”)
Ex-1034	U.S. Patent No. 8,127,142 to Cuppett (“Cuppett”)
Ex-1035	Jaemin Park et al., Secure Profile Provisioning Architecture for Embedded UICC, Int’l Conference on Availability, Reliability & Security 297 (2013) (“Park”)
Ex-1036	Boyd, C. and Mathuria, A., Protocols for Authentication and Key Establishment, Springer-Verlag (2003) (“Boyd-Mathuria”)

I. INTRODUCTION

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Petitioner”) request *inter partes* review (“IPR”) of Claims 1-20 of U.S. Patent No. 12,166,869 (“the ’869 Patent”) (Ex-1001), currently assigned to Network-1 Technologies, Inc. (“PO”).

II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

Real Parties-in-Interest: Petitioner identifies the following real parties-in-interest: Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

Related Matters: PO has asserted the ’869 Patent against Petitioner in *Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd. et al.*, No. 2:25-cv-00667 (E.D. Tex.) (“Samsung litigation”).

Lead and Backup Counsel:

- Lead Counsel:

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

- Backup Counsel:

Benjamin M. Haber (Reg. No. 67,129)
O’Melveny & Myers LLP
400 South Hope Street, 18th 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, 18th 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

Service Information: Petitioner consents to electronic service by email to the following addresses:

- tfink@omm.com
- bhaber@omm.com
- mpensabene@omm.com
- bcook@omm.com
- chogan@omm.com

III. FEE AUTHORIZATION

The PTO is authorized to charge any fees due during this proceeding to Deposit Account No. LA500639.

IV. GROUNDS FOR STANDING

Petitioner certifies that the '869 Patent is available for review, and Petitioner is not barred or estopped from requesting review.

V. PRECISE RELIEF REQUESTED

Petitioner requests review and cancellation of Claims 1-20 as unpatentable based on the following grounds, supported by a declaration from Dr. Sundeep Rangan. Ex-1002 ¶¶1-52; Ex-1003.

Ground	Summary
1	Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri (Ex-1005), Bradley (Ex-1006), and Jeong (Ex-1007)
2	Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri, Bradley, and Ala-Laurila (Ex-1013)
3-4	Claims 5-6 are obvious over Nakhjiri, Bradley, Jeong, and X9.63-Overview (Ex-1011); or Nakhjiri, Bradley, Ala-Laurila, and X9.63-Overview
5-6	Claim 8 is obvious over Nakhjiri, Bradley, Jeong, and Pierce (Ex-1009); or Nakhjiri, Bradley, Ala-Laurila, and Pierce
7-8	Claim 15 is obvious over Nakhjiri, Bradley, Jeong, and GlobalPlatform (Ex-1010); or Nakhjiri, Bradley, Ala-Laurila, and GlobalPlatform

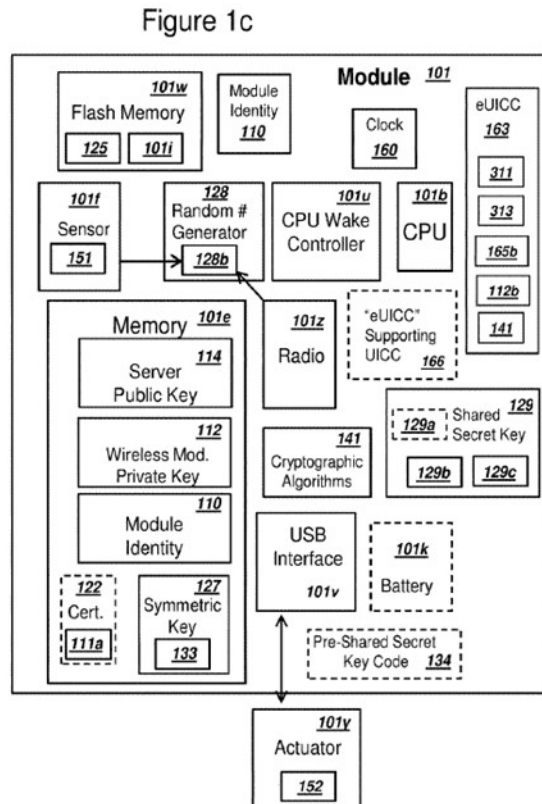
VI. THE CHALLENGED PATENT

The '869 Patent teaches methods for supporting an eUICC (embedded universal integrated circuit card) in a mobile module, securely deriving keys for communicating with servers and a wireless network, including Elliptic Curve Diffie Hellman (ECDH)-based shared secrets, cryptographic parameters, and public/private key pairs used with public key infrastructure. Ex-1001, 1:53–59. The “cryptographic parameters” include, e.g., elliptic curve identifiers and a base point G (Ex-1001, 41:20–22; *see also* Ex-1005, 4:51–56). Ex-1002 ¶¶53-57.

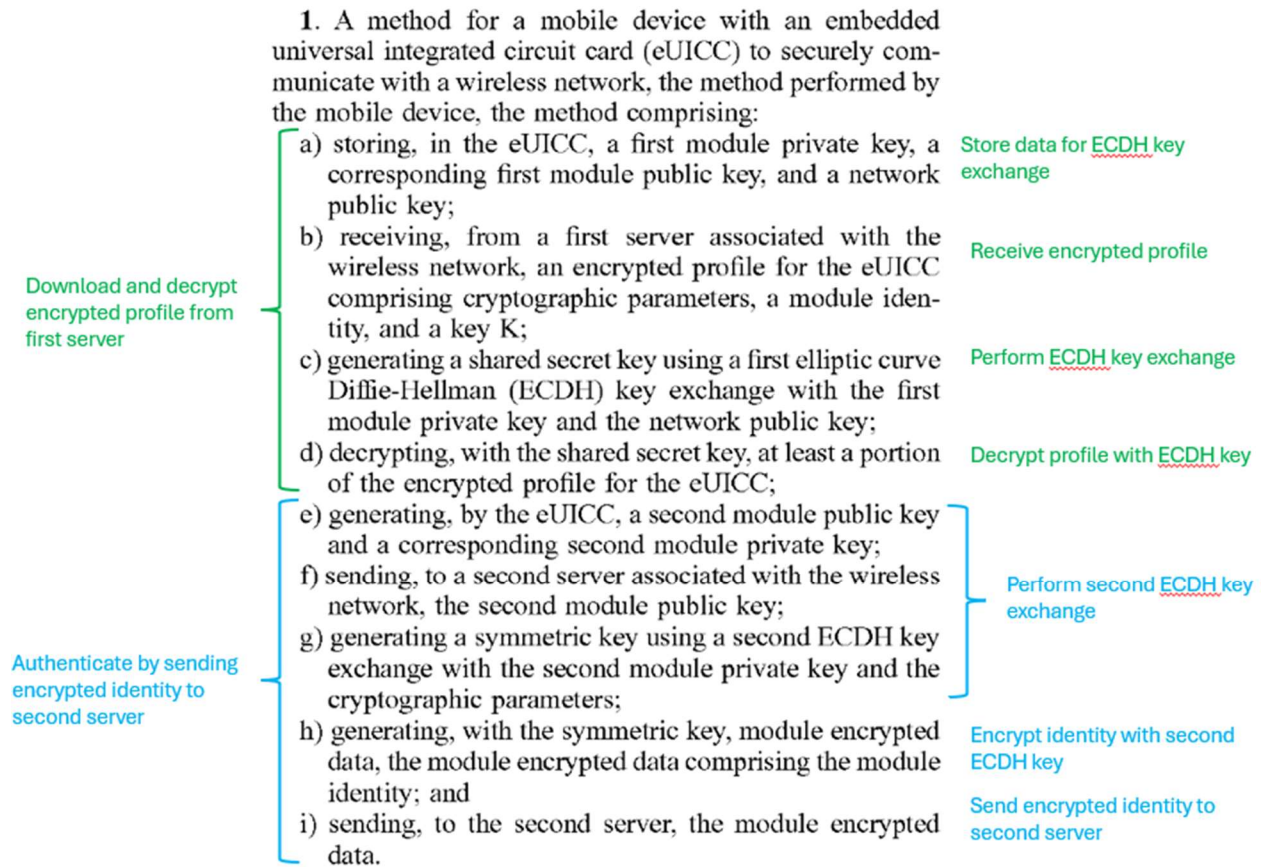
As shown in Figure 1c below,² the '869 Patent teaches a wireless module 101, which may operate “as a smartphone or mobile phone.” Ex-1001, 2:21-22, 18:13-14, Fig. 1c. Module 101 stores “module private key 112, server public key 114, and module identity 110, and a symmetric key 127 in memory/RAM 101e during operation.” Ex-1001, 25:20-23. Module identity 110 is “a unique identifier of module 101” such as “an international mobile subscriber identity number (IMSI).” Ex-1001, 26:23-28. Module 101 also stores cryptographic algorithms 141, which include a suite of algorithms that are used for “(i) deriving a pair of keys comprising a public key and a private key, (ii) encrypting data using public keys, (iii) decrypting data using private keys, (iv) processing secure hash signatures using private keys,

² Throughout, emphasis and annotations are added unless otherwise specified.

and (v) verifying secure hash signatures using public keys.” Ex-1001, 28:5-12. Moreover, module 101 stores “a pre-shared secret key 129a,” which is “shared between module 101 and server 105.” Ex-1001, 29:31-34.



Claim 1 of the '869 Patent, reproduced below, includes two major parts. Elements 1(a)-(d) recite a process for securely downloading an encrypted eUICC profile from a first network server and decrypting it. Elements 1(e)-(i) recite an authentication process whereby the mobile device sends encrypted data (including the module identity) to a second network server. Both the first and second processes rely on cryptographic keys generated through an Elliptic-Curve Diffie-Hellman (ECDH) exchange.



Ex-1001, Cl. 1.

Regarding the first part (downloading the profile), the claim requires performing an elliptic curve Diffie-Hellman (ECDH) exchange between the eUICC (mobile device) and a first network server to create a “shared secret key” that can be used to decrypt the profile sent to the eUICC from the network server. Specifically, the ’869 Patent teaches that the eUICC module may “use a first module private key,” and a server belonging to a mobile network operator and associated with a wireless network may “use a first module public key to establish communication between the two nodes.” Ex-1001, 9:43-47. The server securely sends “the module a set of

cryptographic parameters,” a module identity, and key K in the form of an encrypted profile, which “is decrypted by the module using ... a shared secret key.” Ex-1001, 9:47-57, Cl. 1. The shared secret key is generated by the module “using a first elliptic curve Diffie-Hellman (ECDH) key exchange with the first module private key and the network public key.” Ex-1001, 33:56-62, Cl. 1.

Regarding the second part (authentication), the claim requires a second ECDH exchange with a second server to derive a second shared secret key (“symmetric key”), which is then used to encrypt an identity of the eUICC and send that encrypted identity to the second server. Specifically, the ’869 Patent discloses that the module may use the “cryptographic parameters, a random number generator, and a key pair generation algorithm ... in order to generate a new, second module key pair, which could comprise a second module public key and a second module private key.” Ex-1001, 9:57-63. The module securely sends the second module public key to a second server. Ex-1001, 9:63-67, Cl. 1. Then the module generates “a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters” and generates “module encrypted data ... ciphered with [the] symmetric key,” which includes the module identity. Ex-1001, 41:20-22, Cl. 1. The eUICC module sends the module encrypted data to the second server. Ex-1001, 75:25-26.

VII. PROSECUTION HISTORY OF THE '869 PATENT

The '869 Patent was filed August 3, 2023, and claims priority through a chain of 6 continuation applications (now issued patents), the earliest of which was filed November 19, 2013. The Examiner did not issue any substantive prior art rejections during prosecution, only double patenting rejections based on related patent applications, which the Applicant overcame by filing terminal disclaimers. Ex-1002 ¶58.

VIII. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art at the relevant time (“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. Ex-1002 ¶¶25-27.

IX. PRIORITY DATE

For purposes of this proceeding only, Petitioner applies the earliest alleged priority date of the '869 Patent: November 19, 2013.³ Accordingly, AIA 35 U.S.C. §102 applies and the '869 Patent was never eligible for PGR.

³ Petitioner respectfully reserves the right to challenge the priority date in other proceedings.

X. CLAIM CONSTRUCTION

Petitioner interprets the claims according to their plain and ordinary meaning under *Phillips*. 37 C.F.R. §42.100(b). To resolve this Petition, Petitioner does not believe that any term requires express construction.⁴ CTPG, 44; Ex-1002 ¶¶59.

XI. BRIEF DESCRIPTION OF THE APPLIED PRIOR ART

The challenged claims are obvious over Nakhjiri's UICC/eUICC profile provisioning using ECDH-derived symmetric keys (Ex-1005), combined with Bradley's teaching that subscription profiles include IMSI and K and are delivered encrypted to an embedded UICC for installation (Ex-1006 ¶¶2, 29–31), and Jeong's and Ala-Laurila's teaching to authenticate by sending identifier IMSI encrypted using a Diffie–Hellman–derived symmetric key to the network authentication server (Ex-1007 §§4.1.1, 5, Fig. 6; Ex-1013 ¶26); Ex-1002 ¶60.

A. Nakhjiri (Ex-1005)

Nakhjiri (U.S. Patent No. 9,210,138) was filed on April 17, 2013 and is prior art to the '869 Patent under 35 U.S.C. §102(a)(2). Ex-1002 ¶¶61-63.

⁴ The Samsung litigation is in its infancy. Petitioner respectfully reserves all rights to raise claim construction and other arguments in district court and will request leave to submit the district court's claim construction as soon as it becomes available. Additionally, should PO raise express or implied claim construction arguments in its Preliminary Response, Petitioner will respectfully seek a Preliminary Reply to respond. Consolidated Trial Practice Guide (CTPG), 44-45.

Nakhjiri enables “profiles provided by multiple application service providers to be securely transmitted” to a target device such as, for example, a smartphone having a Universal Integrated Circuit Card (UICC) in a wireless communication network. Ex-1005, 1:34-42, 7:56-62, 2:19-24. A key agreement exchange, shown in Figure 3 below, takes place between the mobile network operator (MNO)’s subscription manager-data preparation (SM-DP) server and the UICC to establish “a profile encryption key (PEK)” using Elliptic Curve Cryptography (ECC). Ex-1005, 5:25-27, Fig. 3. The PEK is created through “an Elliptic Curve Diffie-Hellman exchange (ECDH) algorithm where both the UICC and the MNO end up with exactly the same shared ECDH secret” derived from private/public key pairs. Ex-1005, 5:27-31. The PEK is used “to encrypt the profile for the UICC,” which is delivered “to the target device.” Ex-1005, 5:53-58.

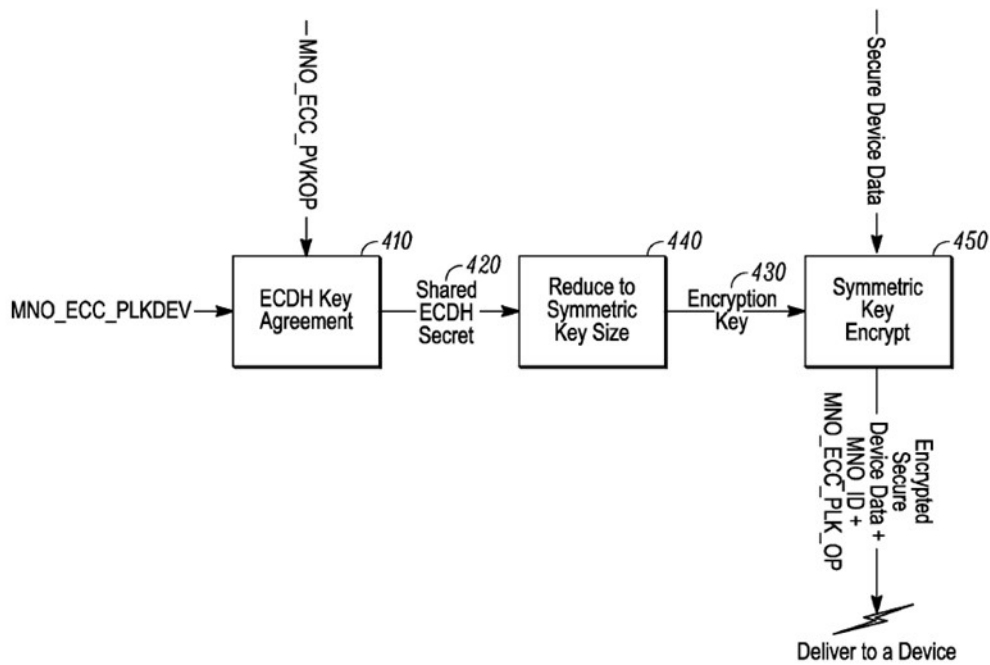


FIG. 3

Nakhjiri’s eUICC/UICC profile includes “security application algorithm codes, data and cryptographic keys” (*id.* 2:4–6); and signing and signature verification of messages between the provisioning server and the eUICC. *Id.* 3:27–37, 5:14–24.

B. Bradley (Ex-1006)

Bradley (U.S. Patent Publication No. 2014/0024343) was filed on October 10, 2013 and is prior art to the ’869 Patent under 35 U.S.C. §102(a)(2). Ex-1002 ¶¶64–65.

Bradley provides additional detail about the eUICC profile, teaching that it includes “relevant subscription information such as the *IMSI*, *K*, *Op*, *IMPU* and

algorithm constants,” where *IMSI* is an international mobile subscriber identity, and *K* is a secure key used for future communications. Ex-1006 ¶29. The secure vault then transmits the “personalisation script to device X encrypted for Device X’s embedded secure element ... over the IP link” and “Device X (including its embedded secure element) decrypts and runs the personalisation script thus provisioning the subscription onto the embedded secure element.” Ex-1006 ¶29; *see also id.* ¶¶2, 17, 30-31.

C. Jeong (Ex-1007)

Jeong was published in the Journal of Korea Multimedia Society, Vol. 13, No. 11 (pp. 1687-97) in November 2010 and is prior art to the ’869 Patent under 35 U.S.C. §102(a)(1). Ex-1016; Ex-1017. It is available on the website of the Korea Multimedia Society (founded in 1997), which publishes a monthly journal and hosts bi-annual conferences. Ex-1017, 1. It also makes full-text reproductions of its journal articles available for download dating back to 1998. Ex-1017, 2-4. Jeong is also available in the catalog of the National Library of Korea on its “official e-government website of Korea.” Ex-1016. Ex-1002 ¶¶66-67. Jeong’s original publication in Korean is attached as Ex-1012, and a certified translation is provided at Ex-1007.

Jeong teaches a “safe authentication key agreement (AKA)” process for securing mobile payments in the “smartphone environment” Ex-1007 §3.2. Jeong

notes that in the prior-art 3GPP-AKA model, the USIM/MS (mobile device) communicates with a Serving Network (SN) and a Home Network (HN) that includes an Authentication Center (AuC). Ex-1007 §2.2. The MS sends its IMSI (International Mobile Subscriber Identity) to the HN for authentication. *Id.* However, Jeong states the conventional method exhibits a “privacy problem due to IMSI plaintext transmission in the existing 3GPP-AKA mutual authentication.” Ex-1007 §3.2. To protect the smartphone’s IMSI from being compromised if sent in the clear, Jeong instead “uses SSK_{MS-HN} , a shared secret key based on the EC-DH algorithm, between the MS [mobile station] and the certificate authority (HN) for mutual authentication.” Ex-1007 §4.1.1(1). Specifically, “The AKA module proposed in this paper prevents IMSI exposure by generating a shared secret key between the MS and the HN for user authentication and encrypting and transmitting the IMSI value of the USIM.” *Id.* §5. Jeong’s “shared secret key is generated by the EC-DH algorithm, and the shared secret key is used for mutual authentication.” *Id.* §3.1.1.

D. Ala-Laurila (Ex-1013)

Ala-Laurila (U.S. Patent Publication No. 2012/0300934) was published on November 29, 2012 and is prior art to the ’869 Patent under 35 U.S.C. §102(a)(1). Ex-1002 ¶¶68-69.

Ala-Laurila teaches “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” known security issues. Ex-1013 ¶¶4-5. Specifically, as shown in Figure 2 below, the MT (mobile terminal) “requests 202 (IMSI request) the identity module SIM for the IMSI identifier and the SIM returns 203 the IMSI identifier.” Ex-1013 ¶26. The MT then sends “the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a Network Access Identifier NAI.” Ex-1013 ¶26. The “NAI comprises the IMSI identifier obtained from the identity module SIM.” Ex-1013 ¶26. Ala-Laurila also teaches that the request “is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm,” where the PAC is the Public Access Controller server that enables the MT to authenticate with the network. Ex-1013 ¶26, Fig. 2 (red box). The PAC transmits data between the MT and the GAGW, which is “an entity in the mobile network GSMNW offering authentication services of mobile subscribers to the WLAN networks.” Ex-1013 ¶22. The GAGW uses “known GSM signalling for requesting authentication data for the identity module SIM, and perform[s] the authentication and calculation of the ciphering key.” Ex-1013 ¶23. Thus, MT obtains IMSI from SIM (steps 202–203), and sends an authentication start request including NAI “comprising the IMSI” to the PAC “preferably in ciphered form ... using the Diffie–Hellman algorithm” (Ex-1013

¶26), and PAC with GAGW performs authentication based on the IMSI. Ex-1013

¶¶22-23, 28, Fig. 2.

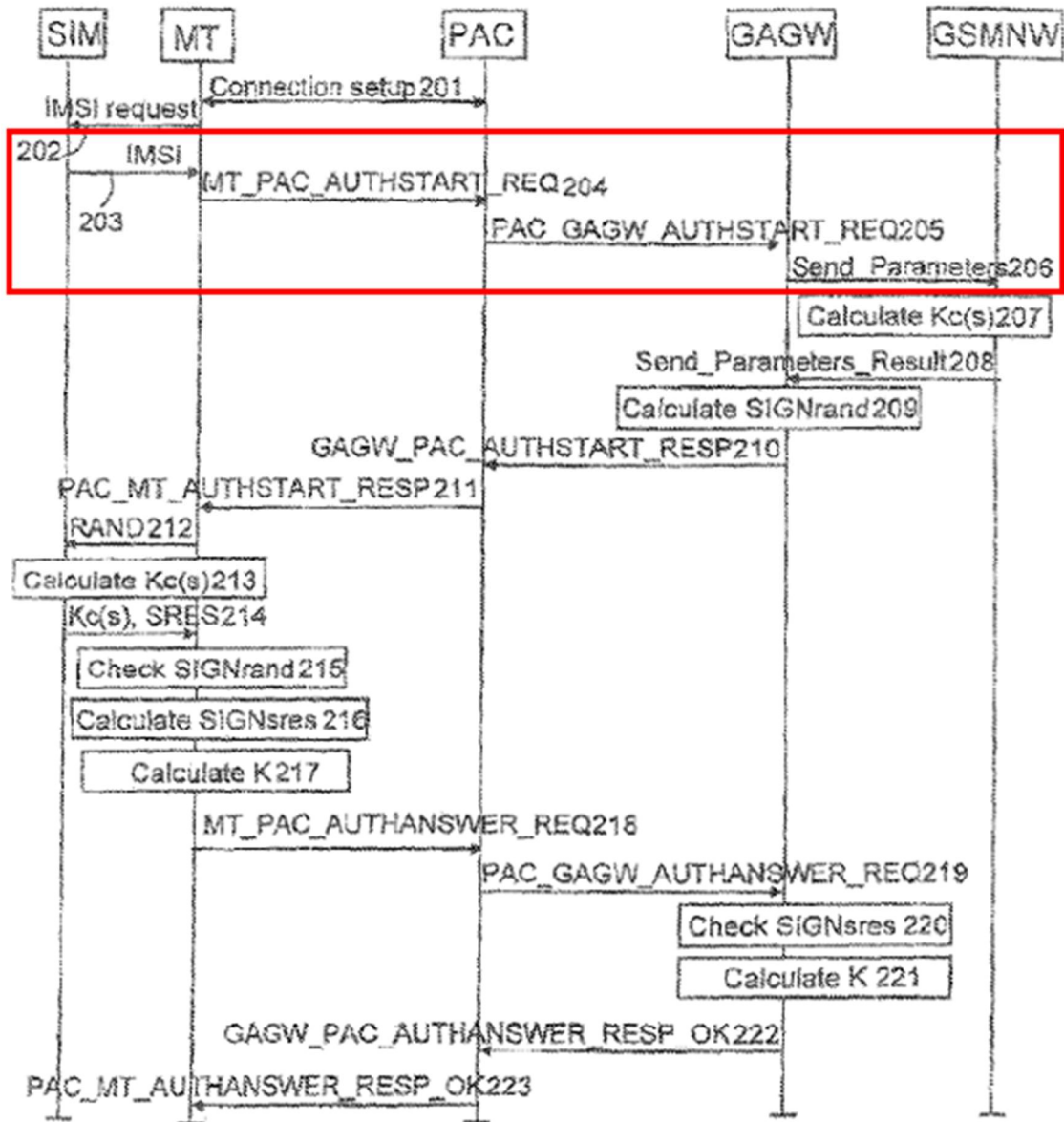


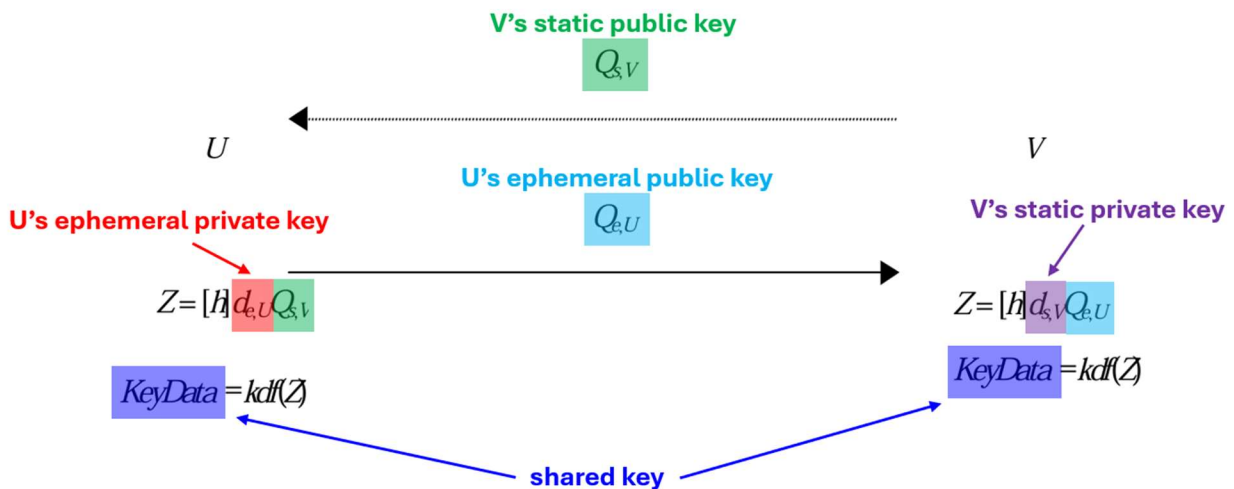
Fig. 2

E. ANSI X9.63-Overview (Ex-1014)

X9.63-Overview (ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography) was authored by Simon Blake-Wilson in 1999, was publicly available in 2000, and is prior art to the '869 Patent under 35 U.S.C. §102(a)(1). Ex-1015; Ex-1002 ¶¶70-71.

X9.63-Overview provides an overview of the ANSI X9.63 standard, which “[s]pecifies key agreement and key transport schemes using elliptic curve cryptography.” Ex-1014, 3. Among the schemes described in X9.63-Overview is the one-pass Diffie-Hellman key-agreement protocol, illustrated below:

ANSI X9.63 - 1-Pass DH



Id. 12. In this protocol, entity U generates an ephemeral public/private key pair ($Q_{e,U}, d_{e,U}$), by randomly selecting an ephemeral private key ($d_{e,U}$) (*id.* 7). Entity U

then sends its ephemeral public key ($Q_{e,U}$) to entity (V). *Id.* 12. Each entity then computes a shared secret Z using its own private key ($d_{e,U}$ for U, and $d_{s,V}$ for V) and the public key received from the other entity ($Q_{s,V}$ for U, and $Q_{e,U}$ for V). *Id.* The shared secret is then input into an X9.63 key-derivation function (KDF) to produce a shared key.

F. Pierce (Ex-1009)

Pierce (U.S. Patent Publication No. 2009/0323967) was published on December 31, 2009 and is prior art to the '869 Patent under 35 U.S.C. §102(a)(1). Ex-1002 ¶¶72-73.

Pierce teaches “techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices.” Ex-1009 ¶1. Specifically, Pierce teaches a method for enabling “the automatic generation of strong cryptographic keys by an embedded processing device at the time of manufacturing, before the product is released for distribution to end users ... by supplying the embedded device with entropy data that it uses to seed a pseudo random number generator (PRNG) that is used to generate the keys.” Ex-1009 ¶19. The “entropy data can be obtained by the embedded device from any of a number of sources, including those both internal and external to the manufactured product” (Ex-1009 ¶19) such as, for

example, “a sensor” or “GPS satellite time data (normally used for determining location coordinates) that are received from the GPS module.” Ex-1009 ¶36.

G. GlobalPlatform (Ex-1010)

GlobalPlatform (GlobalPlatform Remote Application Management over HTTP Card Specification V2.2 – Amendment B) was published in March 2012 and is prior art to the '869 Patent under 35 U.S.C. §102(a)(1). Ex-1018; Ex-1002 ¶¶74-76.

GlobalPlatform “defines a mechanism for an Application Provider to perform Remote Application Management (RAM) according to ETSI TS 102 226 [102 226] (i.e. loading, installation, and personalization) using the HTTP protocol (RFC 2616 [HTTP]) and PSK TLS security Over-The-Air.” Ex-1010, 5. GlobalPlatform further teaches that the connection parameters Tag-Length-Value (TLV) “embed all the needed parameters to establish a point to point TCP connection between the Administration Agent and the Remote administration server.” Ex-1010, 24.

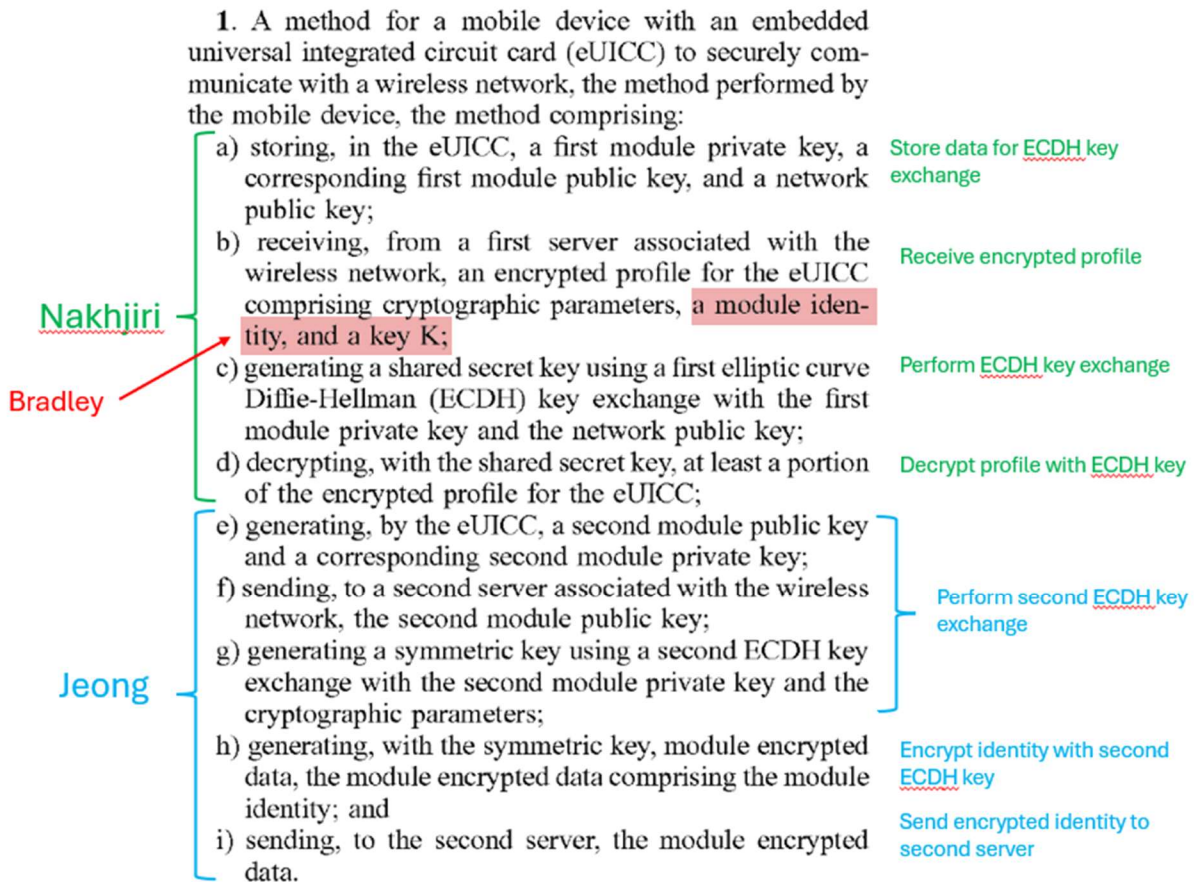
XII. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS

A. Ground 1: Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri, Bradley, and Jeong.

- 1. A POSITA would have been motivated to combine Nakhjiri’s teachings with Bradley’s teachings and Jeong’s teachings and would have had a reasonable expectation of success.**

A POSITA would have been motivated to combine Nakhjiri’s ECDH-based

secure profile delivery to UICCs (Ex-1005, 5:25–6:2) with Bradley’s disclosure that such profiles include identifier IMSI and key K (Ex-1006 ¶29), and with Jeong’s disclosure to transmit the IMSI-based identifier to the network encrypted under an ECDH-derived symmetric key for authentication (Ex-1007 §4.1.1(1)), to yield a unified, predictable eUICC flow. Specifically, Nakhjiri teaches to (i) securely provision profile data (including identifier IMSI and key K, as taught by Bradley) to the eUICC from a first provisioning server (SM-DP / SM-SR); and (ii) authenticate by encrypting the IMSI with an ECDH-derived symmetric key mutually derived with the network authentication server (HN), as taught by Jeong. These are complementary, well-understood steps within the same problem space (securing subscriber credentials and identifiers over untrusted links), and apply the same ECDH mechanism, as taught by both Nakhjiri and Jeong (and X9.63), to two adjacent phases of the lifecycle. Ex-1002 ¶77. Each reference expressly targets secure delivery of subscriber credentials or authentication in mobile environments and uses ECDH; their teachings are analogous and amenable to combination without change in principle of operation. Ex-1005, 2:19–24, 5:25–6:2; Ex-1006 ¶¶2, 29–31; Ex-1007 §§3-5; Ex-1002 ¶¶77-79.



As shown above, Nakhjiri and Bradley describe the provisioning process by which a mobile device with a eUICC downloads a secure profile that will allow it to communicate with the network. Nakhjiri teaches creating a symmetric profile-encryption-key (PEK) to decrypt an encrypted profile received from the network server by using the module’s private key and the server’s public key to perform a local Diffie-Hellman key agreement procedure between the eUICC and the network server. Ex-1005, 5:64:6:2. Other than referring to “data and cryptographic keys” (*id.* 2:4–6), Nakhjiri does not describe the keys and data that are included in the encrypted profile in detail, but Bradley, which similarly teaches decrypting an

encrypted profile received from a server, teaches that the encrypted profile includes “relevant subscription information such as the *IMSI*, [*key*] *K* ... and *algorithm constants*.” Ex-1006 ¶29.

Once the profile, including identifier IMSI and secret key K have been downloaded from the subscription manager and installed in the UICC, the UICC has to authenticate with the MNO (network operator). Ex-1002 ¶80. Prior art systems did so by sending the IMSI in the clear, whereafter the network server would use IMSI to look up an associated key in its database, confirming that the device could be associated with the network. Ex-1007 §2.2. Sending IMSI in the clear is a security risk because interception by an attacker could expose secret keys associated with IMSI. Ex-1002 ¶80. Jeong addresses this specific security problem. Ex-1007 §3.2 (“[W]e propose a robust user authentication module that improves ... [the] privacy problem due to IMSI plaintext transmission in the existing 3GPP-AKA mutual authentication.”). Specifically, “E- $IMSI_{MS}$ ” and other data that has been “encrypted with SSK_{MS-HN} , a shared secret key between HN and MS, are transmitted to the SN located near the MS ... [and] the SN then forwards the received E- $IMSI_{MS}$, MAC_{MS} , T_{MS} to the corresponding certificate authority (HN).” Ex-1007 §3.2. Here, “E- $IMSI_{MS} = E(SSK_{MS-HN}, IMSI_{MS})$,” meaning that it is the IMSI of MS encrypted with SSK_{MS-HN} , the “shared secret key based on the EC-DH algorithm, between MS and the certificate authority (HN) for mutual authentication.” Ex-1007 §4.1.1(1).

While Jeong does not describe the ECDH exchange between MS and *HN* in detail, it does describe a similar ECDH exchange between MS and *SN* (serving network).⁵ And the ECDH exchange between MS and SN is substantially the same as the key exchange in Nakhjiri. A POSITA would have understood that the ECDH process between MS and HN would proceed in the same way as the process between MS and SN (and the process between the module and subscription manager in Nakhjiri) in order to derive the SSK_{MS-HN} key used to encrypt IMSI. Ex-1002 ¶81.

A POSITA would have had a reasonable expectation of success in combining the teachings of Nakhjiri-Bradley-Jeong. Ex-1002 ¶82. All three describe methods for securing wireless communications using similar authentication and key agreement mechanisms and they address complementary security issues resulting in a more robust system for network authentication. Ex-1005, 5:64:6:2, 6:17-21; Ex-1006 ¶29; Ex-1007 §§2.2, 3.2, 4.1, Fig. 6. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations. Ex-1002 ¶82.

⁵ One time symmetric key $OT-SSK_{MS-SN}$ is generated based on an MS secret (private) key and a public key SNP from the SN server and is independently calculated by SN based on the MS public key MSP and SN secret (private) key, along with an elliptic curve starting point P. Ex-1007 §3.2(5)-(7).

2. Independent Claim 1

Generally speaking, Nakhjiri and Bradley teach the first part of the claim (encrypted profile download), and Jeong discloses the second part of the claim (authentication), as described in detail below.

- a. **Element 1[pre]: 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:**

Nakhjiri in view of Bradley and Jeong (“Nakhjiri-Bradley-Jeong”) teaches⁶ the preamble, to the extent it is limiting. Ex-1002 ¶¶29, 83-85.

Nakhjiri teaches techniques for enabling “multiple profiles provided by multiple application service providers to be securely transmitted” to a target device 106 in a wireless communication network. Ex-1005, 1:34-42. As shown in Figure 5 below, Nakhjiri teaches that the target device 106 may be a *smartphone* 106-1 (Ex-1005, 7:56-62), which includes a processor 602 that houses, executes, and processes “instructions related to reading and writing information to and from the target device 106 and/or the components contained therein” such as generating and sending “instructions to the [universal integrated circuit card] UICC 614, cache 620, or

⁶ Petitioner uses the term “teaches” to include both express teachings and those fairly suggested to a person of ordinary skill in the art. *In re Baird*, 16 F.3d 380, 383 (Fed. Cir. 1994); *In re Keller*, 642 F.2d 413, 425 (CCPA, 1981) (“The test for obviousness is...what the combined teachings of the references would have suggested to those of ordinary skill in the art.” (citations omitted)).

memory 604 in the target device.” Ex-1005, 8:2-9, Fig. 5. The secure execution environment includes *embedded UICCs*. Ex-1005, 2:19-24.

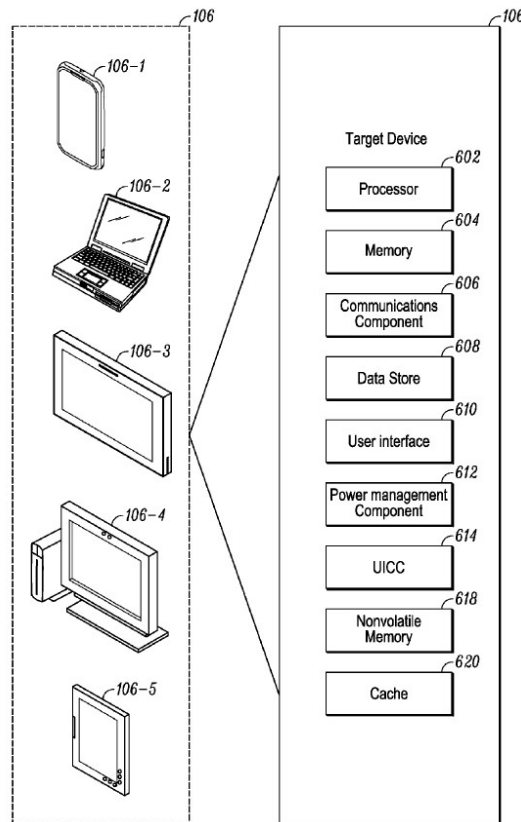


FIG. 5

- b. **Element 1(a): storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key;**

Nakhjiri-Bradley-Jeong teaches Element 1(a). Ex-1002 ¶¶30-31, 86. As background, an ECDH key exchange involves a cryptographic exchange between two entities, A and B. A generates a private/public key pair, d_A and Q_A , and B generates its own private/public key pair, d_B and Q_B . A and B exchange public keys:

$$A: Q_A \rightarrow B$$

B: $Q_B \rightarrow A$

A calculates a symmetric shared secret key, key_{ssk} , based on its own private key and B's public key: $key_{ssk} = kdf(d_A Q_B)$, where $kdf()$ is a key derivation function. Because of the elliptic curve property, $d_A Q_B = d_B Q_A$, B is able to calculate the same symmetric key based on its own private key and A's public key: $key_{ssk} = kdf(d_B Q_A)$. This ECDH-derived symmetric key can then be used to encrypt messages between A and B since they both independently possess the same symmetric key. Ex-1002 ¶86 (citing Ex-1033 (Boyd-Mathuria), 18; Ex-1014). For notational consistency, this public key (Q), private key (d) notation is used below. See Ex-1014 (ANSI X9.63 Overview, using this notation to describe key agreement and transport).

(1) A first module private key

Nakhjiri discloses a first module private key, d_m^{1st} . Ex-1002 ¶87. Nakhjiri teaches that 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" KGF (key generator function). Ex-1005, 5:61-64. The ECC private key (MNO_ECC_PVKDEV) corresponds to the recited "first module private key," as shown in Nakhjiri's Figure 4 (annotated), below, which depicts how the UICC module calculates the ECDH symmetric key:

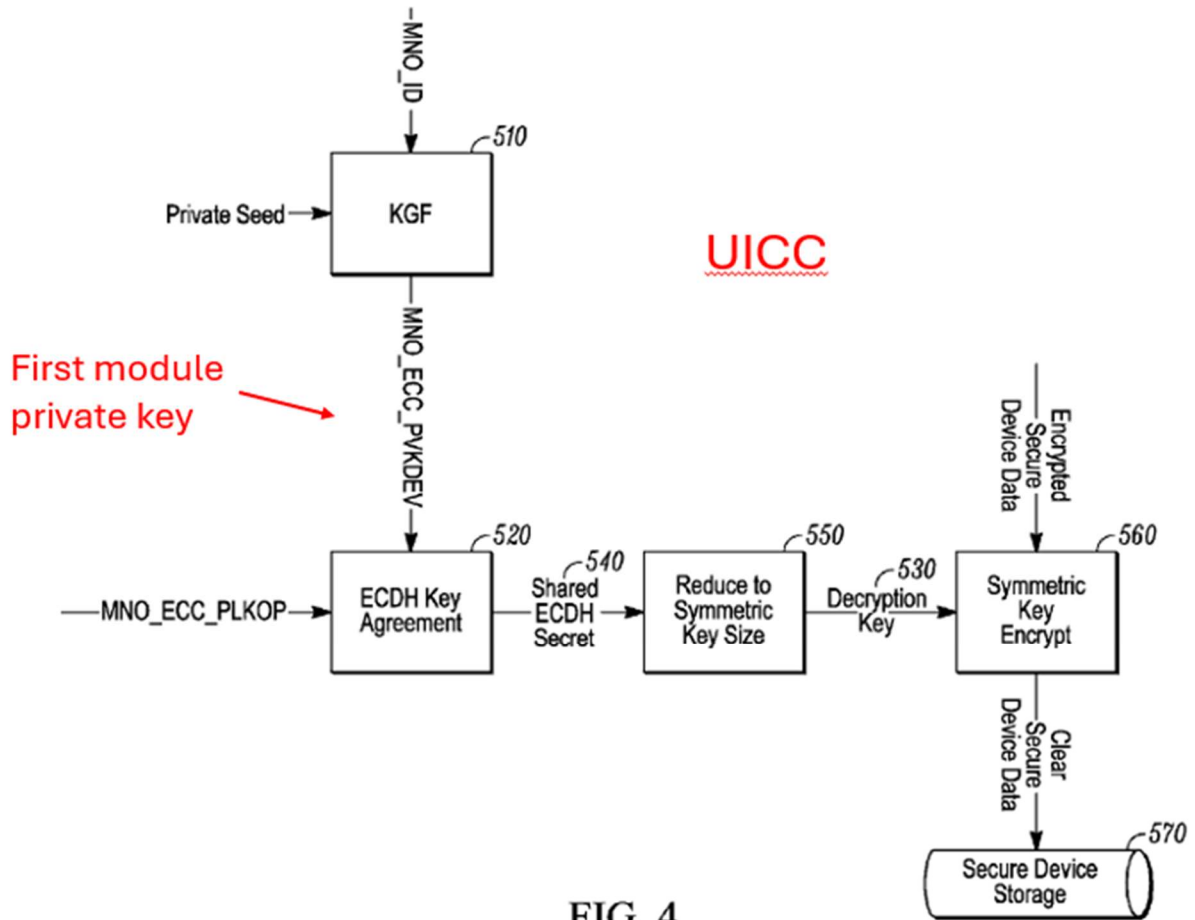


FIG. 4

Thus, $d_m^{1st} = \text{MNO_ECC_PVKDEV}$.

(2) A corresponding first module public key

Nakhjiri discloses a first module public key, Q_m^{1st} , corresponding to d_m^{1st} . Nakhjiri teaches that the device can then calculate its own public key corresponding to its private key: “once the ECC_PVK and the ECC curve are known, the ECC public key (PLK) can be generated simply by having knowledge of the PVK [private key] and the ECC curve” (Ex-1005, 4:31-37), “using Elliptic Curve multiplication operation: $\text{MNO_ECC_PLKDEV} = \text{MNO_ECC_PVKDEV} * G$ where G is the

Elliptic Curve base point.” Ex-1005, 4:51-56. The ECC public key (MNO_ECC_PLKDEV) corresponds to the recited “first module public key,” Q_m^{1st} . This is shown in Nakhjiri’s Figure 3, below, which shows the module’s public key (MNO_ECC_PLKDEV) received at the server and being used for the server’s calculation of the same ECDH symmetric key. Ex-1002 ¶88.

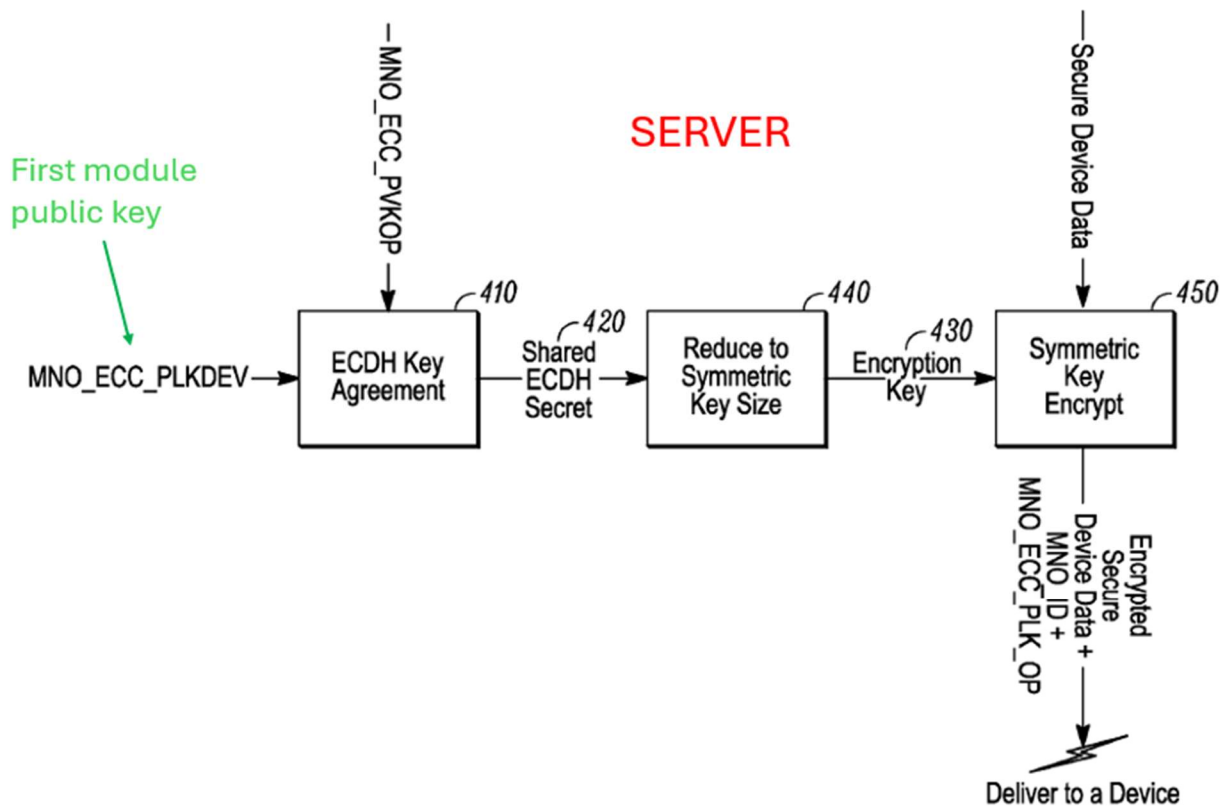


FIG. 3

Thus, $Q_m^{1st} = \text{MNO_ECC_PLKDEV}$.

(3) A network public key

Nakhjiri discloses a network public key, Q_n . Nakhjiri teaches that the “UICC then creates the PEK [profile encryption key] to perform decryption” on an

encrypted profile received from the MNO by using the ECC private key (MNO_ECC_PVKDEV) “and the *MNO ECC public key (MNO_ECC_PLKOP)* to perform a local ECDH key agreement process.” Ex-1005, 5:64:6:2. The MNO ECC public key (MNO_ECC_PLKOP) corresponds to the recited “network public key.” Going back to Figure 4, the eUICC receives the “network public key” (MNO_ECC_PKLOP) from the MNO and uses it, together with its own private key, to create a symmetric key using the ECDH key agreement process:

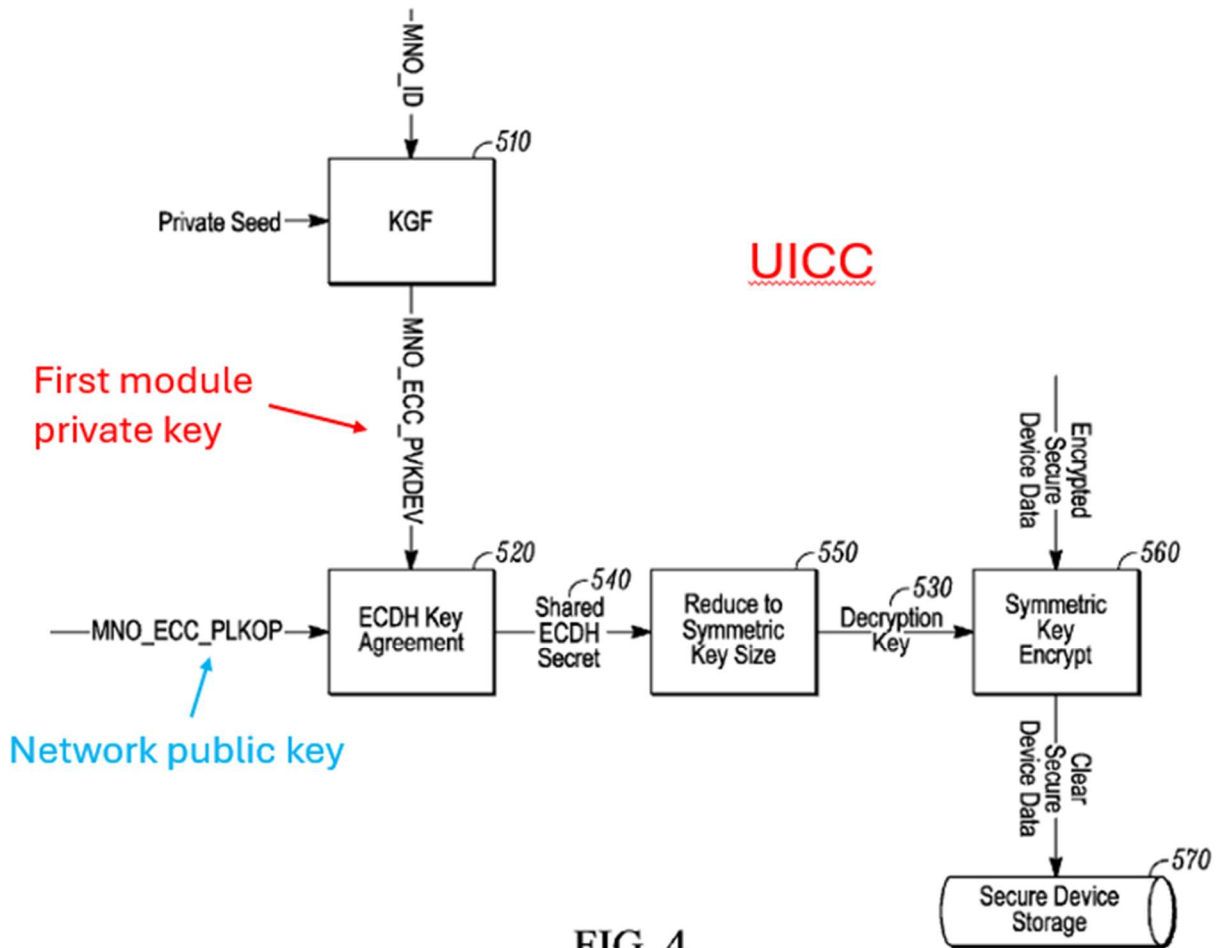


FIG. 4

Thus, $Q_n = \text{MNO_ECC_PLKOP}$. Although not required by the claim, Nakhjiri also discloses a network private key, d_n . Ex-1002 ¶89.

(4) Storing the keys in an eUICC

A POSITA would have understood that the first module private key (MNO_ECC_PVKDEV), first module public key (MNO_ECC_PLKDEV), and network public key (MNO_ECC_PVKDEV) are stored in the eUICC at least long enough for the eUICC to derive the “shared ECDH Secret 540,” shown in Figure 4, above, and send the first module public key (MNO_ECC_PLKDEV) to the network server (*see* Ex-1005, Figure 3). Ex-1002 ¶90. A POSITA would have also understood that the keys are stored in the eUICC because Nakhjiri teaches that the decrypted profile, which includes the “security application algorithm codes, data and cryptographic keys,” is installed “within a secure storage for later execution within the secure execution environment.” Ex-1005, 2:4-10. Specifically, Nakhjiri teaches the UICC generates and holds its ECC private key MNO_ECC_PVKDEV and corresponding public key MNO_ECC_PLKDEV (Ex-1005, 5:61–64, 4:51–56), and receives/uses the MNO ECC public key MNO_ECC_PLKOP (the “network public key”) to compute the shared secret. Ex-1005, 5:40–50, 5:64–6:2. Profiles and keys are stored in secure storage associated with the UICC. Ex-1005, 6:13–16, 2:4–10; Ex-1002 ¶90.

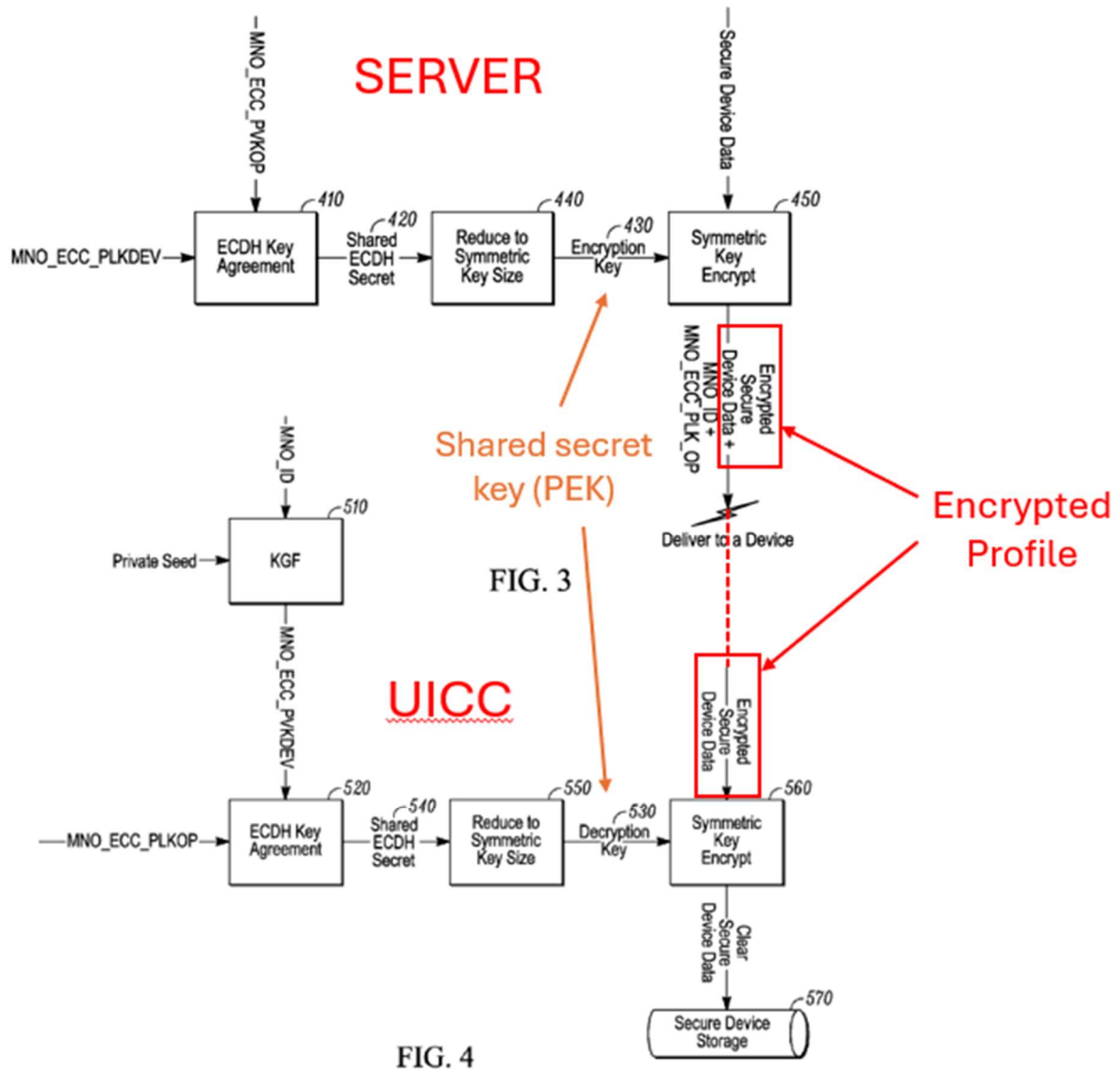
Claim element	Nakhjiri	Bradley	Jeong
First module private key, d_m^{1st}	MNO_ECC_PVKDEV		
First module public key, Q_m^{1st}	MNO_ECC_PLKDEV		
Network public key, Q_n	MNO_ECC_PLKOP		

- c. **Element 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;**

Nakhjiri-Bradley-Jeong teaches Element 1(b). Ex-1002 ¶¶32-34, 91-92.

- (1) **Receiving an encrypted profile for the eUICC from a first server associated with the wireless network**

Nakhjiri teaches that the SM-DP node associated with the mobile network operator (Ex-1005, 2:50-56) uses “its own ECC private key (MNO_ECC_PVKOP) and the UICC public key (MNO_ECC_PLKDEV) ... to perform a local ECDH key agreement 410 and create the PEK 430 from a shared ECDH secret 420.” Ex-1005, 5:45-50; Figs. 3 and 4, annotated below:



Nakhjiri’s PEK is the shared secret key key_{ssk} . The SM-DP server then “uses the PEK to perform a symmetric key encryption process 450 to *encrypt the profile* for the UICC” and delivers “the encrypted profile, along with the MNO device identifier (MNO_ID) and the MNO ECC public key (MNO_ECC_PLKOP) ... to the target device.” Ex-1005, 5:53-58. Nakhjiri further teaches that the “UICC then uses the PEK 530 to perform a symmetric key decryption process 560 to *decrypt the profile*,

which is stored in secure storage device 570 associated with the UICC.” Ex-1005, 6:13-16. The SM-DP corresponds to the recited “first server.” Ex-1002 ¶93.

(2) Encrypted profile comprises cryptographic parameters

Nakhjiri’s encrypted profile includes “security application algorithm codes, data and cryptographic keys” (Ex-1005, 2:4–6), which a POSITA would have understood to be “cryptographic parameters,” which include ECC parameters (curve ID and base point G) used later by the eUICC (*see id.* 4:51–56; Ex-1002 ¶94).⁷

(3) Encrypted profile comprises a module identity and a key K

Nakhjiri does not describe the “cryptographic keys” and “data” included in the profile in detail, but it would have been obvious that the profile would also comprise, for example, a module identity and key K, because these were known parameters to include in an encrypted eUICC profile. Ex-1002 ¶95 (citing Ex-1028 (CSMG), 16; Ex-1027 (Bhuyan) ¶¶25, 59, 62, 65; Ex-1008 (Rajadurai) ¶22; Ex-1025 (Semple) ¶¶26, 33, 47; Ex-1026 (Wang) ¶15). This is also taught by Bradley, which teaches at least two module identities—the IMSI (international mobile subscriber ID) and an ICCID (integrated circuit card identification number).

⁷ In ECC, “cryptographic parameters” are conventionally the curve identifier and base point G used in key agreement. Ex-1005, 4:51–56; Ex-1011, §§2–3; Ex-1002 ¶95 n.5.

Bradley teaches that “relevant subscription information [includes] the *IMSI*, *[key] K*, *Opc*, *IMPU* and algorithm constants.” Ex-1006 ¶29. Further, Bradley teaches “a method for downloading a subscription in an UICC embedded in a” mobile terminal, which includes “transferring an ICCID to the terminal; sending the ICCID over an IP link to a secure vault; selecting in the secure vault a subscription corresponding to the ICCID; transmitting the subscription to the terminal over the IP link;” and “storing the subscription in the terminal.” Ex-1006 ¶¶2, 17.

A POSITA would have understood an ICCID to be an “integrated circuit card identification number” that identifies an eSIM and would also have understood an IMSI to be an international mobile subscriber ID, which also serves to identify the eUICC module. Ex-1002 ¶¶96-97. The ’869 Patent also describes the IMSI as an example of a module identity. Ex-1001, 26:23-28. Thus, a POSITA would have understood that Nakhjiri’s encrypted profile would have included at least identity IMSI and key K, as disclosed in Bradley, as this is a predictable arrangement of known elements. Ex-1002 ¶97.

Thus, in the Nakhjiri-Bradley-Jeong combination, Nakhjiri’s encrypted profile for the eUICC would include at least a module identity IMSI and key K, as taught by Bradley. Ex-1002 ¶98. A POSITA would have been motivated to combine Nakhjiri-Bradley-Jeong and had a reasonable expectation of success in doing so for the reasons explained in Section XII.A.1. Ex-1002 ¶98.

Claim element	Nakhjiri	Bradley	Jeong
First module private key, d_m^{1st}	MNO_ECC_PVKDEV		
First module public key, Q_m^{1st}	MNO_ECC_PLKDEV		
Network public key, Q_n	MNO_ECC_PLKOP		
Encrypted profile with cryptographic parameters, ID, and key K	Profile encrypted by PEK, includes curve ID and base point G and cryptographic keys	ICCID, IMSI, key K	

- d. Element 1(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;**

Nakhjiri-Bradley-Jeong teaches Element 1(c). Ex-1002 ¶¶35-36, 99-100.

As discussed above for claim Element 1(b), Nakhjiri's network server SM-DP uses an ECDH exchange to generate a shared secret key (key_{ssk}) called PEK that is used to encrypt the profile sent to the eUICC. Nakhjiri's UICC computes the same ECDH shared secret as on the server and uses it to create the same shared secret key PEK using its own device private key MNO_ECC_PVKDEV and the network server's public key MNO_ECC_PLKOP, as shown in Figure 4, below.

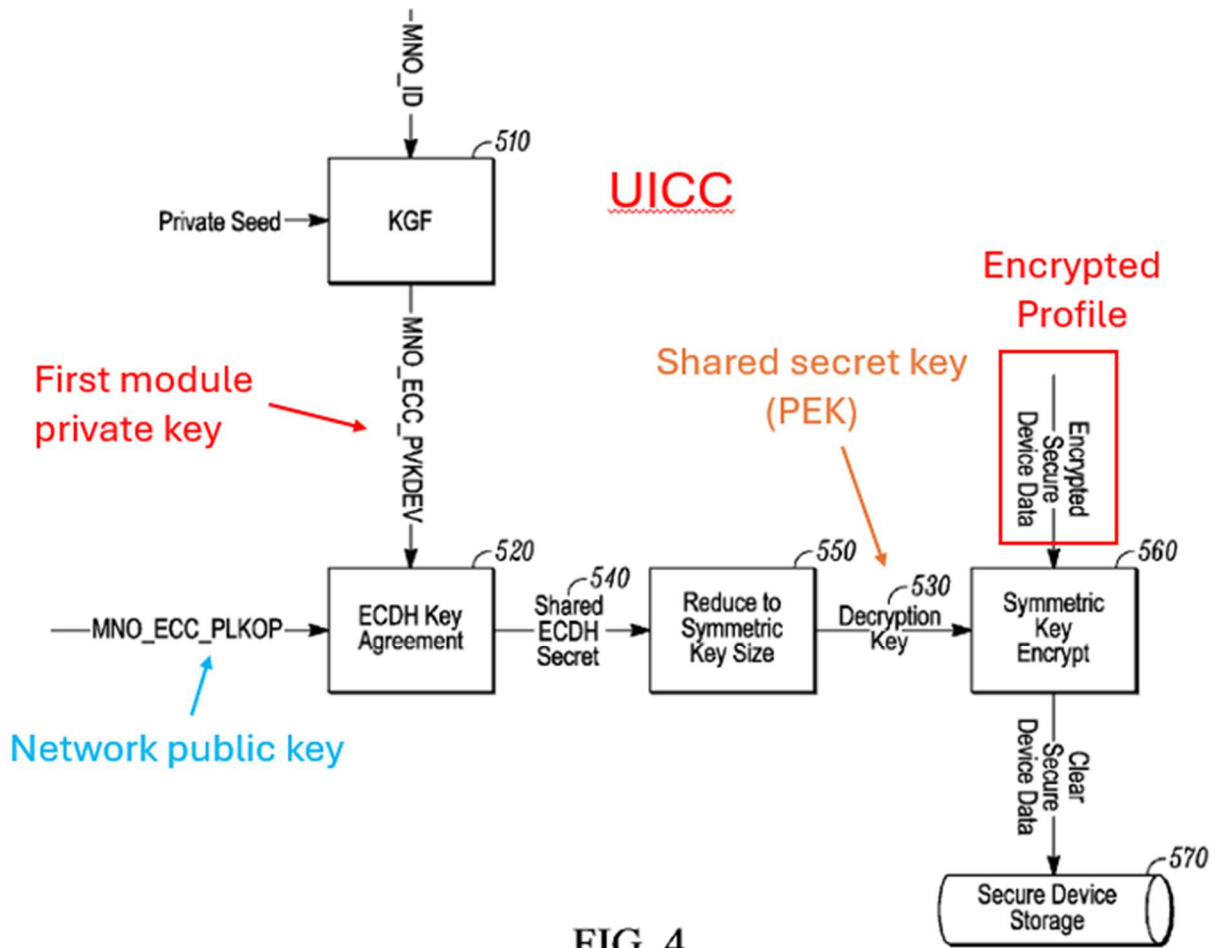


FIG. 4

Specifically, Nakhjiri teaches that “to create the PEK, the UICC uses the device ECC private key for this particular MNO (MNO_ECC_PKDEV) and the MNO ECC public key (MNO_ECC_PLKOP) to perform a local ECDH key agreement process 520.” *Id.* 5:65-62. The ECDH key agreement process 520 creates Shared ECDH secret 540, which is then processed through a hash/key derivation function 550 (“*kdf()*” in the X9.63 notation used above), resulting in shared secret key PEK 530 (decryption key). *Id.* 5:49-50, 6:9-11.

Nakhjiri summarizes the calculation of the ECDH shared secret (from which PEK is derived) independently by both the UICC and the MNO network server, stating “[o]ne example of a key exchange algorithm that may be employed is an Elliptic Curve Diffie-Hellman exchange (ECDH) algorithm where both the UICC and the MNO end up with exactly the same Shared ECDH secret.” Ex-1005, 5:27-31. For example:

Calculated by UICC: Shared ECDH
 Secret=MNO_ECC_PLK*MNO_ECC_PVKDEV

Calculated by MNO: Shared ECDH
 Secret=MNO_ECC_PLKDEV*MNO_ECC_PVK

Ex-1005, 5:31-37. As explained for claim Element 1(a), MNO_ECC_PVKDEV corresponds to the recited “first module private key” and MNO_ECC_PLK corresponds to the recited “network public key.” Ex-1002 ¶101; *see also* Ex-1005, 5:5:40-43 (“SM-DP generates its own ECC private, public key pair (denoted MNO_ECC_PVKOP and MNO_ECC_PLKOP, respectively.”). Nakhjiri thus teaches generating the profile encryption key (PEK) (i.e., shared secret key, key_{ssk}) using ECDH with the first module private key, d_m^{1st} , and network public key, Q_n . Ex-1002 ¶101.

Claim element	Nakhjiri	Bradley	Jeong
First module private key, d_m^{1st}	MNO_ECC_PVKDEV		

First module public key, Q_m^{1st}	MNO_ECC_PLKDEV		
Network public key, Q_n	MNO_ECC_PLKOP		
Encrypted profile with cryptographic parameters, ID, and key K	Profile encrypted by PEK, includes curve ID and base point G and cryptographic keys	ICCID, IMSI, key K	
Shared secret key, key_{SSK}	PEK		

Thus, PEK corresponds to key_{SSK} , where $key_{SSK} = kdf(d_m^{1st} Q_n)$.

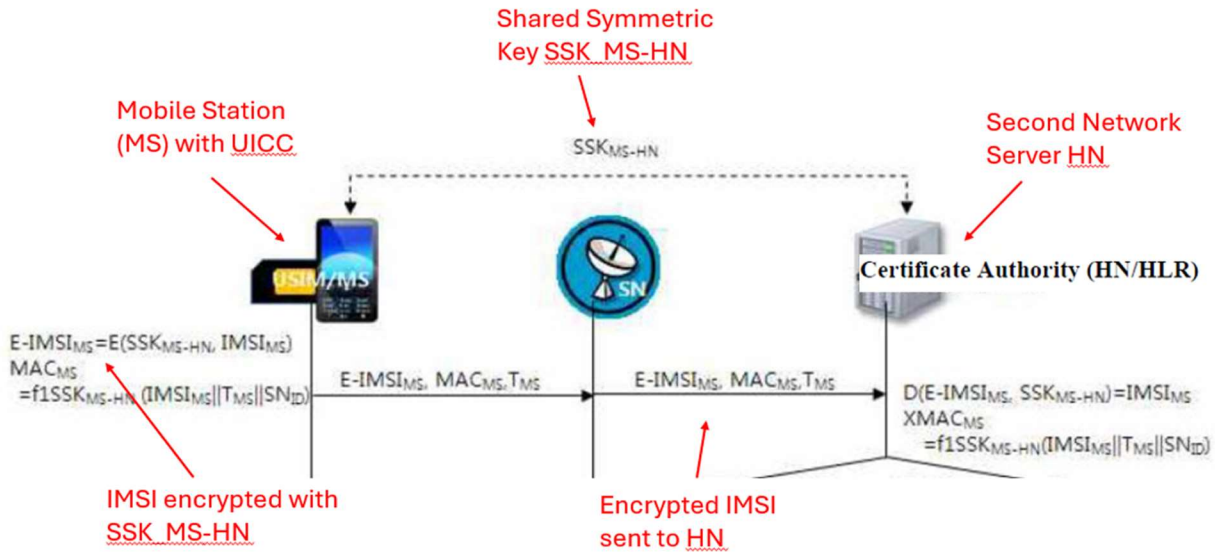
- e. **Element 1(d): decrypting, with the shared secret key, at least a portion of the encrypted profile for the eUICC;**

Nakhjiri-Bradley-Jeong teaches Element 1(d). Ex-1002 ¶¶37-38, 102-103.

As discussed for Element 1(c) above, Nakhjiri teaches that the UICC derives the shared secret key PEK. Ex-1005, 5:65-6:2. “The UICC then uses the PEK 530 to perform a symmetric key decryption process 560 to ***decrypt the profile***, which is stored in secure storage device 570 associated with the UICC.” Ex-1005, 6:13-16. Thus, Nakhjiri and Bradley teach the process claimed in Elements 1(a)-1(d) of receiving an encrypted profile at the UICC and decrypting it with a shared secret key derived between the UICC and the first network server through an ECDH exchange.

f. Element 1(e): generating, by the eUICC, a second module public key and a corresponding second module private key;

Before discussing Element 1(e) specifically, Elements 1(e)-1(i) together, as discussed above, recite an authentication process for sending the identity (IMSI), in encrypted form, from the UICC to a second network server, where the encryption is performed using a symmetric key derived using a second ECDH exchange between the eUICC and the second network server. Using the notation introduced above at claim Element 1(a), the UICC module generates a second module public key Q_m^{2nd} and a corresponding second module private key d_m^{2nd} . And as shown in the annotated excerpt of Figure 6 from Jeong (Ex-1007) below, the eUICC/MS (mobile station) and the Network server HN share a second, shared secret key (the recited “a symmetric key” (key_{SSK}^{2nd}), designated SSK_{MS-HN} to indicate it is shared between the MS and the HN. EX-1007 §4.1.1 (“The AKA module proposed in this paper uses ***SSK_{MS-HN}***, a shared secret key based on the EC-DH algorithm, between the MS and the certificate authority (HN) for mutual authentication”); Ex-1002 ¶¶39-41, 104-105.



And as further indicated above, 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,*” which is the HN server. Ex-1007 §4.1.2.

Although Jeong states that SSK_{MS-HN} is derived between MS and HN using the ECDH algorithm, it does not describe that exchange in detail. However, as discussed above in Section XII.A.1, it was well known in the art (as exemplified in Elements 1(a)-(c)) to use ECDH to generate a shared secret. In claim Element 1(g), this second ECDH exchange results in “a symmetric key” or key_{SSK}^{2nd} .⁸ Ex-1002 ¶105.

⁸ Moreover, Jeong describes the ECDH steps for generating a key between MS and another server called SN, where it creates a One-Time Shared Symmetric Key $OT-SSK_{MS-SN}$. It would have been obvious to a POSITA that the ECDH key agreement

Nakhjiri-Bradley-Jeong teaches Element 1(e). It was well known in the art that after provisioning a device with a profile from a first subscription management server, the mobile device would then have to authenticate with a second network server in order to start using the network for communications. Ex-1002 ¶106.

Because Jeong discloses that a shared symmetric key is derived by ECDH between MS and HN and details another ECDH exchange between MS and SN, and because Nakhjiri describes a similar ECDH exchange between the module and the subscription manager, 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. Ex-1002 ¶107; Ex-1007 §3.2(5). Thus, although Jeong does not specifically provide identifiers for the public/private key pairs used to generate the SSK_{MS-HN} key, the second module private key, d_m^{2nd} would correspond to d_{MS} for Jeong's MS private key, and the second module public key, Q_m^{2nd} would correspond to Q_{MS} for Jeong's MS public key.

Further, it 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. Ex-1002 ¶108. Indeed, Jeong

between MS and HN would proceed the same way it does between MS and SN. Ex-1002 ¶105 n.6.

suggests this dynamic approach is desirable when it describes the one-time ECDH key used to mutually authenticate and secure communications between the MS and SN, (Ex-1007 §3.2 (6-8)), and notes that the one-time key method also protects against “retransmission attacks.” *Id.* §4.1.3.⁹

Claim element	Nakhjiri	Bradley	Jeong
First module public key, Q_m^{1st}	MNO_ECC_PVKDEV		
Network public key, Q_n	MNO_ECC_PLKDEV		
Encrypted profile with cryptographic parameters, ID, and key K	MNO_ECC_PLKOP		
Shared secret key, key_{SSK}	Profile encrypted by PEK, includes curve ID and base point G and cryptographic keys	ICCID, IMSI, key K	
First module public key, Q_m^{1st}	PEK		
Second module public key, Q_m^{2nd}			Q_{MS}
Second module private key, d_m^{2nd}			d_{MS}

⁹ Moreover, Nakhjiri also teaches the same ECDH key generation process whereby “[u]sing the seed and the MNO_ID, the UICC is able to generate the MNO_ECC_PVKDEV and then, using the ECC curve, the UICC is able to create the associated MNO_ECC_PLKDEV,” where MNO_ECC_PVKDEV is the mobile device private key and MNO_ECC_PLKDEV is the associated mobile device public key. Ex-1005, 5:2-5. 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 HN. Ex-1002 ¶108 n.7.

- g. Element 1(f): sending, to a second server associated with the wireless network, the second module public key;**

Nakhjiri-Bradley-Jeong teaches Element 1(f). Ex-1002 ¶¶42-43, 109.

A POSITA would have understood that after generating its public/private key pair, MS would send its public key to the authentication server HN so that the server could perform the ECDH derivation process to generate its own copy of the second shared secret key, key_{SSK}^{2nd} (i.e., recited “symmetric key”).¹⁰ As Jeong discloses, HN includes the authentication server AuC (Ex-1007 §2.2), which a POSITA would have understood to be a “second server associated with the wireless network” and different from the subscription manager server in Nakhjiri. Ex-1002 ¶110.

- h. Element 1(g): generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;**

Nakhjiri-Bradley-Jeong teaches Element 1(g). Ex-1002 ¶¶44-45, 111-112.

A POSITA would have understood that the MS would then generate a symmetric key (key_{SSK}^{2nd}) using its private key d_{MS} and the public key of server HN, Q_{HN} , along with the cryptographic parameter P, indicating the starting point on the elliptic curve for the ECDH exchange.¹¹

¹⁰ Analogously, Jeong discloses the MS “transmits its public key, MSP, and a one-time shared secret key, OT-SSK_{MS-SN} to the SN.” Ex-1007 §3.2(6), Fig. 6 (MSP sent from MS to SN).

¹¹ Analogously, Jeong describes that for the MS-SN exchange, MS derives the SSK

Indeed, Jeong discloses that “[t]he AKA module proposed in this paper uses SSK_{MS-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-HN} , is generated using *the initial point* [P] and *secret key* [d_{MS}] registered in the USIM card and the certificate authority when the USIM card is first registered, and MACMS and XMACMS are generated for mutual authentication.” Ex-1007 §4.1.1. And as discussed above at Element 1(e), a POSITA would have understood the security benefits of generating SSK_{MS-HN} dynamically using generated private/public key pairs (instead of pre-installed ones). Ex-1002 ¶113. A POSITA would have understood that “the initial point” P is a cryptographic parameter of the ECDH algorithm. Ex-1002 ¶¶113-114.

Thus, the “symmetric key” key_{SSK}^{2nd} would correspond to SSK_{MS-HN} .

Claim element	Nakhjiri	Bradley	Jeong
First module public key, Q_m^{1st}	MNO_ECC_PVKDEV		
Network public key, Q_n	MNO_ECC_PLKDEV		
Encrypted profile with cryptographic parameters, ID, and key K	MNO_ECC_PLKOP		

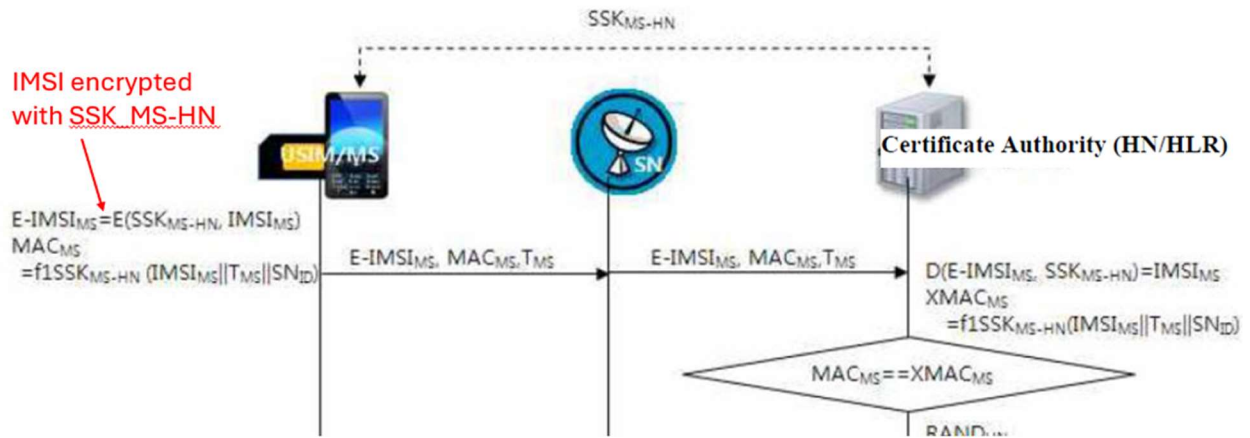
from its own private key MS, the network server’s public key SNP, and cryptographic parameter P (and the SN derives the same SSK using its own private key SN, the MS public key MSP, and cryptographic parameter P). Ex-1007 §3.2.2(6) (“OT- $SSK_{MS-SN} = EC-DH(P, MS, SNP)$ ”), Fig. 6 (“ $SSK_{MS-SN} = EC-DH(P, MS, SNP)$ ”).

Shared secret key, key_{SSK}	Profile encrypted by PEK, includes curve ID and base point G and cryptographic keys	ICCID, IMSI, key K	
First module public key, Q_m^{1st}	PEK		
Second module public key, Q_m^{2nd}			Q_{MS}
Second module private key, d_m^{2nd}			d_{MS}
Symmetric key, key_{SSK}^{2nd}			SSK_{MS-HN}

- i. Element 1(h): generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity; and**

Nakhjiri-Bradley-Jeong teaches Element 1(h). Ex-1002 ¶¶46-49, 115.

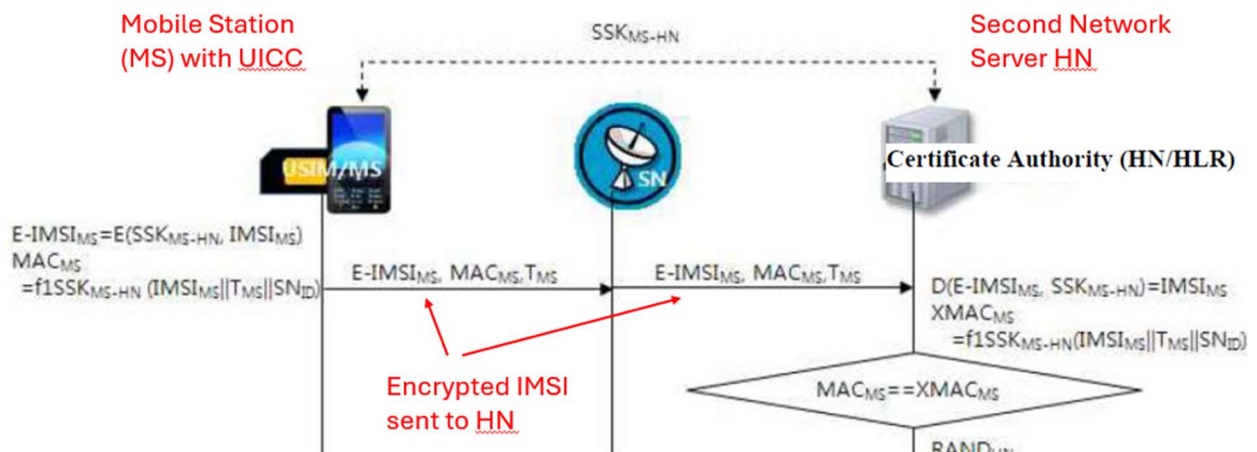
As shown in the excerpt of Figure 6 below, Jeong teaches that the MS prepares module encrypted data $E-IMSI_{MS} = E(SSK_{MS-HN}, IMSI_{MS})$, where the IMSI of MS is encrypted, “E(),” using SSK_{MS-HN} . Ex-1007, Fig. 6. Jeong further states “[t]he AKA module proposed in this paper solves the privacy problem of IMSI plaintext transmission by *encrypting IMSI with SSK_{MS-HN}* and transmitting it to the certificate authority.” Ex-1007 §4.1.2. Thus, Jeong discloses using the symmetric key SSK_{MS-HN} to prepare module encrypted data comprising IMSI, the module identity. Ex-1002 ¶116.



Claim element	Nakhjiri	Bradley	Jeong
First module public key, Q_m^{1st}	MNO_ECC_PVKDEV		
Network public key, Q_n	MNO_ECC_PLKDEV		
Encrypted profile with cryptographic parameters, ID, and key K	MNO_ECC_PLKOP		
Shared secret key, key_{SSK}	Profile encrypted by PEK, includes curve ID and base point G and cryptographic keys	ICCID, IMSI, key K	
First module public key, Q_m^{1st}	PEK		
Second module public key, Q_m^{2nd}			Q_{MS}
Second module private key, d_m^{2nd}			d_{MS}
Symmetric key, key_{SSK}^{2nd}			SSK_{MS-HN}
Module encrypted data			E-IMSI

j. Element 1(i): sending, to the second server, the module encrypted data.

Nakhjiri-Bradley-Jeong teaches Element 1(i) for the reasons described in the previous section. Ex-1002 ¶¶50-52, 117. As mentioned above, Jeong states “[t]he 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.*” Ex-1007 §4.1.2. This is shown in the excerpt of Figure 6 below:



As discussed for claim Element 1(f) above, a POSITA would have understood the home network HN including authentication server AuC to be a second / different server from the subscription manager server of Nakhjiri that sends the encrypted profile. Ex-1002 ¶¶118-119.

Thus, Nakhjiri-Bradley-Jeong renders obvious Claim 1.

3. Dependent Claims 2-4, 7, 9-14, and 16-20

- a. Claim 2: The method of claim 1, wherein the module identity comprises an international mobile subscriber identity (IMSI).**

Nakhjiri-Bradley-Jeong teaches Claim 2. Ex-1002 ¶¶120-121.

Bradley teaches that the module identity comprises an IMSI. Bradley teaches that “[t]he secure vault verifies the ICCID/secret activation code pairing and if valid it securely packages, encrypts and signs the entire personalisation script for the related embedded UICC ... as well as the relevant subscription information such as *the IMSI*.” Ex-1006 ¶31; *see also id.* ¶¶29–31. Jeong also teaches that the module identity comprises an IMSI. *E.g.*, Ex-1007 §§1, 2.2 (“USIM/MS identifies itself by sending *IMSI* (International Mobile Subscriber Identity)”).

- b. Claim 3: The method of claim 1, wherein the module identity comprises a permanent identifier for the mobile device.**

Nakhjiri-Bradley-Jeong teaches Claim 3. Ex-1002 ¶122.

Bradley teaches that the module identity comprises both ICCID and IMSI, which are permanent identifiers for the mobile device. Bradley teaches “Device X reads the ICCID from” an activation token and then “sends this ICCID over an IP link to a secure vault,” which “verifies the ICCID/secret activation code pairing and if valid it securely packages, encrypts and signs the entire personalisation script for the related embedded UICC as well as the relevant subscription information such as

the IMSI.” Ex-1006 ¶¶30-31. Jeong also teaches that the module identity comprises an IMSI. *E.g.*, Ex-1007 §2.2. Both the ICCID and IMSI are well known to be permanent identifiers for the mobile device. Ex-1002 ¶123.

c. Claim 4: The method of claim 1, wherein the cryptographic parameters comprise an identifier for a set of cryptographic parameters.

Nakhjiri-Bradley-Jeong teaches Claim 4. Ex-1002 ¶124.

Nakhjiri’s eUICC profile includes “security application algorithm codes, data and cryptographic keys.” Ex-1005, 2:4-6. And “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.” Ex-1005, 5:61-64. Nakhjiri discloses ECC curve/base point G. Ex-1005, 4:51–56. Nakhjiri also discloses identifier “g” and prime number “p” that identify elliptic curve parameters for ECDH key generation. *E.g.*, Ex-1005, 7:5-16 (“MNO_DH_PLKDEV= $g^{\text{MNO_DH_PVKDEV}} \bmod p$... where g is called a generator and p is a large prime number.”). One or more of Nakhjiri’s security application algorithm codes, KGF, ECC curve/base point G, and parameters g and p correspond to the recited “identifier for a set of cryptographic parameters.” Ex-1002 ¶125 (citing, *e.g.*, Ex-1025 (Semple) ¶33; Ex-1024 (Gouget) ¶¶42-45). This is also taught by Bradley.

Bradley teaches that the secure vault “securely packages, encrypts and signs the entire personalisation script for the related embedded UICC (containing SIM application, USIM application, ISIM application, CSIM application, any other network authentication applications as well as any SIM application Toolkit applications and Operating System Customisations/mechanisms related to that specific MNO) as well as the relevant subscription information such as the IMSI, K, Opc, IMPU and algorithm constants.” Ex-1006 ¶31; *see also id.* ¶29. A POSITA would have understood that the authentication applications, SIM application Toolkit applications, Operating system Customisations/mechanisms, and algorithm constants are identifiers for a set of cryptographic parameters. Ex-1002 ¶126.

This is also taught by Jeong. Jeong discloses that “the SN transmits to the MS the initial point for generating a one-time SSK,” where the initial point P identifies where on the ECC curve the key generation algorithm begins, thus identifying a set of cryptographic parameters. Ex-1007 §3.2.2(5); Ex-1002 ¶127.

- d. Claim 7: The method of claim 1, wherein the first server mutually derives the shared secret key using the first ECDH key exchange with the first module public key and a network private key corresponding to the network public key.**

Nakhjiri-Bradley-Jeong teaches Claim 7. Ex-1002 ¶128.

Nakhjiri teaches that the “Diffie-Hellman key agreement is performed ... where both the UICC and the MNO end up with exactly the same Shared DH secret:

Calculated by UICC: Shared DH

$$\text{Secret} = \text{MNO_DH_PLK}^{\text{MNO_DH_PVKDEV}} \bmod p$$

Calculated by MNO: Shared DH

$$\text{Secret} = \text{MNO_DH_PLKDEV}^{\text{MNO_DH_PVK}} \bmod p$$

where g is called a generator and p is a large prime number ... and where MNO_DH_PLKDEV is UICC's Diffie-Hellman public key, MNO_DH_PVK is the DH private key which belongs to the MNO and MNO_DH_PLK is the corresponding MNO public key." Ex-1005, 7:6-17. The "first server" is the MNO's SM-DP node. Ex-1002 ¶129.

- e. **Claim 9: The method of claim 1, further comprising in step h) generating, with the symmetric key and an Advanced Encryption Standard (AES), the module encrypted data.**

Nakhjiri-Bradley-Jeong teaches Claim 9. Ex-1002 ¶130.

As explained for Element 1[h], the Nakhjiri-Bradley-Jeong combination teaches generating the module encrypted data with the symmetric key. Ex-1002 ¶131. Nakhjiri also teaches that AES may be used for the KGF/KDF for generating the symmetric key. Specifically, Nakhjiri teaches that "for a highly robust implementation a hardware key ladder may be implemented such that both the seed and the PVK cannot be exposed without hardware tampering." Ex-1005, 4:57-59. For example, "the KGF can be a standard MAC (Message Authentication Code)

function such as HMAC-SHA1, HMAC-SHA256, AES-CMAC, and so on.” Ex-1005, 4:61-63. Thus, the KGF/KDF used to generate the symmetric key for encrypting the module encrypted data may be based on an AES standard. Ex-1002 ¶131.

f. Claim 10: The method of claim 1, wherein steps g) and h) occur before step f).

Nakhjiri-Bradley-Jeong Claim 10. Ex-1002 ¶¶132-133.

This dependent claim specifies that generating the second symmetric key (step g) and using it to encrypt the module data (including identity) (step h) happen before the second module public key is sent to the second server (step f). As explained for claim Elements 1[f]-1[h], in the Nakhjiri-Bradley-Jeong combination, Jeong discloses “the MS generates $OT-SSK_{MS-SN}$ with its own secret key to the public key received from the SN. **Then, it transmits its public key, *MSP***, and a one-time shared secret key, $OT-SSK_{MS-SN}$ **to the SN.**” Ex-1007 §3.2(6). Thus, step (g), generating the symmetric key, happens before step (f), sending the second module public key, *MSP*, to the server. As explained for claim Elements 1[e]-1[h], a POSITA would have understood the generation of SSK_{MS-HN} to occur in the same way $OT-SSK_{MS-SN}$ is generated.

Moreover, the ordering of these steps is a simple design choice. And first encrypting IMSI (step h) and then sending *MSP* to the second server (step f) would

minimize communication transactions because the encrypted IMSI and public key could then be sent at the same time. Ex-1002 ¶134.

- g. Claim 11: The method of claim 1, wherein the network public key is associated with an eUICC subscription manager.**

Nakhjiri-Bradley-Jeong teaches Claim 11. Ex-1002 ¶¶135-136.

Nakhjiri teaches that source node 102 is “associated with a mobile network operator, the trusted intermediate node is a subscription manager-data preparation (SM-DP), other intermediate nodes are non-serving subscription managers (SMs), and a last intermediate node, which is trusted by the target device 106, is a serving subscription manager-secure routing (SM-SR)” for the UICC. Ex-1005, 2:50-58. Nakhjiri further teaches that “to establish a profile encryption key (PEK) using ECC, a key agreement exchange may take place between the MNO SM-DP and each UICC.” Ex-1005, 5:25-27. Moreover, Nakhjiri teaches that the encrypted profile created by the SM-DP “and the MNO ECC public key (MNO ECC PLKOP) are delivered to the target device.” Ex-1005, 5:40-58.

- h. Claim 12: The method of claim 11, wherein the eUICC subscription manager comprises the first server.**

Nakhjiri-Bradley-Jeong teaches Claim 12. Ex-1002 ¶137.

As shown in Figure 1 below, Nakhjiri teaches that “[e]nvironment 100 includes a provisioning infrastructure that includes a source node 102, one or more wired and/or wireless communication networks 104, and intermediate nodes 108,”

which transmit “profiles to target device 106.” Ex-1005, 2:37-42. Source node 102 is “associated with a mobile network operator, the trusted intermediate node is a subscription manager-data preparation (SM-DP), other intermediate nodes are non-serving subscription managers (SMs), and a last intermediate node, which is trusted by the target device 106, is a serving subscription manager-secure routing (SM-SR)” for the UICC. Ex-1005, 2:50-58. Nakhjiri’s intermediate node associated with SM-DP corresponds to the recited “first server.” Ex-1002 ¶138.

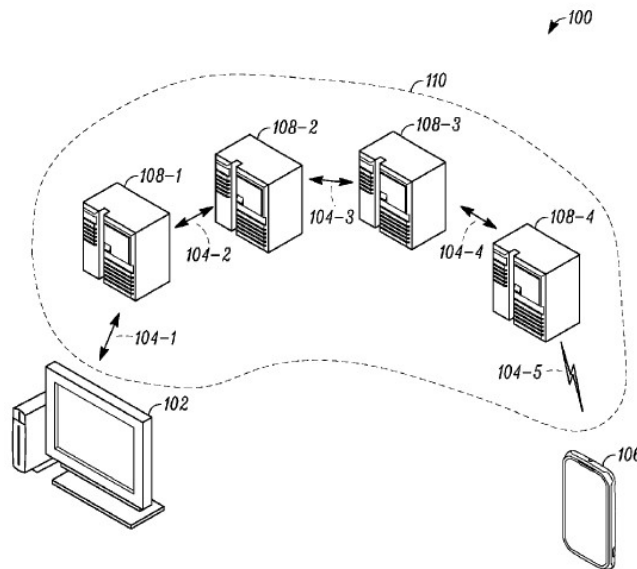


FIG. 1

- i. **Claim 13: The method of claim 1, further comprising:**
- j) **receiving, from the wireless network, a random number (RAND) and generating a response (RES) using the RAND and the key K.**

Nakhjiri-Bradley-Jeong teaches Claim 13. Ex-1002 ¶139.

Jeong describes the well-known traditional 3GPP-AKA method, which it illustrates in Figure 2, below. The USIM/MS sends IMSI to the SN and HN. Ex-

1007 §2.2. The HN returns a random number RAND (highlighted below), which the MS uses to calculate a response RES (highlighted below). *Id.* It is well known that in the 3GPP-AKA, RES is calculated using the RAND and the key K. Ex-1002 ¶140. “The SN authenticates the device and the user by comparing the received RES with the XRES it has stored.” Ex-1007 §2.2, Fig. 2.

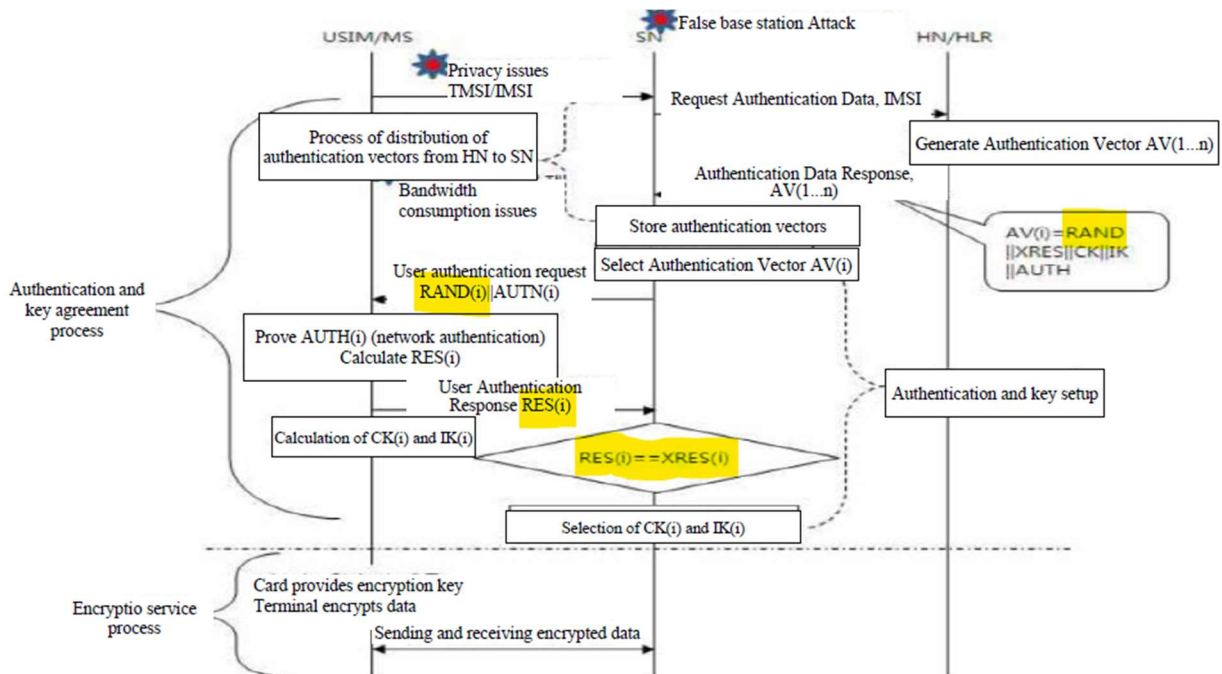


Figure 2. 3GPP-AKA Mutual Authentication Flow [10]

Jeong suggests certain improvements to this algorithm: “The AKA module designed in this paper *uses the existing 3GPP-AKA authentication method*, but we analyzed the problems that may occur in the existing 3GPP-AKA and improved the problems.” Ex-1007 §4. In particular, “[t]he 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.” Ex-1007 §4.2. While Jeong also suggests other improvements for reducing the required data storage in the SN, a POSITA primarily interested in enhancing security would not necessarily also want to further alter the AKA procedure to save storage and would have followed Jeong’s guidance to use “the existing 3GPP-AKA authentication method” but fix the “privacy problem of IMSI plaintext transmission by encrypting IMSI,” as taught by Jeong while retaining the proven RES, XRES authentication procedure using RAND and the key K. Ex-1002 ¶141.

- j. Claim 14: The method of claim 1, further comprising before step b), authenticating the first server by (i) receiving a server digital signature and (ii) verifying the server digital signature with a server public key.**

Nakhjiri-Bradley-Jeong teaches Claim 14. Ex-1002 ¶142.

Nakhjiri discloses that the packets received by the target device from the provisioning server are signed by the source node (first server) and all intermediate nodes:

Generally, target device 106 receives the profile in packets that are transmitted through a node path 110. As part of the outer layer encryption process the packets *have a cryptographic signature for each node along the required node path*. FIG. 2 illustrates a packet 112 in simplified form, which has cryptographic signatures from each of the intermediate nodes 108 (“Int. #1 Sig.” etc.), as well as *an end-to-end cryptographic signature (shown as “Source Sig.”)*, which is signed over the payload (e.g., sensitive data), which may also include a profile.

Ex-1005, 3:27-37. Nakhjiri further discloses that “the UICC can obtain the MNO ECC public key (MNO ECC PLKOP) from the MNO along with the encrypted data.” *Id.* 6:3-5. Nakhjiri also discloses that if the UICC makes its own key list public, any party could use a UICC public key to encrypt an illegitimate profile. *Id.* 5:14-17. To avoid this attack, Nakhjiri teaches that the MNO SM-DP (first sever) could “sign the encrypted profile” and that the UICC would use a certificate for the SM-DP to authenticate it (*id.* 5:17-21), which a POSITA would have understood to mean that the verification is done with the server’s public key. Ex-1002 ¶143. Though Nakhjiri disfavors this approach over just keeping the keylist secret because it requires the UICC to store certificates of many SM-DP’s (Ex-1005, 5:14-24), that is only a disadvantage when managing many profiles from many SM-DPs and would not be a problem for managing just a few profiles.¹² Ex-1002 ¶143. Thus, Nakhjiri-Bradley-Jeong renders Claim 14 obvious.

- k. Claim 16: The method of claim 1, wherein the first server, the second server, and the wireless network are associated with a mobile network operator.**

Nakhjiri-Bradley-Jeong teaches Claim 16. Ex-1002 ¶144.

¹² Nakhjiri’s observation that storing many SM-DP certificates could be undesirable operationally (Ex-1005, 5:14–24) does not criticize or discourage use of signatures per se; it proposes an alternative (key list secrecy). Selecting certificate-based verification for a smaller operator set remains an obvious, expressly taught option. Ex-1002 ¶143 n.10.

Nakhjiri teaches that the first server (i.e., intermediate node for SM-DP) and wireless network are associated with a mobile network operator. Nakhjiri teaches that “[e]nvironment 100 includes a provisioning infrastructure that includes a source node 102, one or more wired and/or wireless communication networks 104, and intermediate nodes 108,” which transmit “profiles to target device 106.” Ex-1005, 2:37-42. Nakhjiri further teaches that “source node 102 is associated with an ASP (e.g., a mobile network operator) in secure communication with a trusted one of the intermediate nodes ... such as a trusted subscription manager capable of end-to-end encryption of a packet having the sensitive data.” Ex-1005, 2:45-49. Source node 102 is “associated with a mobile network operator, the trusted intermediate node is a subscription manager-data preparation (SM-DP), other intermediate nodes are non-serving subscription managers (SMs), and a last intermediate node, which is trusted by the target device 106, is a serving subscription manager-secure routing (SM-SR)” for the UICC. Ex-1005, 2:50-58. Nakhjiri further teaches that “to establish a profile encryption key (PEK) using ECC, a key agreement exchange may take place between the MNO SM-DP and each UICC.” Ex-1005, 5:25-27. A POSITA would have understood that Nakhjiri’s teaching that the provisioning architecture includes a plurality of intermediate nodes means that a second server also associated with the mobile network operator is included. Ex-1002 ¶145.

As explained for claim Element 1[f], Jeong teaches a second server HN (home network / certificate authority) including an authentication center (AuC), which is the counterpart of the mobile station MS in the second ECDH exchange in the Nakhjiri-Bradley-Jeong combination. Ex-1007 §2.2; *see also id.* §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.***”).

Thus, both the first server (subscription manager for preparing and delivering the secure profile) and the second server (HN / certificate authority for authenticating the mobile device) are associated with the MNO. Ex-1002 ¶¶146-147.

I. Claim 17: The method of claim 1, wherein the eUICC comprises a processor, firmware, and protected memory.

Nakhjiri-Bradley-Jeong teaches Claim 17. Ex-1002 ¶¶148-149.

Nakhjiri teaches that its “UICC 614 may include an internal central processing unit (CPU), random access memory (RAM), read-only memory (ROM), electrically-erasable programmable read only memory (EEPROM), other non-volatile or volatile memory, and/or input/output circuitry.” Ex-1005, 8:63-9:3. Nakhjiri further teaches any or all of its modules and components “can be implemented as hardware, firmware, fixed logic circuitry, or any combination thereof.” Ex-1005, 10:35-28. It further teaches that profiles are stored “within a ***secure storage*** for later execution

within the secure execution environment.” Ex-1005, 2:9-10. And the profile “is stored in *secure storage device* 570 associated with the UICC.” *Id.* 6:13-16.

m. Claim 18: The method of claim 1, wherein the cryptographic parameters include a base point G for an elliptic curve.

Nakhjiri-Bradley-Jeong teaches Claim 18. Ex-1002 ¶150.

Nakhjiri teaches that its encryption algorithm “employs Elliptic Curve Cryptography (ECC) as the public key agreement algorithm which is used to randomly generate a private key.”¹³ Ex-1005, 6:61-63, 4:51-56 (describing ECC parameter G). Nakhjiri further teaches that the “Diffie-Hellman key agreement is performed ... where g is called a generator and p is a large prime number.” Ex-1005, 7:7-20. Jeong similarly discloses that “the SN transmits to the MS the initial point for generating a one-time SSK” using an ECDH exchange. Ex-1007 §3.2.2(5). A POSITA would have understood these parameters to be base points or starting points for an elliptic curve used in the ECDH algorithm. Ex-1002 ¶151.

n. Claim 19: The method of claim 1, wherein the mobile device comprises a wireless device with a radio for communicating with a plurality of base stations for the wireless network.

Nakhjiri-Bradley-Jeong teaches Claim 19. Ex-1002 ¶¶152-153.

¹³ In ECC, “cryptographic parameters” are conventionally the curve identifier and base point G used in key agreement. Ex-1005, 4:51–56; Ex-1011, §§2–3; Ex-1002 ¶151 n.11.

Nakhjiri's mobile device is a wireless device with a radio for communicating with a plurality of base stations. For example, Nakhjiri teaches that the communication component of its mobile device includes "transmit chain components and receive chain components associated with a transmitter and receiver." Ex-1005, 8:28-32. Nakhjiri also teaches that its mobile device includes a nonvolatile memory component 618, which contains "subscription, connection, or any information related to establishing a connection with a wireless network or authenticating a user to such a network." Ex-1005, 9:21-25. Nakhjiri further teaches that the "wireless network may utilize an access technology and/or communication protocol or standard such as, but not limited to, CDMA2000 1X (IS-2000), 1x, 1xRTT, CDMA2000, and/or 1xEV-DO (Evolution-Data Optimized), also known as EV-DO or EV, or any other access technology that is part of the 3G access technology family." Ex-1005, 9:25-31. Moreover, Nakhjiri teaches that it stores "information related to radio access networks utilizing several access technologies and/or communication protocols, such as, but not limited to, Global System for Mobile Communication (GSM), Enhanced Data Rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), High Speed Packet Access (HSPA), Long Term Evolution (LTE), LTE Advanced, or any other high-speed data packet network access technology, including those access technologies that are part of the 4G access technology family." Ex-1005, 9:47-59.

- o. Claim 20: The method of claim 1, wherein the eUICC comprises a package soldered to a circuit board of the mobile device.**

Nakhjiri-Bradley-Jeong teaches Claim 20. Ex-1002 ¶154.

Bradley teaches that it was “known to solder or weld the UICC in a terminal, in order to get it dependent of this terminal.” Ex-1006 ¶10. Specifically, Bradley teaches that the chip is “soldered to the mother-board of the terminal or machine and constitutes an e-UICC.” Ex-1006 ¶10. Bradley further teaches that its invention “applies to such soldered UICCs (e-UICCs).” Ex-1006 ¶11. In the Nakhjiri-Bradley-Jeong combination, Nakhjiri’s eUICC is a package soldered to a circuit board of the mobile device, as taught by Bradley. Ex-1002 ¶155.

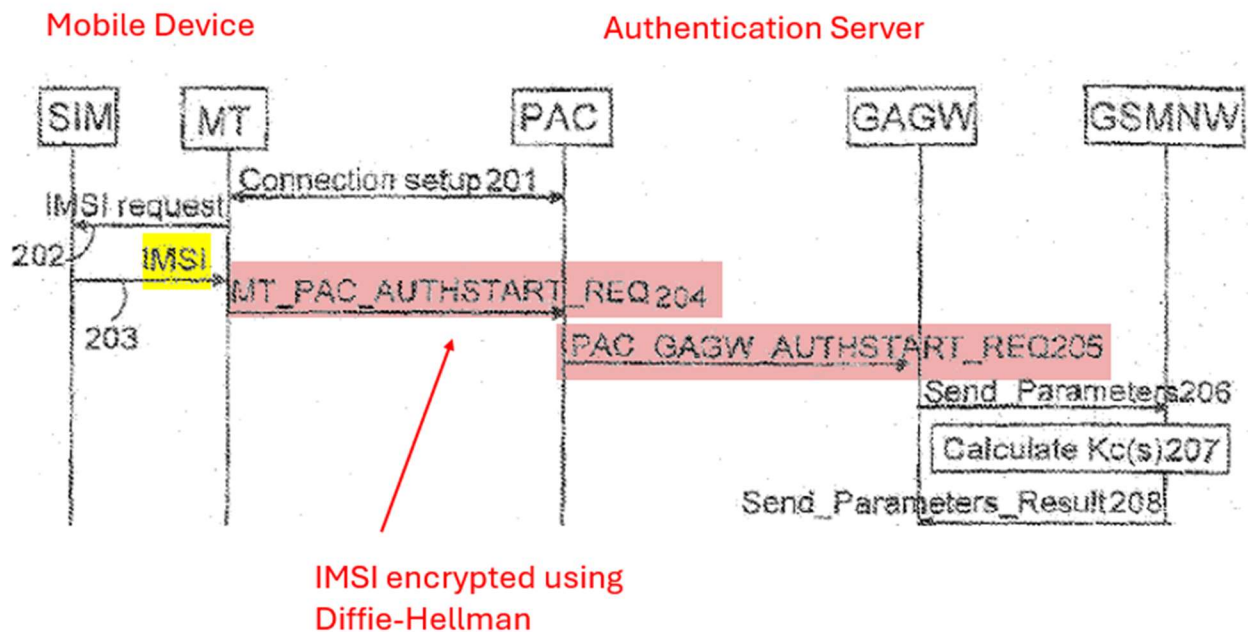
B. Ground 2: Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri in view of Bradley and Ala-Laurila.

- 1. A POSITA would have been motivated to combine Nakhjiri-Bradley with Ala-Laurila and would have had a reasonable expectation of success.**

A POSITA would have been motivated to combine Nakhjiri-Bradley’s ECDH-based secure profile delivery to UICCs (Ex-1005, 5:25–6:2; Ex-1006 ¶29) with Ala-Laurila’s disclosure to transmit the IMSI-based identifier to the network encrypted under a Diffie-Hellman-derived symmetric key for authentication (Ex-1013 ¶26), to yield a unified, predictable eUICC flow: (i) securely provision profile data (including IMSI and K) to the eUICC; (ii) authenticate by encrypting the IMSI with a Diffie-Hellman-derived symmetric key toward network

authentication servers (PAC/GAGW). These complementary steps (provisioning and authenticating) use the same ECDH mechanism for two adjacent phases of the lifecycle. Ex-1002 ¶156. The references' teachings are analogous and amenable to combination without change in principle of operation. Ex-1005, 2:19–24, 5:25–6:2; Ex-1006 ¶¶2, 29–31; Ex-1013 ¶¶22–26, 28; Ex-1002 ¶156.

Nakhjiri-Bradley teaches steps 1(a)-1(d). Ala-Laurila further teaches authenticating by sending IMSI to a network server and specifically addresses the security problem of sending IMSI in the clear. In Ala-Laurila's method, the mobile terminal (MT) obtains the IMSI from the SIM and then encrypts it before sending it to the network public access controller (PAC), which is in communication with the authentication server (GAGW), as shown in the excerpted figure below. Ex-1013, Fig. 2.



MT sends an authentication request to PAC that “comprises the IMSI identifier” and that “is preferably sent *in ciphered form* to the PAC *using the Diffie-Hellman algorithm.*” Ex-1013 ¶26; Ex-1002 ¶¶157-158.

2. Independent Claim 1

a. Elements 1[pre]; 1[a]-[d]:

Nakhjiri in view of Bradley and Ala-Laurila (“Nakhjiri-Bradley-Ala-Laurila”) teaches Elements 1[pre] and 1[a]-[d] for the same reasons discussed above for Ground 1. Ex-1002 ¶159.

b. Element 1(e): generating, by the eUICC, a second module public key and a corresponding second module private key;

Nakhjiri-Bradley-Ala-Laurila teaches Element 1(e). Ex-1002 ¶160.

Ala-Laurila’s authentication flow requires a Diffie-Hellman exchange with the PAC/GAGW, i.e., deriving a symmetric key from a keypair exchange between the MT and a second network authentication server. Ex-1013 ¶¶22–26. 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”). Ex-1002 ¶161.

Specifically, Ala-Laurila teaches that the MT sends “the authentication starting request (MT_PAC_AUTHSTART_REQ)” including an NAI, which “comprises the IMSI identifier obtained from the identity module SIM.” Ex-1013

¶26. The authentication request “is preferably sent *in ciphered form to the PAC using the Diffie-Hellman algorithm.*” Ex-1013 ¶26. The PAC communicates with the server GAGW for authentication. Ex-1013 ¶¶22-23. Ala-Laurila does not describe the Diffie-Hellman exchange in detail, but a POSITA would have understood, based at least on Nakhjiri, that the Diffie-Hellman process includes mutual derivation of a shared symmetric key based on an exchange of private/public keys associated with the entities communicating with one another. Ex-1002 ¶162. Specifically, the mobile device (UICC) sends the module public key to the authentication server, and uses its own module private key (and the authentication server public key) to generate the Diffie-Hellman symmetric key. Ex-1002 ¶162. Thus, in the Nakhjiri-Bradley-Ala-Laurila combination, Nakhjiri’s process where “the UICC ... generate[s] its own ECC private key (MNO_ECC_PVKDEV)” and “then creates the PEK to perform decryption ... us[ing] the device ECC private key for this particular MNO (MNO_ECC_PVKDEV) and the MNO ECC public key (MNO_ECC_PLKOP) to perform a local ECDH key agreement process,” would be modified 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. Ex-1002 ¶162.

- c. Element 1(f): sending, to a second server associated with the wireless network, the second module public key;**

Nakhjiri-Bradley-Ala-Laurila teaches Element 1(f) for the reasons described in the previous limitation. Ex-1002 ¶163.

Ala-Laurila teaches using a Diffie-Hellman key exchange process to secure the communications between the MT and the PAC/GAGW, which is “an entity in the mobile network GSMNW offering authentication services of mobile subscribers to the WLAN networks.” Ex-1013 ¶¶22-26. The PAC and GAGW performs authentication and corresponds to the recited “second server.” Ex-1002 ¶164. 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), as taught by Ala-Laurila, instead of the MNO provisioning server, using the same ECDH process. Ex-1002 ¶164.

- d. Element 1(g): generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;**

Nakhjiri-Bradley-Ala-Laurila teaches Element 1(g) for the reasons described for claim Elements 1(e)-1(f). Ex-1002 ¶165. A POSITA would have used Nakhjiri’s ECDH procedure to create the symmetric key Ala-Laurila uses to encrypt IMSI. Ex-1002 ¶165; Ex-1013 ¶¶22-23, 25-26. Thus, in the Nakhjiri-Bradley-Ala-Laurila combination, Nakhjiri’s process would be modified to generate a symmetric key

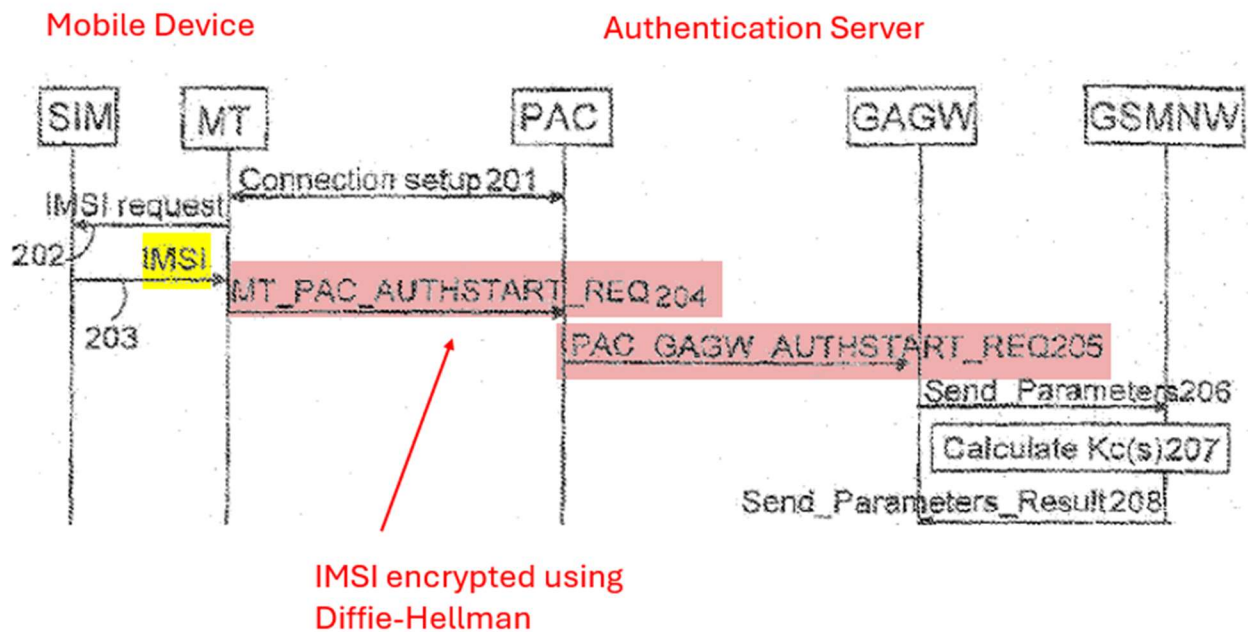
using a second ECDH key exchange with the second module private key for mutual authentication with an authentication server, as taught by Ala-Laurila, (instead of the MNO provisioning server, as taught by Nakhjiri), using the same elliptic curve Diffie-Hellman process. Ex-1002 ¶165. Using the ECC parameters (curve/base point G) (Ex-1005, 4:51–56) satisfies “cryptographic parameters”; the ECDH yields the symmetric key used for subsequent encryption. Ex-1013 ¶26; Ex-1002 ¶165.

- e. **Element 1(h): generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity; and**

Nakhjiri-Bradley-Ala-Laurila teaches Element 1(h). Ex-1002 ¶166.

As shown in Figure 2 below, Ala-Laurila teaches that the MT first “requests 202 (IMSI request) the identity module SIM for the IMSI identifier and the SIM returns 203 the IMSI identifier.” Ex-1013 ¶26. The MT then sends “the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a Network Access Identifier NAI.” Ex-1013 ¶26. “The NAI comprises the IMSI identifier obtained from the identity module SIM.” Ex-1013 ¶26. The request “is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm.” Ex-1013 ¶26, Fig. 2. Ala-Laurila thus generates the encrypted IMSI (i.e., module identity) using a symmetric key derived during the ECDH process. As explained for claim Elements 1(e)-1(g), Nakhjiri already describes the ECDH key exchange process with a provisioning server, including the process of generating a

symmetric key. A POSITA would have understood that the same process would be used to derive a Diffie-Hellman key for sending the IMSI to the authentication server, as taught by Ala-Laurila. Ex-1002 ¶167. In the Nakhjiri-Bradley-Ala-Laurila combination, the IMSI sent from the MT to the PAC (and GAGW) is encrypted using the symmetric key derived using the ECDH process described above, as taught by Ala-Laurila and Nakhjiri. Ex-1013, Fig. 2; Ex-1002 ¶167.



f. Element 1(i): sending, to the second server, the module encrypted data.

Nakhjiri-Bradley-Ala-Laurila teaches Element 1(i) for the reasons described in the previous section. Ex-1002 ¶168. Specifically, Ala-Laurila teaches sending the IMSI-containing NAI “in ciphered form ... using the Diffie–Hellman algorithm” to the PAC. Ex-1013 ¶26 (steps 202–204, Fig. 2). That is the claimed

module-encrypted data comprising the module identity sent to the second server. Ex-1002 ¶¶168-169.

Thus, Nakhjiri-Bradley-Ala-Laurila renders obvious Claim 1.

3. Dependent Claims 2-4, 7, 9-14, and 16-20

a. Claims 2-4, 7, 9, 11-12, 14, and 17-20.

Claims 2-4, 7, 9, 11-12, 14, and 17-20 are invalid for the same reasons taught by Nakhjiri and Bradley in Ground 1, above. Ex-1002 ¶170.

b. Claim 10: The method of claim 1, wherein steps g) and h) occur before step f).

Nakhjiri-Bradley-Ala-Laurila teaches Claim 10. Ex-1002 ¶171.

Claim 10 requires that generating the symmetric key (g) and generating module encrypted data including IMSI (h) occurs before sending the second module public key to the second server (f). ECDH and symmetric encryption steps can be computed before or in parallel with sharing the public key; precomputation and ordering are design choices well within POSITA's skill. Ex-1002 ¶172. For example, SEC1 contemplates ephemeral ECDH keys and precomputation. Ex-1011, §§3.3, 3.6 (31–33, 56–57); *see also* Ex-1014, 12 (showing ephemeral key generation); Ex-1002 ¶172. Applying that to authentication yields steps (g) and (h) before sending (f).

Moreover, Nakhjiri teaches an analogous example: “in connection with FIG. 3, the UICC can obtain the MNO ECC public key (MNO_ECC_PKLOP) from the

MNO *along with the encrypted data...*” Ex-1005, 6:2-5. In other words, the MNO in this example has already generated the symmetric key and encrypted the data package before the MNO public key is sent because the MNO public key is sent *along with* the encrypted data package. Ex-1002 ¶173. Thus, it would have been simple design choice for the mobile device to perform steps (g) and (h) immediately after step (e) whereby the UICC generates the symmetric key and encrypts the module identity with it before it sends the second module public key to the server. Ex-1002 ¶173.

- c. **Claim 13: The method of claim 1, further comprising:
j) receiving, from the wireless network, a random number (RAND) and generating a response (RES) using the RAND and the key K.**

Nakhjiri-Bradley-Ala-Laurila teaches Claim 13. Ex-1002 ¶¶174-175.

Ala-Laurila teaches that the “authentication center AuC forms 207 (Calculate Kc(s)) one or more GSM triplets (RAND, SRES, Kc) in a known manner using the secret key Ki according to the IMSI identifier.” Ex-1013 ¶28. The “GSM triplet comprises a challenge code, i.e. a random number, RAND, an authentication response SRES formed on the basis of the RAND and a secret key Ki using an algorithm A3, and a first ciphering key Kc formed on the basis of the RAND and the secret key Ki using an algorithm A8.” Ex-1013 ¶28. Ala-Laurila teaches that “[t]he HLR sends the triplet ... to the GAGW 208 (Send_Parameters_Result) 0028.” Ex-

1013 ¶28. The MT then “feeds 212 the challenge code/s RAND into the identity module SIM,” which “calculates 213 (Calculate Kc(s)) at least one first ciphering key Kc according to the mobile network GSMNW and an authentication response (responses) SRES in a manner that corresponds with the one used in the authentication center AuC and transmits 214 these to the other parts of the terminal MT (preferably to the control means CM carrying out authentication and the calculation of the second ciphering key K).” Ex-1013 ¶31.

- d. Claim 16: The method of claim 1, wherein the first server, the second server, and the wireless network are associated with a mobile network operator.**

Nakhjiri-Bradley-Ala-Laurila teaches Claim 16. Ex-1002 ¶176.

Ground 1 as applied to Claim 16 explains that the first server and wireless network of Nakhjiri are associated with a mobile network operator. *See* Section XII.A.3.k. As explained with respect to claim Element 1(f), Ala-Laurila teaches a second server (PAC and/or GAGW) associated with a mobile network operator for authentication, which is the client’s counterpart in the second ECDH exchange in the Nakhjiri-Bradley-Ala-Laurila combination. Ex-1002 ¶177. In the Nakhjiri-Bradley-Ala-Laurila combination, one of Nakhjiri’s nodes that is associated with the mobile network operator would include the functions of Ala-Laurila’s PAC and/or GAGW authentication server, which acts the client’s counterpart in the second ECDH exchange. Ex-1002 ¶177.

- C. Grounds 3-4: Claims 5-6 are obvious over Nakhjiri, Bradley, Jeong, and X9.63-Overview; or Nakhjiri, Bradley, Ala-Laurila, and X9.63-Overview**
- 1. A POSITA would have been motivated to combine Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila with X9.63-Overview and would have had a reasonable expectation of success.**

All of these references relate to secure methods of provisioning and/or authenticating a mobile device with a wireless network, and each focuses on well-known and complementary weaknesses in that process. *See* Sections XII.A.1 and XII.B.1; Ex-1002 ¶178.

While Nakhjiri refers generally to using a hash function including, for example, a “standard MAC (Message Authentication Code) function such as HMAC-SHA1, HMAC-SHA256, AES-CMAC” for the key generation function (KGF)¹⁴ (Ex-1005, 4:60-63), it was commonly known to apply one of several specific hash-based key derivation functions (KDFs) to a Diffie-Hellman shared secret in order to generate a cryptographically sound symmetric key with desirable properties. Ex-1002 ¶179. It would have been an obvious design choice for Nakhjiri’s shared profile encryption key (PEK) in the first ECDH exchange with the first server to have been derived by applying the ANSI standard X-9.63 KDF to the

¹⁴ While Nakhjiri uses the term “KGF,” a POSITA would have understood that a key generation function (KGF) is interchangeable with the recited “key derivation function” (KDF) of Claims 5-6, which is a known term of art. Ex-1002 ¶179 n.12.

Diffie-Hellman shared secret because this was a well-known concept by 2013, and X-9.63 was developed specifically for SIM environments such as those taught by Nakhjiri. Ex-1002 ¶179. For example, the X9.63 overview, published in 2000, notes that ANSI X9.63 is a “key derivation function” that “derives keying material from shared secret value” and is a “simple hash function.” Ex-1014, 9. Further, it enables “specific key agreement and key transport schemes using elliptic curve cryptography” (*id.* 3), and uses an encryption scheme “based on elliptic curve Diffie-Hellman.” *Id.* 9.

Similarly, Jeong’s second ECDH exchange / Ala-Laurila’s Diffie-Hellman exchange with the second server uses the same type of public/private key exchange described in Nakhjiri, and it would similarly have been obvious to apply ANSI X-9.63 to properly randomize Jeong’s ECDH SSK_{MS-HN} key or Ala-Laurila’s derived key for communicating with PAC. Specifically, a POSITA would have been motivated to apply the well-known X9.63 key derivation function to derive the ECDH keys of Jeong / Ala-Laurila with good cryptographic properties according to a standardized algorithm. Ex-1002 ¶180.

A POSITA would have had a reasonable expectation of success in combining the teachings of Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila with X9.63-Overview. Ex-1002 ¶181. All describe methods for securing wireless communications using similar key agreement mechanisms and they address

complementary security issues resulting in a more robust system for network authentication. *See* Sections XII.A.1 and XII.B.1. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations. Ex-1002 ¶181.

2. Dependent Claims 5-6

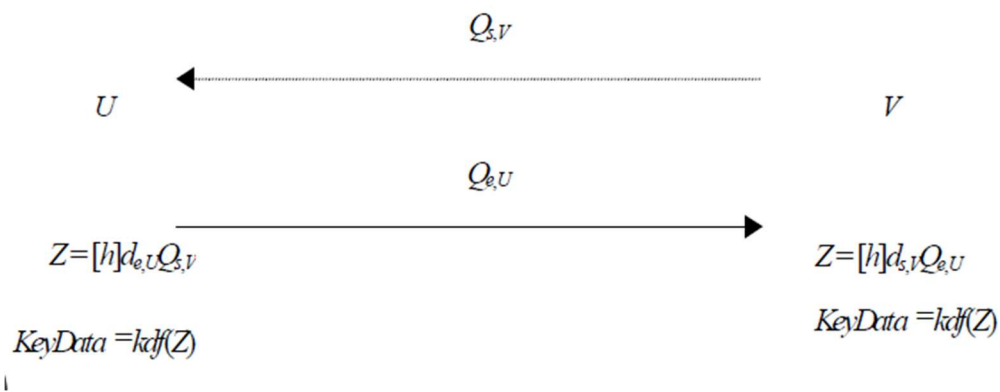
- a. **Claim 5: The method of claim 1, further comprising in step c) deriving the shared secret key using an American National Standards Institute (ANSI) standard X-9.63 key derivation function.**

Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila in view of X9.63-Overview teaches Claim 5. Ex-1002 ¶182.

As explained in Ground 1 applied to Element 1(c), Nakhjiri teaches that a key agreement exchange takes place “between the MNO SM-DP and each UICC” to establish “a profile encryption key (PEK) using ECC.” Ex-1005, 5:25-27. Nakhjiri further teaches that “[o]ne example of a key exchange algorithm that may be employed is an Elliptic Curve Diffie-Hellman exchange (ECDH) algorithm where both the UICC and the MNO end up with exactly the same Shared ECDH secret.” Ex-1005, 5:27-31. Moreover, Nakhjiri teaches that the key generation function (KGF) used “may be proprietary or a well-established function.” Ex-1005, 4:60-61. For instance, “the KGF can be a standard MAC (Message Authentication Code) function such as HMAC-SHA1, HMAC-SHA256, AES-CMAC, and so on.” Ex-

1005, 4:61-63. A POSITA would have understood that ANSI X-9.63 is a well-known KDF that would have been obvious to try. Ex-1002 ¶183. X9.63-Overview also provides an example of applying the X9.63 KDF to a Diffie-Hellman (DH) exchange that matches with that disclosed in Nakhjiri:

ANSI X9.63 - 1-Pass DH



Ex-1014, 12 (showing entities U and V exchanging public keys Q_V and Q_U , calculating shared secret Z , and then creating a symmetric key by applying X9.63 KDF to shared secret Z).

A POSITA would have looked to X9.63-Overview for additional implementation details for Nakhjiri's method, given that Nakhjiri teaches that elliptic curve Diffie Hellman is an example of a cryptographic algorithm that may be utilized for Nakhjiri's method. Ex-1005, 4:28-37; Ex-1014, 3, 9, 12; Ex-1002 ¶184.

- b. Claim 6: The method of claim 1, further comprising in step g) deriving the symmetric key using an ANSI standard X-9.63 key derivation function.**

Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila with X9.63-Overview teaches Claim 6. Ex-1002 ¶185.

As explained in Grounds 1 and 2 for Element 1(g), Jeong and Ala-Laurila teach deriving a symmetric key using a second ECDH exchange with a second (authentication) server. Ex-1002 ¶186. Like Nakhjiri's first ECDH exchange, Jeong's and Ala-Laurila's second ECDH exchange also benefits from the application of X9.63-Overview's well known X9.63 key derivation function, which serves to randomize the Diffie-Hellman shared secret and create a symmetric key with good cryptographic properties according to a standardized algorithm. Ex-1014, 3, 9, 12; Ex-1002 ¶186.

- D. Grounds 5-6: Claim 8 is obvious over Nakhjiri, Bradley, Jeong, and Pierce or Nakhjiri, Bradley, Ala-Laurila, and Pierce.**

1. Dependent Claim 8

- a. Claim 8: The method of claim 1, further comprising in step e), generating, by the eUICC, the second module public key and the second module private key using a random number generator and input from a sensor.**

Pierce teaches a method for enabling "the automatic generation of strong cryptographic keys by an embedded processing device at the time of manufacturing, before the product is released for distribution to end users ... by supplying the

embedded device with entropy data that it uses to seed a pseudo random number generator (PRNG) that is used to generate the keys.” Ex-1009 ¶19; *see also id.* ¶38 (“The entropy data is used as a seed value for the PRNG, which will yield a nearly random number suitable for use in generating strong cryptographic keys ... including asymmetric public-private key pairs.”). Pierce further teaches that the “entropy data can be obtained by the embedded device from any of a number of sources, including those both internal and external to the manufactured product.” Ex-1009 ¶19. Entropy data can be measured, for example, “from a sensor” and “GPS satellite time data (normally used for determining location coordinates) that are received from the GPS module.” Ex-1009 ¶36; Ex-1002 ¶187.

A POSITA would have been motivated to generate, using Jeong’s USIM/MS or Ala-Laurila’s SIM/MT, the second module public key and second module private key using input from a sensor because, as taught by Pierce, “[t]he generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered.” Ex-1009 ¶4. Moreover, as Pierce teaches, using entropy data such as sensor “protects against key compromise” (Ex-1009 ¶14) because the data is “transient and not later discernible” or “internal to the manufactured product and not readily discernible without possession and analysis of the product.” Ex-1009 ¶35. Specifically, Pierce teaches seeding a PRNG with entropy from sensors or GPS time to generate ‘strong cryptographic keys ... including asymmetric public-private

key pairs.’ Ex-1009 ¶¶19, 36, 38. A POSITA would use such entropy in the system when generating the second ECDH keypair at authentication to harden against key compromise. Ex-1002 ¶188.

A POSITA would have had a reasonable expectation of success in combining Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila with Pierce. Ex-1002 ¶189. All describe methods for securing wireless communications using authentication and key agreement mechanisms. *See* Sections XII.A.1 and XII.B.1; Ex-1009, Abstract. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations. Ex-1002 ¶189.

E. Grounds 7-8: Claim 15 is obvious over Nakhjiri, Bradley, Jeong, and GlobalPlatform or Nakhjiri, Bradley, Ala-Laurila, and GlobalPlatform.

1. Dependent Claim 15

- a. Claim 15: The method of claim 1, further comprising (i) in step a), storing a server name for the first server and a port number in a nonvolatile memory of the eUICC, and (ii) before step b) sending the first module public key to the first server.**

GlobalPlatform teaches that the connection parameters TLV “embed all the needed parameters to establish a point to point TCP connection between the Administration Agent and the Remote administration server.” Ex-1010, 24. As

shown in Table 3-4 below, for example, the TLV security domain administration session parameters include an “Administration Host parameter.” Ex-1010, 24; *see also id.* 26 (“This TLV defines the ‘Host’ header value to be used by the Security Domain when sending a POST request.”). A POSITA would have understood that a port number would also be needed to establish a point to point TCP connection and thus this would have also been included in the saved parameters. Ex-1002 ¶190. GlobalPlatform’s RAM over HTTP defines TLV session parameters that “embed all the needed parameters to establish a point-to-point TCP connection,” including an Administration Host (Table 3-4) and associated connection headers. Ex-1010, 24–26. A POSITA would also store the port number with the host for TCP connection setup, and would store these in nonvolatile eUICC memory before initial contact to send the first module public key. A POSITA would have also understood that it was standard procedure that the eUICC would save the server name and port number before sending the first module public key to the first server. Ex-1002 ¶190.

Table 3-4: TLV Security Domain Administration Session Parameters

Tag	Length	Name		Presence			
'85'	1-n	Security Domain Administration Session Parameters		Optional			
		Tag	Length		Name		
		'84'	1-n		Connection parameters tag		
		'85'	1-n		Security parameters value		
		'86'	1-n		Retry policy parameters value		
		'89'	1-n		HTTP POST parameters value		
					Tag	Length	Name
					'8A'	1-n	Administration Host parameter
					'8B'	1-n	Agent ID parameter
		'8C'	1-n	Administration URI parameter			

GlobalPlatform states that its specification is “intended primarily for card manufacturers and application developers developing GlobalPlatform implementations” and “[i]t is assumed that the reader is familiar with smart cards and smart card production.” Ex-1010, 5. A POSITA would have looked to GlobalPlatform for additional implementation details for the Nakhjiri-Bradley-based combinations because they all relate to smartcard technologies (Ex-1005, 1:18-30; Ex-1006 ¶¶2-6) and Bradley specifically states that “[t]he integration of the ETSI framework and the Application management framework of GlobalPlatform is standardized in the UICC configuration.” Ex-1006 ¶8. Nakhjiri also notes that “these same techniques [for provisioning a UICC profile] may be used by a bank that provisions smart cards for mobile banking.” Ex-1005, 2:58-61. A POSITA would thus have been motivated to apply GlobalPlatform’s TLV security domain administration session parameters, which teach to store a server name and port number in the eUICC before sending the module’s public key to the server, to Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila because it is a well-known smartcard specification. Ex-1002 ¶191. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations. Ex-1002 ¶¶191-194.

XIII. CONCLUSION

Petitioner requests institution of IPR for Claims 1-20 of the '869 Patent based on each of the grounds in this Petition.

Respectfully Submitted,

/s/ William M. Fink

William M. Fink (Reg. No. 72,332)

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Petitioner certifies that this petition includes 13,859 words, as measured by Microsoft Word, exclusive of the table of contents, mandatory notices under §42.8, certificates of service, word count, and exhibits.

CERTIFICATE OF SERVICE (37 C.F.R. §42.6(e)(1))

The undersigned hereby certifies that the above document was served on November 20, 2025, by filing this document through the Patent Trial and Appeal Board P-TACTS System, as well as delivering a copy via express mail upon the following attorneys of record for the Patent Owner:

Amster, Rothstein, & Ebenstein LLP
405 Lexington Avenue
Floor 48
New York, NY 10174

A courtesy copy was sent to the below counsel via electronic mail:

Demetrios Anaipakos
Amir H. Alavi
Michael McBride
Steven Jugle
C. Ryan Pinckney
Connie Flores Jones
ALAVI & ANAIPAKOS PLLC
609 Main Street, Suite 3200
Houston, Texas 77002
Telephone: (713) 751-2362
Facsimile: (713) 751-2341
danaipakos@aatriallaw.com
aalavi@aatriallaw.com
mmcbride@aatriallaw.com
sjugle@aatriallaw.com
rpinckney@aatriallaw.com
cfloresjones@aatriallaw.com

Michael F. Heim
Eric J. Enger
R. Allan Bullwinkel
William B. Collier, Jr.
HEIM, PAYNE & CHORUSH, LLP
609 Main St. Suite 3200
Houston, Texas 77002
Telephone: (713) 221-2000
Facsimile: (713) 221-2021
mheim@hpcllp.com
eenger@hpcllp.com
abullwinkel@hpcllp.com
wcollier@hpcllp.com

Andrea L. Fair
Claire A. Henry
MILLER FAIR HENRY PLLC
1507 Bill Owens Parkway
Longview, Texas 75604
(903) 757-6400 (telephone)
andrea@millerfairhenry.com
claire@millerfairhenry.com

Dated: November 20, 2025

Respectfully submitted,

/s/ William M. Fink

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

Attorney for Petitioner