

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

**DECLARATION OF SUNDEEP RANGAN IN SUPPORT OF PETITION
FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 12,166,869**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. BACKGROUND AND QUALIFICATIONS	2
III. INFORMATION CONSIDERED	4
IV. RELEVANT LEGAL STANDARDS	5
A. Claim Interpretation	5
B. Perspective of One of Ordinary Skill in the Art.....	5
C. Obviousness.....	6
V. LEVEL OF ORDINARY SKILL IN THE ART	8
VI. SUMMARY OF MY OPINIONS	9
VII. TECHNOLOGICAL BACKGROUND	10
A. Mobile device with an eUICC performing a method to securely communicate with a wireless network	10
B. Storing a first module private key, a corresponding first module public key, and a network public key in the eUICC	12
C. Receiving from a first server an encrypted profile for the eUICC comprising cryptographic parameters, module identity, and key K	14
D. Generating a shared secret key using a first ECDH key exchange with the first module private key and the network public key.....	18
E. Decrypting at least a portion of the encrypted profile for the eUICC with the shared secret key	20
F. Generating, by the eUICC, a second module public key and a corresponding second module private key	21
G. Sending the second module public key to a second server	24
H. Generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters	26
I. Generating with the symmetric key module encrypted data comprising the module identity	28
J. Sending the module encrypted data to the second server	31

TABLE OF CONTENTS
(continued)

	Page
VIII. THE '869 PATENT AND ITS FILE HISTORY	33
IX. CLAIM CONSTRUCTION	37
X. OVERVIEW OF THE APPLIED PRIOR ART REFERENCES	37
A. Nakhjiri (Ex-1005)	38
B. Bradley (Ex-1006).....	39
C. Jeong (Ex-1007)	40
D. Ala-Laurila (Ex-1013).....	42
E. ANSI X9.63-Overview (Ex-1014).....	44
F. Pierce (Ex-1009).....	46
G. GlobalPlatform (Ex-1010).....	47
XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS	48
A. Ground 1: Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri, Bradley, and Jeong.....	48
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.....	48
2. Independent Claim 1	52
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:.....	52
b. Element 1(a): storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key;.....	53
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;	60

TABLE OF CONTENTS
(continued)

	Page
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;	65
e. Element 1(d): decrypting, with the shared secret key, at least a portion of the encrypted profile for the eUICC;	68
f. Element 1(e): generating, by the eUICC, a second module public key and a corresponding second module private key;	68
g. Element 1(f): sending, to a second server associated with the wireless network, the second module public key;	72
h. Element 1(g): generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;	73
i. Element 1(h): generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity; and	74
j. Element 1(i): sending, to the second server, the module encrypted data.	76
3. Dependent Claims 2-4, 7, 9-14, and 16-20	77
a. Claim 2: The method of claim 1, wherein the module identity comprises an international mobile subscriber identity (IMSI).	77
b. Claim 3: The method of claim 1, wherein the module identity comprises a permanent identifier for the mobile device.	77
c. Claim 4: The method of claim 1, wherein the cryptographic parameters comprise an identifier for a set of cryptographic parameters.	79

TABLE OF CONTENTS
(continued)

	Page
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.	80
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.	81
f. Claim 10: The method of claim 1, wherein steps g) and h) occur before step f).	82
g. Claim 11: The method of claim 1, wherein the network public key is associated with an eUICC subscription manager.	83
h. Claim 12: The method of claim 11, wherein the eUICC subscription manager comprises the first server.	83
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.	85
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.	86
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.	88
l. Claim 17: The method of claim 1, wherein the eUICC comprises a processor, firmware, and protected memory.	89

TABLE OF CONTENTS
(continued)

	Page
m. Claim 18: The method of claim 1, wherein the cryptographic parameters include a base point G for an elliptic curve.....	90
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.	91
o. Claim 20: The method of claim 1, wherein the eUICC comprises a package soldered to a circuit board of the mobile device.	92
B. Ground 2: Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri in view of Bradley and Ala-Laurila	92
1. A POSITA would have been motivated to combine Nakhjiri-Bradley with Ala-Laurila and would have had a reasonable expectation of success.....	92
2. Independent Claim 1	94
a. Elements 1[pre]; 1[a]-[d]:.....	94
b. Element 1(e): generating, by the eUICC, a second module public key and a corresponding second module private key;	95
c. Element 1(f): sending, to a second server associated with the wireless network, the second module public key;	96
d. Element 1(g): generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;.....	97
e. Element 1(h): generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity; and	98
f. Element 1(i): sending, to the second server, the module encrypted data.....	99
3. Dependent Claims 2-4, 7, 9-14, and 16-20	100

TABLE OF CONTENTS
(continued)

	Page
a. Claims 2-4, 7, 9, 11-12, 14, and 17-20	100
b. Claim 10: The method of claim 1, wherein steps g) and h) occur before step f).....	100
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.....	101
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.	102
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	102
1. A POSITA would have been motivated to combine Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila’s teachings with X9.63-Overview’s teachings and would have had a reasonable expectation of success.	102
2. Dependent Claims 5-6.....	104
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.	105
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.....	106
D. Grounds 5-6: Claim 8 is obvious over Nakhjiri, Bradley, Jeong, and Pierce or Nakhjiri, Bradley, Ala-Laurila, and Pierce.....	107
1. Dependent Claim 8.....	107

TABLE OF CONTENTS
(continued)

	Page
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.	107
E. Grounds 7-8: Claim 15 is obvious over Nakhjiri, Bradley, Jeong, and GlobalPlatform or Nakhjiri, Bradley, Ala-Laurila, and GlobalPlatform.	109
1. Dependent Claim 15	109
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.....	109
XII. CONCLUSION.....	111

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-1030	INTENTIONALLY LEFT BLANK

Ex. No.	Description
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

1. My name is Sundeeep Rangan. I am presently a professor in the Department of Electrical and Computer Engineering at New York University, Brooklyn, New York. My residence is in Jersey City, New Jersey, and my place of business is in Brooklyn, New York. I am over the age of eighteen, and I am a citizen of the United States.

2. I have been retained to provide this Declaration by Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (“Petitioner”) as an independent expert consultant in this inter partes review (“IPR”) proceeding before the United States Patent and Trademark Office (“PTO”).

3. I have been asked by Petitioner Counsel (“Counsel”) to consider whether certain references disclose, teach and/or suggest the features recited in Claims 1-20 of U.S. Patent No. 12,166,869 (“the ’869 Patent”) (Ex-1001), which I understand is currently assigned to currently assigned to Network-1 Technologies, Inc. (“PO”). My opinions and the bases for my opinions are set forth below.

4. I am being compensated at my ordinary and customary consulting rate for my work, which is \$750 per hour. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other direct financial interest in this proceeding.

II. BACKGROUND AND QUALIFICATIONS

5. I received a B.A.Sc. in Electrical Engineering from the University of Waterloo in Waterloo, Canada in 1992. I then received an M.S. in 1995 and a Ph.D. in 1997, both in Electrical Engineering, from the University of California at Berkeley, California. My doctoral thesis was entitled, “Robust Identification and Control of Multimodal Systems with Applications to Semiconductor Manufacturing.”

6. I am currently a tenured professor in the Department of Electrical and Computer Engineering at New York University in Brooklyn, New York. I am also Associate Director of NYU WIRELESS. I have held both positions since 2018 and have been on the faculty at New York University since 2010.

7. Prior to becoming a full professor, I was an Associate Professor of Electrical and Computer Engineering at New York University from 2010 to 2018 and was Director of NYU WIRELESS from 2016 to 2018. At NYU, my focus is in wireless communications, signal processing, and information theory.

8. From 2006 to 2010, I was Senior Director of Engineering at Qualcomm Technologies in Bridgewater, New Jersey, where I supervised the advanced research and development group responsible for cellular communication products. I also led engineering teams in high performance base station ASICs for both the 3GPP Long-Term Evolution (LTE) and earlier 3GPP2 Universal Mobile Broadband (UMB)

systems. I supervised development of PHY and MAC algorithms, ASIC simulation and verification methodologies, and MAC-layer software. I also led feasibility studies, architectural planning, and early development for a 4G femtocell ASIC. The system-on-chip (SoC) was a multimode device supporting 3G and 4G cellular standards, peak rates in excess of 300 Mbps DL and 120 Mbps UL, and contained several processors and DSPs.

9. During 2000 to 2006, I was Director of Flarion Technologies in Bedminster, New Jersey, which was a company I co-founded to commercialize Flash-OFDM, one of the first cellular OFDM data systems and a precursor to later 4G standards including WiMAX and LTE. The company grew to over 150 employees with trials with tier 1 carriers worldwide. Flarion was sold to Qualcomm for \$800 million in 2006.

10. Before that, I was a Member of Technical Staff at Bell Labs, Lucent Technologies from 1998 to 2000 and was a Postdoctoral Research Fellow at the University of Michigan at Ann Arbor, Michigan from 1997 to 1998.

11. I have authored or co-authored dozens of articles in refereed journals and approximately 100 conference papers. I am also a named inventor on 59 issued U.S. patents. A list of my publications during the last ten years is included in my CV, which is attached as Ex-1003.

12. I have previously offered testimony as an expert witness. A list of my prior engagements for the last four years in which I testified as an expert at trial or by deposition is also included in my CV.

13. Based on my background and experience, as set forth more fully in my CV, I am familiar with the state of the art in the field of wireless communications in the 2013 time frame. I am a technical expert in the fields relating to the '869 Patent and other related fields, and I remain an active researcher in these fields.

14. Based on my professional experience, I believe I am qualified to testify as an expert on matters related to the '869 Patent.

III. INFORMATION CONSIDERED

15. In preparation for my Declaration, I have considered the materials I discuss in my Declaration, including, for example, the '869 Patent, the references cited by the '869 Patent, the prosecution history of the '869 Patent (including the references cited therein), various background articles and materials referenced in my Declaration, and the prior art references I identify in my Declaration. In addition, my opinions are further based on my education, training, experience, and knowledge in the relevant field.

IV. RELEVANT LEGAL STANDARDS

16. I am not an attorney and offer no legal opinions. For the purposes of my Declaration, I have been informed about certain aspects of the law that are relevant to my analysis, as summarized below.

A. Claim Interpretation

17. I have been informed and understand that in an IPR proceeding, claims are to be interpreted according to the *Phillips* claim construction standard. I understand that under this standard, the meaning of claim terms is considered from the viewpoint of a hypothetical “person of ordinary skill in the art” (“POSITA”) at the time of the alleged invention. I have been informed and understand that claim construction is a matter of law and that the final claim constructions for this proceeding will be determined by the Patent Trial and Appeal Board (“PTAB”).

18. I provide my opinions regarding terms that may require explicit construction to resolve the grounds I present in my Declaration in Section IX.

B. Perspective of One of Ordinary Skill in the Art

19. I have been informed and understand that a patent is to be understood from the perspective of a hypothetical POSITA. Such an individual is considered to possess normal skills and knowledge in a particular technical field (as opposed to being a genius). I understand that in considering what the claims of a patent require, what was known prior to that patent, what a prior art reference discloses, and whether an invention is obvious or not, one must use the perspective of such a POSITA.

C. Obviousness

20. I have been informed and understand that a patent claim is obvious under 35 U.S.C. §103, and therefore invalid, if the claimed subject matter, as a whole, would have been obvious to a POSITA as of the priority date of the patent based on one or more prior art references and/or the knowledge of a POSITA.

21. I understand that an obviousness analysis must consider (1) the scope and content of the prior art, (2) the differences between the claims and the prior art, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations, if any, of non-obviousness (such as unexpected results, commercial success, long-felt but unmet need, failure of others, copying by others, and skepticism of experts).

22. I understand that a prior art reference may be combined with other references to disclose each element of the invention under 35 U.S.C. §103. I understand that a reference may also be combined with the knowledge of a POSITA, and that this knowledge may be used to combine multiple references. I further understand that a POSITA is presumed to know the relevant prior art. I understand that the obviousness analysis may take into account the inferences and creative steps that a POSITA would employ.

23. In determining whether a prior art reference would have been combined with other prior art or other information known to a POSITA, I understand that the following principles may be considered:

- a. whether the references to be combined involve non-analogous art;
- b. whether the references to be combined are in different fields of endeavor than the alleged invention in the Patent;
- c. whether the references to be combined are reasonably pertinent to the problems to which the inventions of the Patent are directed;
- d. whether the combination is of familiar elements according to known methods that yields predictable results;
- e. whether a combination involves the substitution of one known element for another that yields predictable results;
- f. whether the combination involves the use of a known technique to improve similar items or methods in the same way that yields predictable results;
- g. whether the combination involves the application of a known technique to a prior art reference that is ready for improvement, to yield predictable results;
- h. whether the combination is “obvious to try”;
- i. whether the combination involves the known work in one field of endeavor prompting variations of it for use in either the same field or a different one based on design incentives or other market forces, where the variations are predictable to a POSITA;

- j. whether there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention;
 - k. whether the combination requires modifications that render the prior art unsatisfactory for its intended use;
 - l. whether the combination requires modifications that change the principle of operation of the reference;
 - m. whether the combination is reasonably expected to be a success; and
- whether the combination possesses the requisite degree of predictability at the time the invention was made.

24. I understand that in determining whether a combination of prior art references renders a claim obvious, it is helpful to consider whether there is some teaching, suggestion, or motivation to combine the references and a reasonable expectation of success in doing so. I understand, however, that a teaching, suggestion, or motivation to combine is not required.

V. LEVEL OF ORDINARY SKILL IN THE ART

25. I am familiar with the level of ordinary skill in the art with respect to the '869 Patent around its filing date. Based on my experience working, teaching, and conducting research in the relevant field, and based on my review of the '869

Patent specification, claims, file history, and prior art, I believe one of ordinary skill in the art around the time of the alleged invention of the '869 Patent 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, with additional education substituting for experience and vice versa.

26. In determining the level of ordinary skill in the art, I considered, for example, the type of problems encountered in the art, prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field.

27. I met or exceeded the knowledge and experience that a POSITA would have had in 2002. I have extensive experience with wireless communications including the provisioning of mobile devices and the network authentication and access processes.

VI. SUMMARY OF MY OPINIONS

28. As I explain below in detail in my Declaration, it is my opinion that Claims 1-20 of the '869 Patent would have been obvious under 35 U.S.C. §103 on the following grounds.

- **Ground 1:** Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri (Ex-1005) in view of Bradley (Ex-1006) and Jeong (Ex-1007).

- **Ground 2:** Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri, Bradley, and Ala-Laurila (Ex-1013).
- **Grounds 3-4:** Claims 5-6 are obvious over Nakhjiri in view of Bradley, Jeong, and X9.63-Overview (Ex-1014); or Nakhjiri, Bradley, Ala-Laurila, and X9.63-Overview.
- **Grounds 5-6:** Claim 8 is obvious over Nakhjiri in view of Bradley, Jeong, and Pierce (Ex-1009); or Nakhjiri, Bradley, Ala-Laurila, and Pierce.
- **Grounds 7-8:** Claim 15 is obvious over Nakhjiri in view of Bradley, Jeong, and GlobalPlatform (Ex-1010); or Nakhjiri, Bradley, Ala-Laurila, and GlobalPlatform.

VII. TECHNOLOGICAL BACKGROUND

A. Mobile device with an eUICC performing a method to securely communicate with a wireless network

29. Methods for using a mobile device with an eUICC to perform a method to securely communicate with a wireless network were well known by 2013. For example, Rajadurai teaches a method for “establishing a communication session with the operator network using the IMSI assigned to the user equipment,” wherein “an authentication and authorization server securely provisions an UICC in the user equipment “with the IMSI, the selected security profile, and the random number using the security keys.” Ex-1008 (Rajadurai) ¶¶22, 33, Fig. 4. Moreover, 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 associated with storing the ciphering key in the terminal and access point in advance. Ex-1013 (Ala-Laurila) ¶¶4-5; *see also* Ex-1028 (CSMG), 5 (a mobile device’s “SIM identifies the subscriber to the network and enables this identity to be securely authenticated”); Ex-1029 (Farnham), Abstract (“[a] method of establishing a secure communications link between a terminal and a server”); Ex-1027 (Bhuyan) ¶1 (“a method of authenticating a mobile device” in a telecommunications network “using a network provisioned security module and subsequent secure communications between the mobile device and the network”); Ex-1032 (Nguyen) ¶1 (“method and apparatus for end-to-end mobile user security in a network”); Ex-1033 (Natarajan) ¶2 (“system and method for secure transaction of data between at least one wireless communication device and a server by using ... ECC (Elliptic Curve Cryptography) and SKE (Symmetric Key Encryption) mechanisms.”); Ex-1024 (Gouget) ¶11 (“a method for establishing a secure communication channel between a client (C) and a remote server (S)” where data is exchanged “through an intermediate entity (G)”); Ex-1035 (Park), 297 (teaching a “secure profile provisioning architecture” for “[e]mbedded UICC (hereafter eUICC),” which is “a new form of UICC (Universal Integrated Circuit Card)” that is “soldered into a device during manufacturing”).

B. Storing a first module private key, a corresponding first module public key, and a network public key in the eUICC

30. Secure communication methods involving storing a first module private key and a corresponding first module public key in the eUICC were well known by 2013. For example, Rajadurai teaches that “[w]hen installed for a first time, the UICC 112 installed in each of the user equipments 102A-N includes a private key infrastructure (PKI) (including an UE certificate, and a root certificate) or a vendor shared key, a machine identifier, security capabilities, and storage space for storing provisioning data.” Ex-1008 (Rajadurai) ¶18. Rajadurai further teaches that “[t]he provisioning data may include” IMSI, “a security profile selected by the network operator, and a subscription key.” Ex-1008 (Rajadurai) ¶18. Rajadurai notes that “each of the user equipments 102A-N includes the UICC 112 without the provisioning data of the network operator” but further teaches that the UICC smart card receives “provisioning data from the operator network 104” (Ex-1008 (Rajadurai) ¶42) and is “capable of storing provisioning data.” Ex-1008 (Rajadurai) ¶40. Moreover, Park teaches that “[t]he traditional UICC is pre-provisioned by the SIM Vendor on the behalf of MNO by using the MNO’s data and applications (hereafter profiles) such as NAA(Network Access Application) with related data (e.g. IMSI (International Mobile Subscriber Identity), *keys*, authentication algorithm, etc.) and fundamental VASs (Value-Added Services).” Ex-1035 (Park), 297. Park further teaches that “[t]he eUICC ID and capability information are signed

by the eUICC Vendors private key,” and this signed value is added to a message send from the eUICC to the SM-SR. Ex-1035 (Park), 300. Park also explains that the eUICC Vendor private key is part of a public key pair (i.e., it corresponds to an eUICC Vendor public key), and that it is generated by the eUICC Vendor and stored on the eUICC during the pre-provisioning stage. Ex-1035 (Park), 300.

31. Additionally, secure communication methods involving storing a network public key in the eUICC were known by 2013. For example, Farnham teaches that non-volatile programme memory in the mobile device stores “public keys for one or more server operators.” Ex-1029 (Farnham) ¶¶38, 51 (“the mobile terminal ... is assumed to have a copy of the server’s (public) encrypting key”), 57 (“the SIM may contain the server’s public value”). Moreover, Farnham teaches that “[t]he mobile terminal B or client can obtain the server’s public value $Y_A = g^a \text{ mod } p$ where [a] is the private key of the server, for example from a server key exchange” or “[p]referably ... the server’s public value is stored in the SIM.” Ex-1029 (Farnham) ¶68; *see also* Ex-1025 (Semple) ¶¶48 (“BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x ”), 49 (“MT 606 receives the triplet (RAND, P^x , SIG) 610”); Ex-1026 (Wang) ¶42 (WTRU selects server public key k_a from a set of public keys broadcast by the LTE network); Ex-1033 (Natarajan) ¶¶30 (“the server 110 generates a random number ‘r’ upon receiving client hello message,” “computes a resultant masking process of random

number ... using the generated random number 'r', Mask, a transaction ID by matching hash function, wherein the Mask=156-bits," "encrypts a message with the resultant masking process of random number 's' thereby matching hash function, adding a nonce value for security with help of a public key 'PUB' of the wireless communication device 120 using an ECE Encryption algorithm and then the server 212 sends the encrypted message ... to the wireless communication device"), 31 ("the wireless communication device 120 retrieves the random number 'r' and the Mask ... thereby matching hash function with help of a private key 'k' of the wireless communication device 120 upon receiving the encrypted message thereby using an ECE Decryption algorithm and subsequently the wireless communication device 120 splits the random number 'r' and the Mask and then subsequently verifies the values of the random number with the Nonce value for security and the resultant masking process of random number 's' with hash function").

C. Receiving from a first server an encrypted profile for the eUICC comprising cryptographic parameters, module identity, and key K

32. Secure communication methods involving receiving from a first server an encrypted profile for the eUICC comprising cryptographic parameters, a module identity, and a key K were well known by 2013. For example, CSMG teaches that "[t]he International Mobile Subscriber Identity (IMSI) is a unique identifier associated with each GSM and UMTS subscription," which "is stored as a 64-bit field in the SIM and is sent by the phone to the network when the device is asked to

identify by the network.” Ex-1028 (CSMG), 16. Moreover, CSMG teaches that “[i]n order to prove the identity of the device, a secret key, ‘Ki’ is also used” and “may be stored in a proprietary file specific to each SIM card vendor.” Ex-1028 (CSMG), 16. CSMG further teaches that “MNO-specific authentication algorithms are also stored on the SIM and used to generate unique responses to network authentication challenges” to “ensure that each MNO retains unique ownership over the SIM card and its authentication abilities.” Ex-1028 (CSMG), 16, 21 (“The authentication process for GSM uses MNO-specific encryption algorithms (A3, A8) to identify and authenticate a subscriber.”); *see also* Ex-1013 (Ala-Laurila) ¶¶18 (“The SIM comprises an International Mobile Subscriber Identity IMSI which represents the subscriber in the network, thus operating as an identifier of the terminal MT. ... The SIM also comprises a secret key Ki, an algorithm A8 for forming a ciphering key Kc and an algorithm A3 for forming an authentication response SRES (Signed Response).”), 25 (“MT is offered an identifier IMSI and a secret key Ki by the subscriber identity application SIM included therein”); Ex-1029 (Farnham) ¶38 (non-volatile programme memory stores “symmetric and asymmetric cryptography code”); Ex-1027 (Bhuyan) ¶¶25 (a SIM “is used to store a secret key that is been preloaded onto the card when the card is made” and the secret key is “shared a priori between the mobile phone and the network operator before any communication is initiated”), 59 (authentication server “generates in response to the [user’s

authentication] request a unique identifier for the mobile device” referred to as the IMSI “as well as a secret key Ki”), 62 (provisioning server “encrypts and sends a file containing the security parameters IMSI and Ki to the mobile device ... using the password provided by the user” along with “the software-based security module,” which “is an application that is run by the mobile device”), 65 (user then “installs the security module on the mobile device 210 and also stores the security parameters IMSI and Ki”).

33. Moreover, Rajadurai teaches that “the authentication and authorization server 108 securely provisions the UICC 112 in the user equipment 102A with the IMSI, the selected security profile, and the random number using the security keys.” Ex-1008 (Rajadurai) ¶22. Rajadurai further teaches “[t]he security profile contains a security algorithm (e.g., AES, SNOW 3G, MILENAGE, the like) supported modes of the security algorithm, and a key length.” Ex-1008 (Rajadurai) ¶18. Moreover, Rajadurai teaches that the user equipment then “generates a subscription key using the operator shared key and the random number and stores the IMSI assigned by the network operator along with security profile and subscription key and uses the IMSI for establishing communication sessions with the operator network 104.” Ex-1008 (Rajadurai) ¶22; *see also id.* ¶28; Ex-1025 (Semple) ¶¶26 (“[t]he IMSI is a unique number that is associated with an MT 102 in the network”), 27 (the “process of registering with a service provider may involve authenticating MT 102 by using a

pre-shared secret key (e.g., stored in a GSM SIM, CDMA Authentication Module, or other legacy module”), 33 (“SIM 204 may contain a secret key K_i , an implementation of GSM authentication and key agreement algorithms (i.e., the GSM A3/A8 algorithms)”); MT 102 and BSF 106 “may also share a pre-determined generator P of a cyclic group, such as the multiplicative subgroup of a finite field or a point in an elliptic curve, allowing them to employ the Diffie-Hellman key exchange.”), 47 (HLR 104 “includes a database that contains mobile subscriber information for a wireless carrier, including an International Mobile Subscriber Identity (IMSI) for each MT 102 belonging to the subscriber,” which “is also stored in the Subscriber Identity Module (SIM) of each MT 102.”), 48 (P is “previously provisioned to both the BSF 604 and MT 606.”), Figs. 2, 6; Ex-1026 (Wang) ¶15 (mobile device (WTRU) stores a user ID in the form of an IMSI as part of the “initial security parameters”).

34. SEC1 also teaches “public-key cryptographic schemes based on elliptic curve cryptography (ECC).” Ex-1011, 1. SEC1 teaches that “[t]he list of supported key derivation functions at this time is: ANSI-X9.63-KDF.” Ex-1011, 31-32. SEC1 further teaches that “[t]he key derivation function ANSI-X9.63-KDF is the simple hash function construct described in ANS X9.63 [X9.63].” Ex-1011, 32-33. Moreover, SEC1 teaches that “[e]ntities U and V should perform the following setup

procedure to prepare to use the elliptic curve Diffie-Hellman scheme ... Let KDF denote the key derivation function chosen.” Ex-1011, 56-57.

D. Generating a shared secret key using a first ECDH key exchange with the first module private key and the network public key

35. Secure communication methods involving generating a shared secret key using a first ECDH key exchange with the first module private key and the network public key were well known by 2013. For example, Rajadurai teaches that “the authentication and authorization server 108 provides the IMSI, the random number and the security profile to the user equipment 102A” and “the user equipment 102A derives the subscription key using the operator shared key and the random number. At step 238, the user equipment 102A stores the subscription key and the IMSI along with the security profile in the storage space of the UICC 112.” Ex-1008 (Rajadurai) ¶28; *see also* Ex-1034 (Cuppett), 5:50-56 (“Examples of known asymmetric encryption systems that can be used include ... Diffie-Hellman.”). As another example, Gouget teaches generating “the common secret by the client (C) and by the server (S) ... based on the ephemeral secret key (sk_{cc}) of said ephemeral key pair (sk_{cc}, pk_{cc}) of the client (C) ... according to the Diffie-Hellman protocol.” Ex-1024 (Gouget) ¶12. For example, Gouget teaches that “[i]n the Chip Authentication CA step: the client C is authenticated by the server S by verifying an authentication token computed from an exchanged Diffie-Hellman key” based on the client-side public key, which “is the long-term key pk_c certified during

the passive authentication step PA” and the server-side public key, which “is the ephemeral key pk_s chosen by the server S during the terminal authentication step TA.” Ex-1024 (Gouget) ¶39. Gouget further teaches that “[t]he Diffie-Hellman key shared between the client C and the server S is used to compute or verify the authentication token and also to establish the secure channel.” Ex-1024 (Gouget) ¶39. “This Diffie-Hellman key is computed from pk_c and sk_s at the server side and from sk_c and pk_s at the client side.” Ex-1024 (Gouget) ¶39; *see also id.* ¶¶40-41. Specifically, “[t]he client C calculates the common secret key as following: $K=KDF(sk_c, pk_s, sk_{cc}, pk_s)$,” the server “also calculates the common secret key as following: $K=KDF(sk_s, pk_c, sk_s, pk_{cc})$,” “where KDF is a Key Derivation Function” and the protocol used “is the Diffie-Hellman protocol (DH or ECDH).” Ex-1024 (Gouget) ¶¶42-45.

36. Moreover, Farnham teaches employing a Diffie-Hellman cryptographic technique, wherein “[t]he mobile terminal B can compute a key for a symmetric session $k=Y_A^b \bmod p=(g^a \bmod p)^b \bmod p=g^{ab} \bmod p$ and the server A can compute the same session key $k=(g^b \bmod p)^a \bmod p=g^{ba} \bmod p$ ” so that “[e]ncrypted data or software may then be sent to the terminal B by encrypting it with a session key or the session key may be used by both the terminal and server to generate another common key, for example by operating on data known to both with K.” Ex-1029 (Farnham) ¶¶66, 68; *see also id.* ¶¶12, 14, 57; *see also, e.g.,* Ex-1033 (Natarajan)

¶¶14 (“In the ECC ... [d]uring the communication, a permutation technique (cubing a random number w.r.to a prime $p=2 \bmod 3$) is used between the wireless communication device and the server ends in order to avoid reply attack.”), 27-49 (exemplary authentication process using ECC), 38-49 (describing an example “of the Secure Transaction of Data Using EAP Protocol Based on ECC”); *see also* Ex-1025 (Semple) ¶¶51 (Once Semple’s MT has received the server public key P^x and has derived its own module private key y , it can calculate a Diffie-Hellman shared secret $(P^y)^x$, or P^{xy} ; the BSF similarly calculates $(P^y)^x$, or P^{xy} , using its own private key x and the module public key P^y , thus allowing them to mutually derive the same shared secret; “MT 606 and BSF 604 have thus carried out a mutually authenticated Diffie-Hellman key exchange and agree on a key P^{xy} which they compute respectively.”).

E. Decrypting at least a portion of the encrypted profile for the eUICC with the shared secret key

37. Secure communication methods involving decrypting at least a portion of the encrypted profile for the eUICC with the shared secret key were well known by 2013. For example, Rajadurai teaches that “the user equipment 102A decrypts the encrypted operator shared key and derives the subscription key using the decrypted operator shared key and the random number. At step 324, the user equipment 102A stores the subscription key and the IMSI along with the security profile in the storage space of the UICC 112.” Ex-1008 (Rajadurai) ¶32; *see also*

Ex-1034 (Cuppett), 2:19-21 (“The decryption key on the token decrypts the data received from the server and permits its display on the client.”), 5:35-41 (“A preferred embodiment of the authentication/decryption system employs an asymmetric encryption system (public key/private key pair). As such, the enterprise system ... uses a unique public key to encrypt confidential enterprise data fields (end-to-end). A unique private key, which resides on the portable token, is needed for decrypting the confidential fields.”).

38. Moreover, Park teaches that, upon receiving the encrypted profile block from the SM-DP, “PM of eUICC performs the necessary cryptographic operations for the secure communication channel, and then PI of eUICC decrypts and verifies the received profile blocks.” Ex-1035 (Park), 300. Because each of the SM-DP and eUICC share the same SM-DP Credential (claimed “profile key”), the SM-DP Credential is a shared secret key—i.e., one that can be used for both encryption and decryption, and decrypting each profile block, as performed by the eUICC, would involve using the SM-DP Credential (i.e., shared secret key).

F. Generating, by the eUICC, a second module public key and a corresponding second module private key

39. Secure communication methods involving generating, by the eUICC, a second module public key and a corresponding second module private key were well known by 2013. For example, Gouget teaches a three-step “mutual authentication” method comprising “a terminal authentication step, a passive authentication step,

and a chip authentication step.” Ex-1024 (Gouget) ¶4. Specifically, Gouget teaches “a method for establishing a secure communication channel between a client (C) and a remote server (S)” where the client (C) and remote server (S) exchange “data through an intermediate entity (G),” the client (C) has “a long-term key pair (sk_c, pk_c),” and the remote server generates “an ephemeral key (sk_s, pk_s).” Ex-1024 (Gouget) ¶11. Gouget further teaches that the method comprises “a mutual authentication step” where “the client (C) sends a public key (pk_c) of said long-term key pair (sk_c, pk_c) and the proof that said public key (pk_c) is valid to the server (S)” and “the remote server (S) sends the public key (pk_s) of said ephemeral key pair (sk_s, pk_s) to the client (C).” Ex-1024 (Gouget) ¶11; *see also id.* ¶36. Moreover, Gouget teaches that “the client (C) generates an ephemeral key pair (sk_{cc}, pk_{cc}) and sends the public key (pk_{cc}) of said ephemeral key pair (sk_{cc}, pk_{cc}) to the server (S) so as to generate a secret common to the client (C) and to the remote server (S) for opening the secure communication channel.” Ex-1024 (Gouget) ¶11; *see also id.* ¶41 (“The client C also generates an ephemeral key pair (sk_{cc}, pk_{cc}) during the chip Authentication step CA.”).

40. Moreover, Ala-Laurila teaches using a Diffie-Hellman key exchange process to secure the communications between the MT and an authentication server. 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 (Ala-Laurila) ¶26. The authentication request “is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm.” Ex-1013 (Ala-Laurila) ¶26. The PAC is in communication with the authentication server (GAGW). Ex-1013 (Ala-Laurila) ¶¶22-23; *see also* Ex-1025 (Semple) ¶¶48 (teaching a Diffie-Hellman key derivation process based on a shared cryptographic parameter P, “where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of an elliptic curve”; “BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x ” which is sent to the MT), 49 (“MT 606 receives the triplet (RAND, P^x , SIG) 610”; MT 606 performs the converse process and “generates a random number y and computes P^y ”), 51 (“MT 606 and BSF 603 have thus carried out a mutually authenticated Diffie-Hellman key exchange and agree on a key P^{xy} which they compute respectively.”).

41. Similarly, Farnham teaches employing “an anonymous Diffie-Hellman cryptographic technique.” Ex-1029 (Farnham) ¶66. Specifically, Farnham teaches that “[t]he terminal chooses a random value b, computes $g^b \text{ mod } p$ and sends $M1 \ g^b \text{ mod } p$ (encrypted) to the server.” Ex-1029 (Farnham) ¶68; *see also* Ex-1032 (Nguyen) ¶36 (“MS_1 can use its own private key P_1 to compute its own public key Q_1 using a chosen base point B on a specific Elliptic Curve algorithm. The base point ‘B’ can be a random value selected from an elliptic curve algorithm.”);

Ex-1033 (Natarajan) ¶¶32 (“the wireless communication device 120 generates and adds the signature {signs} with message having a resultant value ‘m’, wherein the resultant value ‘m’ { $m=r^3 \bmod p$ } a 137-bit number} is obtained using permutation technique of the random number ‘r’, with respect to its private key ‘k’ thereby using an ECDSA-163 algorithm and subsequently the wireless communication device 120 sends the resultant message {sig_value} to the server”), 33 (“the server 110 verifies the signature {sig_value} of the received resultant message with help of the public key ‘PUB’ of the wireless communication device 120 using ECDSA-163 algorithm and subsequently the server 110 retrieves the resultant value ‘m’ { $r^3 \bmod p$ } by using permutation technique of the random number ‘r’”), 36 (“The wireless communication device 120 uses its private key ‘k’ of 163-bits for Elliptic Cryptography (EC) decryption and EC signature generation and uses its public key ‘PUB’ for Elliptic Cryptography (EC) decryption and EC signature verification and a known Pseudo Random Number Generator (PRNG) which accepts a seed for generating the random numbers.”).

G. Sending the second module public key to a second server

42. Secure communication methods involving sending the module public key to a second server were well known by 2013. For example, Gouget teaches that the client C “generates an ephemeral key pair (sk_{cc}, pk_{cc}) during the chip Authentication step CA and sends the public key pk_{cc} of said ephemeral key pair

(sk_{cc}, pk_{cc}) to the server S.” Ex-1024 (Gouget) ¶41. Moreover, Ala-Laurila teaches using a Diffie-Hellman key exchange process to secure the communications between the MT and the PAC. Ex-1013 (Ala-Laurila) ¶¶25-26. Additionally, 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” that 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 (Ala-Laurila) ¶¶22-23. Ala-Laurila further teaches that the MT sends “the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a” NAI. Ex-1013 (Ala-Laurila) ¶26. Ala-Laurila teaches that “[t]he NAI comprises the IMSI identifier obtained from the identity module SIM.” Ex-1013 (Ala-Laurila) ¶26. Ala-Laurila also teaches that the request “is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm.” Ex-1013 (Ala-Laurila) ¶26.

43. Farnham also teaches that “the Diffie-Hellman value $g^b \text{ mod } p$ may be encrypted using the originator’s (that is, in this example, B’s) private key. More specifically it may be protected by sending the Diffie-Hellman value as a digital signature from which the signed message is recoverable. The recipient may then recover $g^b \text{ mod } p$ using the originator’s public key, more specifically by extracting the message from the signature.” Ex-1029 (Farnham) ¶¶70, 79 (“The session key

may be computed ... using an appropriate publicly known non-reversible function f such as MD5 (Message Digest 5, as defined in RFC 1321) and SHA-1 (secure Hash Algorithm-1, see, for example, US National Bureau of Standards Federal Information Processing Standards (FIPS) Publication 180-1.”); *see also* Ex-1025 (Semple) ¶50 (BSF “receives P^y ,” which is the module public key).

H. Generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters

44. Secure communication methods involving generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters were well known by 2013. For example, Gouget teaches generating “the common secret by the client (C) and by the server (S) ... based on the ephemeral secret key (sk_{cc}) of said ephemeral key pair (sk_{cc}, pk_{cc}) of the client (C) ... according to the Diffie-Hellman protocol.” Ex-1024 (Gouget) ¶12. For example, Gouget teaches that “[i]n the Chip Authentication CA step: the client C is authenticated by the server S by verifying an authentication token computed from an exchanged Diffie-Hellman key” based on the client-side public key, which “is the long-term key pk_c certified during the passive authentication step PA” and the server-side public key, which “is the ephemeral key pk_s chosen by the server S during the terminal authentication step TA.” Ex-1024 (Gouget) ¶39. Gouget further teaches that “[t]he Diffie-Hellman key shared between the client C and the server S

is used to compute or verify the authentication token and also to establish the secure channel.” Ex-1024 (Gouget) ¶39. “This Diffie-Hellman key is computed from pk_c and sk_s at the server side and from sk_c and pk_s at the client side.” Ex-1024 (Gouget) ¶39; *see also id.* ¶¶40-41. Specifically, “[t]he client C calculates the common secret key as following: $K=KDF(sk_c, pk_s, sk_{cc}, pk_s)$,” the server “also calculates the common secret key as following: $K=KDF(sk_s, pk_c, sk_s, pk_{cc})$,” “where KDF is a Key Derivation Function” and the protocol used “is the Diffie-Hellman protocol (DH or ECDH).” Ex-1024 (Gouget) ¶¶42-45.

45. Moreover, Farnham teaches employing a Diffie-Hellman cryptographic technique, wherein “[t]he mobile terminal B can compute a key for a symmetric session $k=Y_A^b \bmod p=(g^a \bmod p)^b \bmod p=g^{ab} \bmod p$ and the server A can compute the same session key $k=(g^b \bmod p)^a \bmod p=g^{ba} \bmod p$ ” so that “[e]ncrypted data or software may then be sent to the terminal B by encrypting it with a session key or the session key may be used by both the terminal and server to generate another common key, for example by operating on data known to both with K.” Ex-1029 (Farnham) ¶¶66, 68; *see also id.* ¶¶12, 14, 57; *see also, e.g.*, Ex-1033 (Natarajan) ¶¶14 (“In the ECC ... [d]uring the communication, a permutation technique (cubing a random number w.r.to a prime $p=2 \bmod 3$) is used between the wireless communication device and the server ends in order to avoid reply attack.”), 27-49 (exemplary authentication process using ECC), 38-49 (describing an example “of

the Secure Transaction of Data Using EAP Protocol Based on ECC”); *see also* Ex-1025 (Semple) ¶¶51 (Once Semple’s MT has received the server public key P^x and has derived its own module private key y , it can calculate a Diffie-Hellman shared secret $(P^y)^x$, or P^{xy} ; the BSF similarly calculates $(P^y)^x$, or P^{xy} , using its own private key x and the module public key P^y , thus allowing them to mutually derive the same shared secret; “MT 606 and BSF 604 have thus carried out a mutually authenticated Diffie-Hellman key exchange and agree on a key P^{xy} which they compute respectively.”).

I. Generating with the symmetric key module encrypted data comprising the module identity

46. Secure communication methods involving generating with the symmetric key module encrypted data comprising the module identity were well known by 2013. For example, Farnham teaches that “the Diffie-Hellman value $g^b \text{ mod } p$ may be encrypted using the originator’s (that is, in this example, B’s) private key. More specifically it may be protected by sending the Diffie-Hellman value as a digital signature from which the signed message is recoverable. The recipient may then recover $g^b \text{ mod } p$ using the originator’s public key, more specifically by extracting the message from the signature.” Ex-1029 (Farnham) ¶70; *see also id.* ¶13 (“The identity of the sender or recipient may be included within the message with, optionally, a time stamp or random number or nonce (as described above with reference to other aspects of the invention).”). Rajadurai also teaches a method for

“establishing a communication session with the operator network using the IMSI assigned to the user equipment.” Ex-1008 (Rajadurai) ¶33, Fig. 4. Specifically, Rajadurai teaches that “the user equipment 102A sends a non-access stratum message including the assigned IMSI to the operator network 104.” Ex-1008 (Rajadurai) ¶33.

47. Moreover, 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 (Ala-Laurila) ¶26. The MT then sends “the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a Network Access Identifier NAI.” Ex-1013 (Ala-Laurila) ¶26. Ala-Laurila teaches that “[t]he NAI comprises the IMSI identifier obtained from the identity module SIM.” Ex-1013 (Ala-Laurila) ¶26. Ala-Laurila also teaches that the request “is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm.” Ex-1013 (Ala-Laurila) ¶26, Fig. 2. Ala-Laurila thus generating the encrypted IMSI (i.e., module identity) with a symmetric key derived during the Diffie-Hellman process.

48. Additionally, Gouget teaches that “a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key sk_c has been revealed.” Ex-1024 (Gouget) ¶22. Gouget further teaches that the client

C “generates an ephemeral key pair (sk_{cc}, pk_{cc}) during the chip Authentication step CA and sends the public key pk_{cc} of said ephemeral key pair (sk_{cc}, pk_{cc}) to the server S.” Ex-1024 (Gouget) ¶41. Specifically, “[t]he client C calculates the common secret key as following: $K=KDF(sk_c, pk_s, sk_{cc}, pk_s)$,” the server “also calculates the common secret key as following: $K=KDF(sk_s, pk_c, sk_s, pk_{cc})$,” “where KDF is a Key Derivation Function” and the protocol used “is the Diffie-Hellman protocol (DH or ECDH).” Ex-1024 (Gouget) ¶¶41-45. Additionally, Gouget teaches that “[t]he secure channel can then be established with the common secret” and “[b]y doing so, the security impact is reduced significantly when the long-term secret of the client is compromised.” Ex-1024 (Gouget) ¶¶47-48; *see also* Ex-1026 (Wang) ¶28 (“The present invention provides methods for initial loading and generation of security parameters, encryption key arrangements between the WTRU 210 and a network, **IMSI encryption**, and WTRU signaling adjustment for the IMSI encryption for the initial NAS signaling messages, which will be explained in detail hereinafter.”), 31 (teaching “ciphering on the attach message and the IMSI with the initial CK (from USIM or system information broadcast)” and then sending the “connection request message including ciphered attach message and IMSI along with the MAC-I.”; “Unlike the conventional attachment procedure, the attach message and the IMSI are protected with the initial CK and IK.”).

49. It was also known by 2013 that the module encrypted data includes the module identity. For example, Ala-Laurila teaches that “[t]he NAI *comprises the IMSI* identifier obtained from the identity module SIM.” Ex-1013 (Ala-Laurila) ¶26. Ala-Laurila also teaches that the request “is *preferably sent in ciphered form* to the PAC using the Diffie-Hellman algorithm.” Ex-1013 (Ala-Laurila) ¶26; *see also* Ex-1008 (Rajadurai) ¶33, Fig. 4.

J. Sending the module encrypted data to the second server

50. Secure communication methods involving sending the module encrypted data to the second server were well known by 2013. For example, Farnham teaches that “the Diffie-Hellman value $g^b \text{ mod } p$ may be encrypted using the originator’s (that is, in this example, B’s) private key. More specifically it may be protected by sending the Diffie-Hellman value as a digital signature from which the signed message is recoverable. The recipient may then recover $g^b \text{ mod } p$ using the originator’s public key, more specifically by extracting the message from the signature.” Ex-1029 (Farnham) ¶¶70, 79 (“The session key may be computed ... using an appropriate publicly known non-reversible function f such as MD5 (Message Digest 5, as defined in RFC 1321) and SHA-1 (secure Hash Algorithm-1, see, for example, US National Bureau of Standards Federal Information Processing Standards (FIPS) Publication 180-1.”)).

51. Moreover, Ala-Laurila teaches that the MT sends “the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a” NAI. Ex-1013 (Ala-Laurila) ¶26. Ala-Laurila teaches that “[t]he NAI comprises the IMSI identifier obtained from the identity module SIM.” Ex-1013 (Ala-Laurila) ¶26. Ala-Laurila also teaches that the request “is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm.” Ex-1013 (Ala-Laurila) ¶26. Rajadurai also teaches that “the user equipment 102A sends a non-access stratum message including the assigned IMSI to the operator network 104” (Ex-1008 (Rajadurai) ¶33), which “includes an authentication and authorization server 108, and a home subscriber server 110.” Ex-1008 (Rajadurai) ¶16.

52. Farnham further teaches that asymmetric cryptography can “be used to digitally sign messages by encrypting either the message or a message digest, using the private key.” Ex-1029 (Farnham) ¶6 (“A message digest is derived from the original message and is generally shorter than the original message making it difficult to compute the original message from the digest; a so-called hash function may be used to generate a message digest.”); *see also* Ex-1031 (Brainis) ¶37 (“both the authenticity and the data integrity” can be verified “with e.g. Message Authentication Code (MAC) or Hash-based Message Authentication Code (HMAC)”). Moreover, Gouget teaches that “a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext

data transmitted into the secure channel, even if the permanent secret key sk_c has been revealed.” Ex-1024 (Gouget) ¶22. Gouget further teaches that the secure channel is “established with the common secret.” Ex-1024 (Gouget) ¶47; *see also* Ex-1026 (Wang) ¶31 (“The C-PDCP layer 213 then performs ciphering on the attach message and the IMSI with the initial CK (from USIM or system information broadcast), and sends an LTE RRC connection request message including ciphered attach message and IMSI along with the MAC-I from the RRC layer 213 (steps 312, 314)”), Fig. 3.

VIII. THE '869 PATENT AND ITS FILE HISTORY

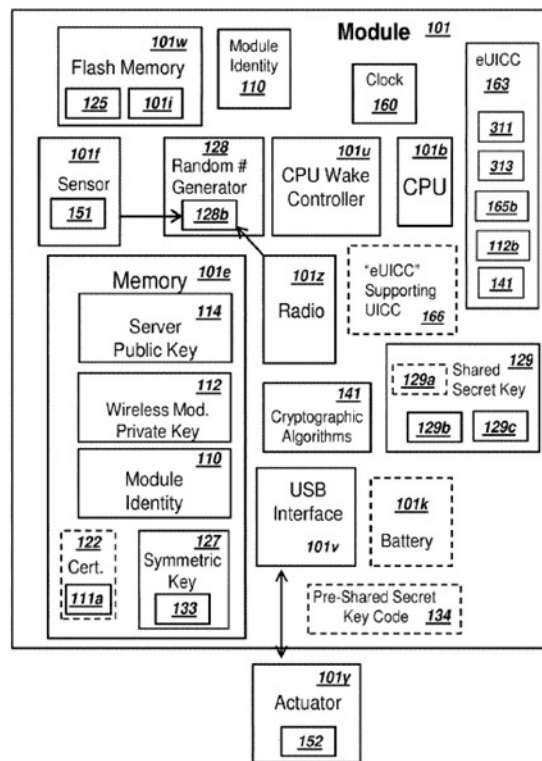
53. The '869 Patent teaches methods for supporting an eUICC (embedded universal integrated circuit card) in a mobile module, securely deriving keys for communicating with servers and a wireless network, including Elliptic Curve Diffie Hellman (ECDH)-based shared secrets, cryptographic parameters, and 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).

54. 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

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

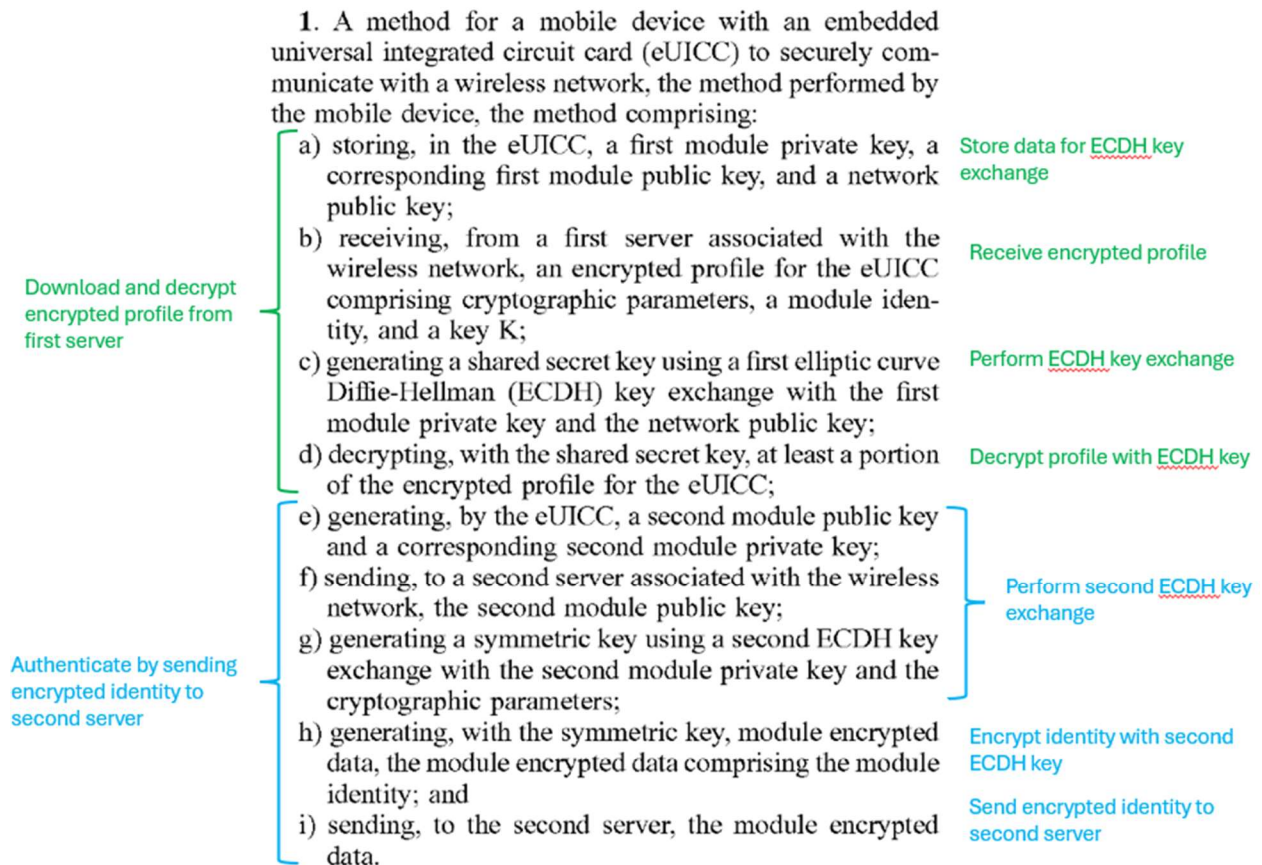
114, and module identity 110, and a symmetric key 127 in memory/RAM 101e during operation.” Ex-1001, 25:20-23. Module identity 110 is “a unique identifier of module 101” such as “an international mobile subscriber identity number (IMSI).” Ex-1001, 26:23-28. Module 101 also stores cryptographic algorithms 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, 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.

Figure 1c



55. 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.

56. 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.

57. 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.

58. 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.

IX. CLAIM CONSTRUCTION

59. For the purposes of my Declaration, I do not believe that any term requires explicit construction to resolve the issues I present in my Declaration because the prior art discloses or renders obvious the claim limitations under any potential construction of the claims.

X. OVERVIEW OF THE APPLIED PRIOR ART REFERENCES

60. In my opinion, 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).

A. Nakhjiri (Ex-1005)

61. Nakhjiri (U.S. Patent No. 9,210,138) was filed on April 17, 2013 and I understand it qualifies as prior art to the ’869 Patent.

62. Nakhjiri enables “multiple 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, as 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.

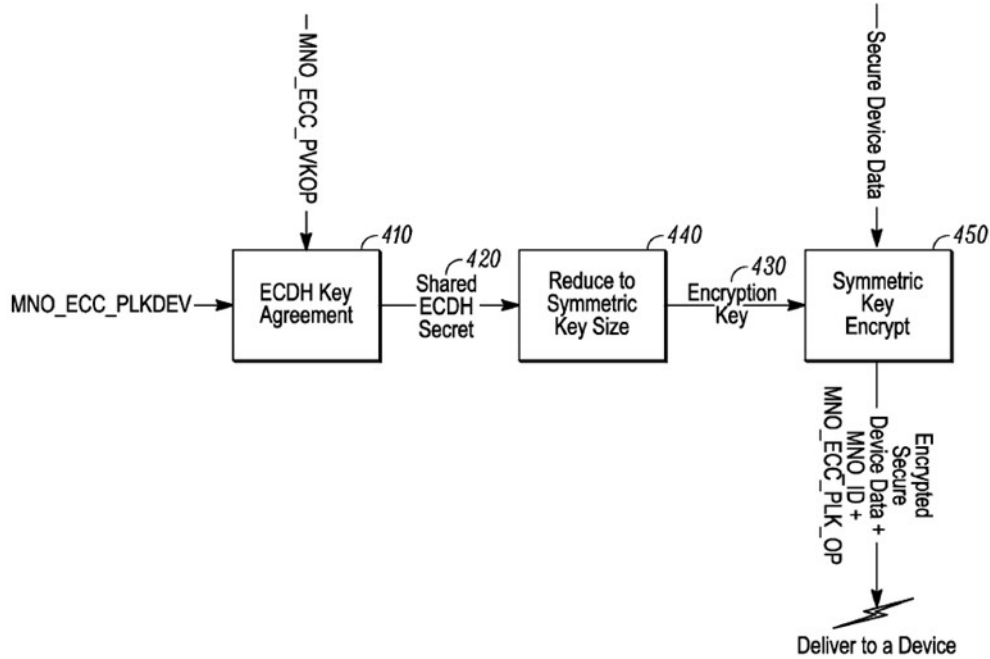


FIG. 3

63. 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)

64. Bradley (U.S. Patent Publication No. 2014/0024343) was filed on October 10, 2013 and I understand it qualifies as prior art to the ’869 Patent.

65. Bradley provides additional detail about the eUICC profile, teaching that it includes “relevant subscription information such as the *IMSI, K, Opc, 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)

66. Jeong was published in the Journal of Korea Multimedia Society, Vol. 13, No. 11 (pp. 1687-97) in November 2010 and I understand it qualifies as prior art to the ’869 Patent. The original publication in Korean is attached as Ex-1012, and a certified translation is provided at Ex-1007. I was able to access the original Korean publication on the website of the Korea Multimedia Society, which was founded in 1997. Ex-1017. The society 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. I was also able to find an entry for the Jeong paper in the catalog of the National Library of Korea on its “official e-government website of Korea.” Ex-1016. In my experience as an academic researcher, a POSITA would consult academic journals such as that of the

Korean Multimedia Society to search for reliable research on subjects such as cryptographic methods for authentication in cellular networks.

67. 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.

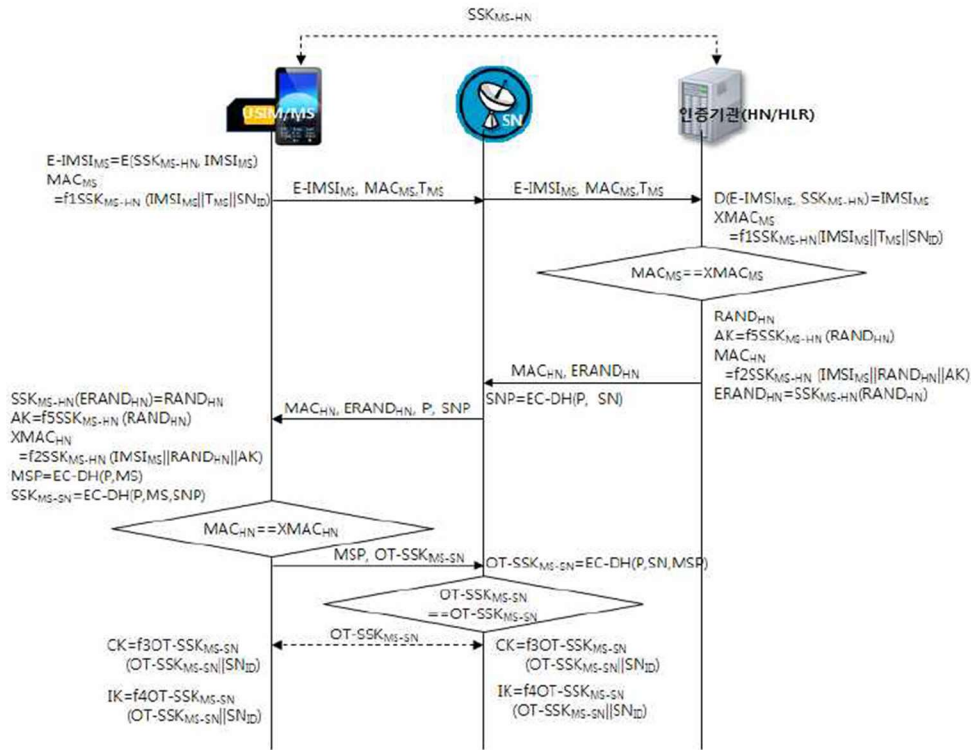


그림 6. 안전한 AKA 절차

D. Ala-Laurila (Ex-1013)

68. Ala-Laurila (U.S. Patent Publication No. 2012/0300934) was published on November 29, 2012 and I understand it qualifies as prior art to the '869 Patent.

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.

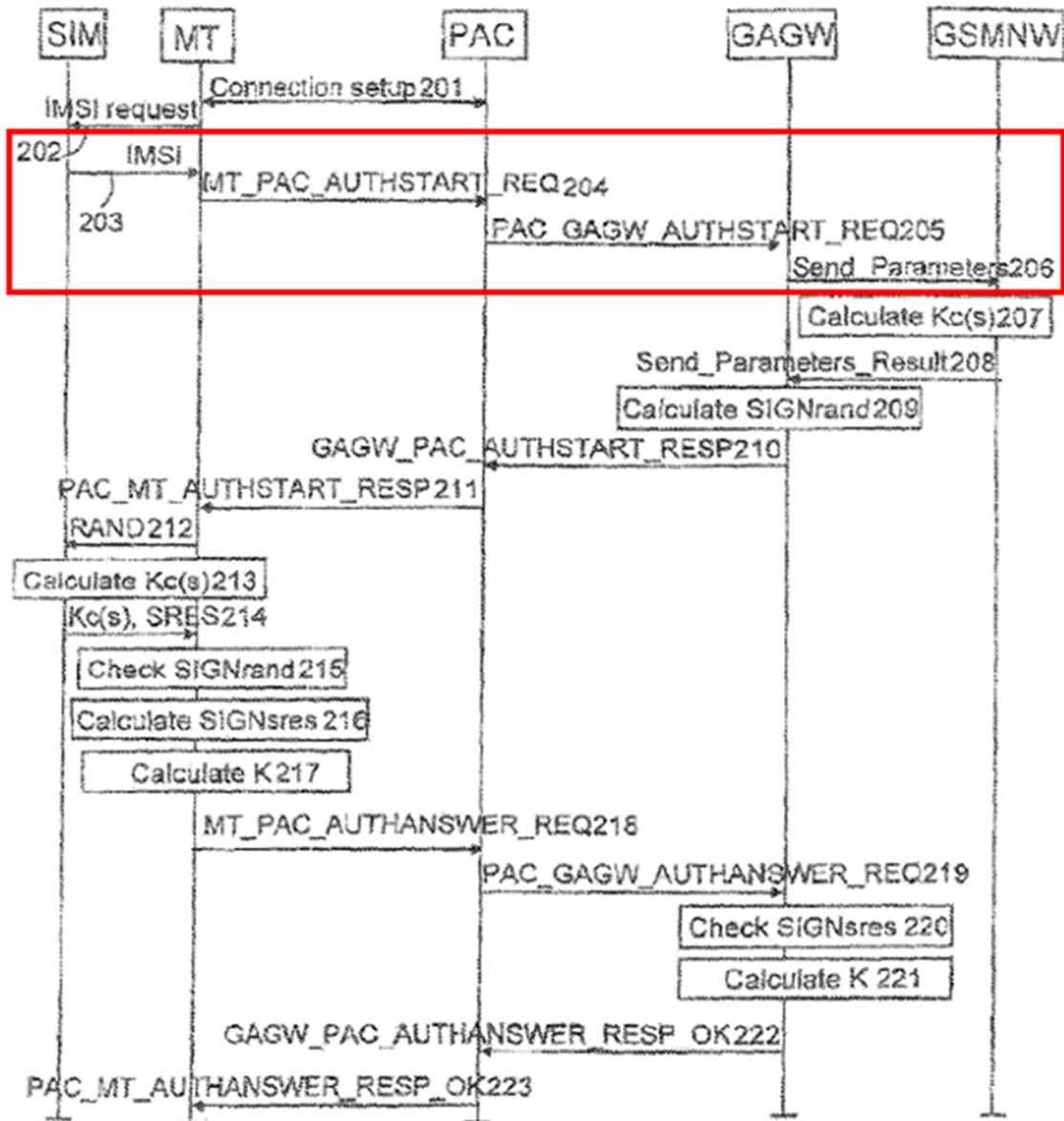


Fig. 2

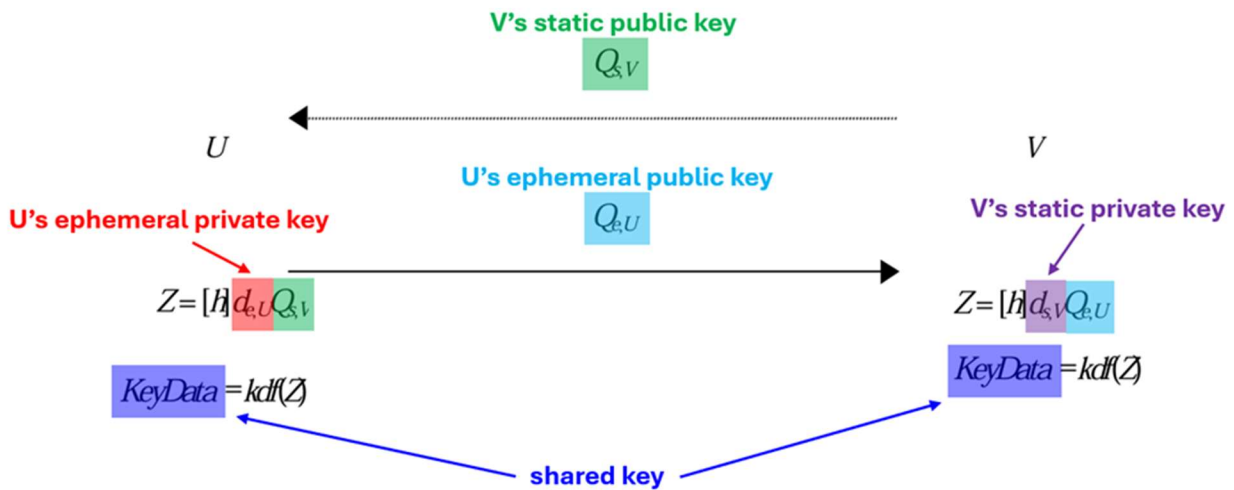
E. ANSI X9.63-Overview (Ex-1014)

70. 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, I understand it qualifies as prior art to the '869 Patent. I reviewed the declaration from the author and understand that

this document was publicly available well before 2013. Ex-1015. The ANSI X9.63 standard was also a well-known key derivation function in the field of cryptography and secure authentication and would have been familiar to a POSITA.

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)

72. Pierce (U.S. Patent Publication No. 2009/0323967) was published on December 31, 2009 and I understand it qualifies as prior art to the '869 Patent.

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)

74. GlobalPlatform (GlobalPlatform Remote Application Management over HTTP Card Specification V2.2 – Amendment B) was published in March 2012 and I understand it qualifies as prior art to the '869 Patent. A POSITA would have been well aware of the GlobalPlatform standard, which was developed for the smart card industry and served as a basis for much of the cryptographic development in the ETSI and 3GPP cellular standards.

75. I reviewed the declaration of Tono Aspinall, Operations Director at GlobalPlatform, Inc. and understand that GlobalPlatform publishes and makes available specifications, including Ex-1010, on its public website in the “GlobalPlatform Technology Document Library,” and that the date on each specification’s cover indicates the month of publication. Ex-1018.

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.

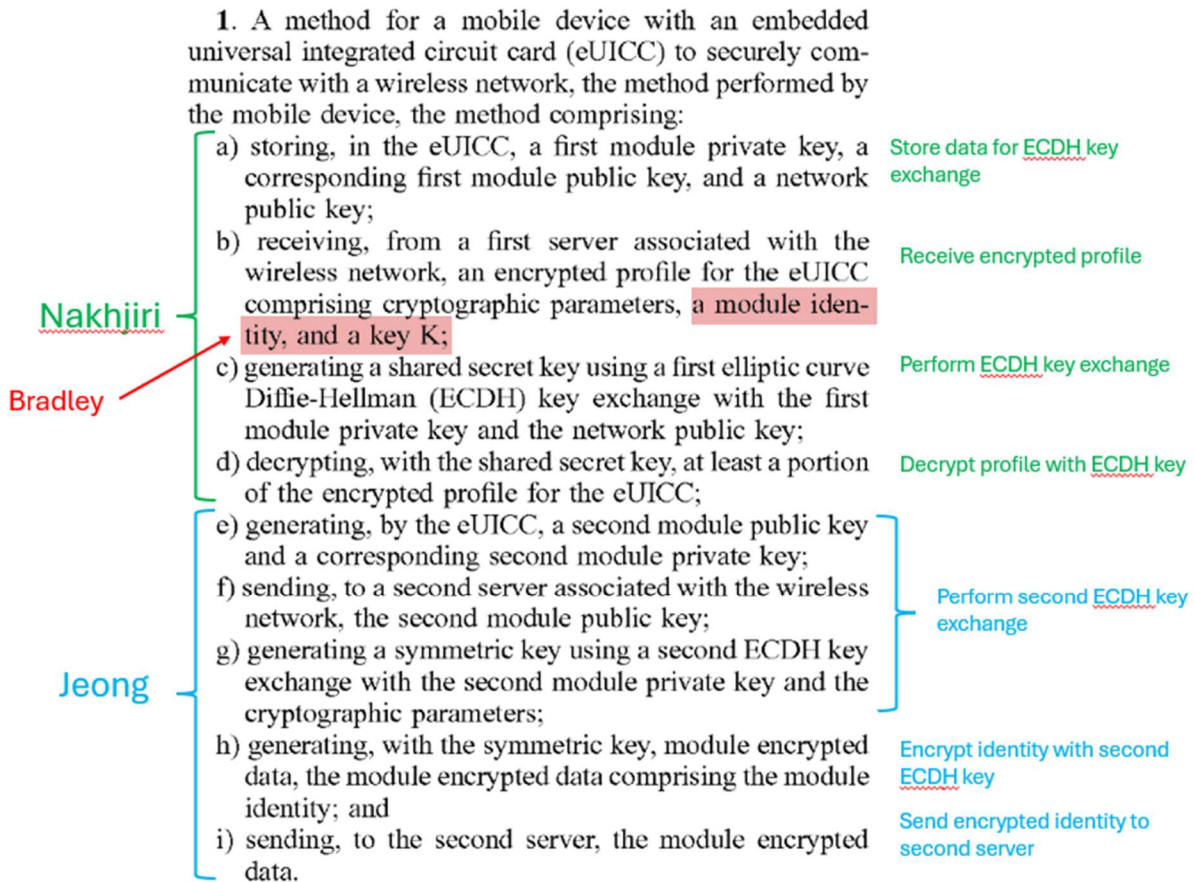
XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS

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.

77. In addition to the reasons set forth below, 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: (i) securely provision profile data (including identifier IMSI and key K) 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). 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 to two adjacent phases of the lifecycle. 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.

78. Below is a summary of claim 1 showing where each limitation is disclosed in the prior art:



79. 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. As described above, 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.

80. 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). 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. 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, 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).

81. 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).³ 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.

82. A POSITA would have had a reasonable expectation of success in combining the teachings of Nakhjiri-Bradley-Jeong. 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

³ 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).

that would have been amenable to various well-understood and predictable combinations.

2. Independent Claim 1

83. 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:**

84. In my opinion, Nakhjiri in view of Bradley and Jeong (“Nakhjiri-Bradley-Jeong”) teaches⁴ the preamble, to the extent it is limiting.

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

⁴ I understand from Counsel that the term “teaches” to include both express teachings and those fairly suggested to a person of ordinary skill in the art.

“instructions to the [universal integrated circuit card] UICC 614, cache 620, or 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.

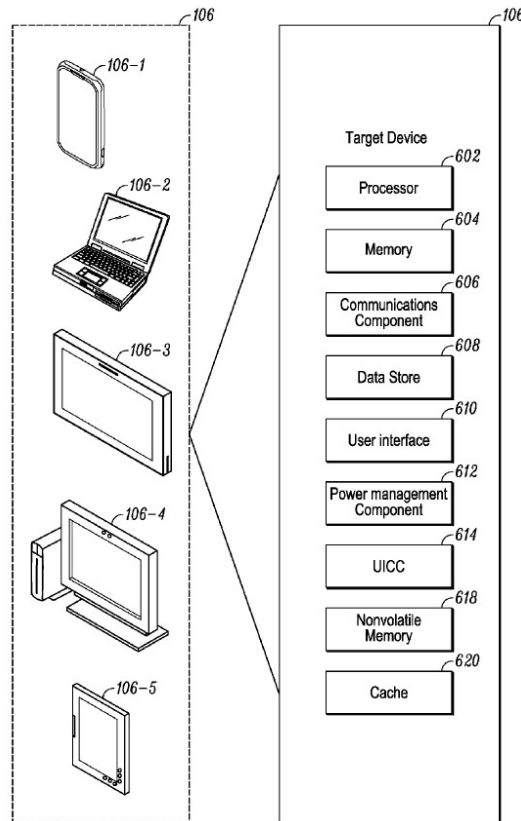


FIG. 5

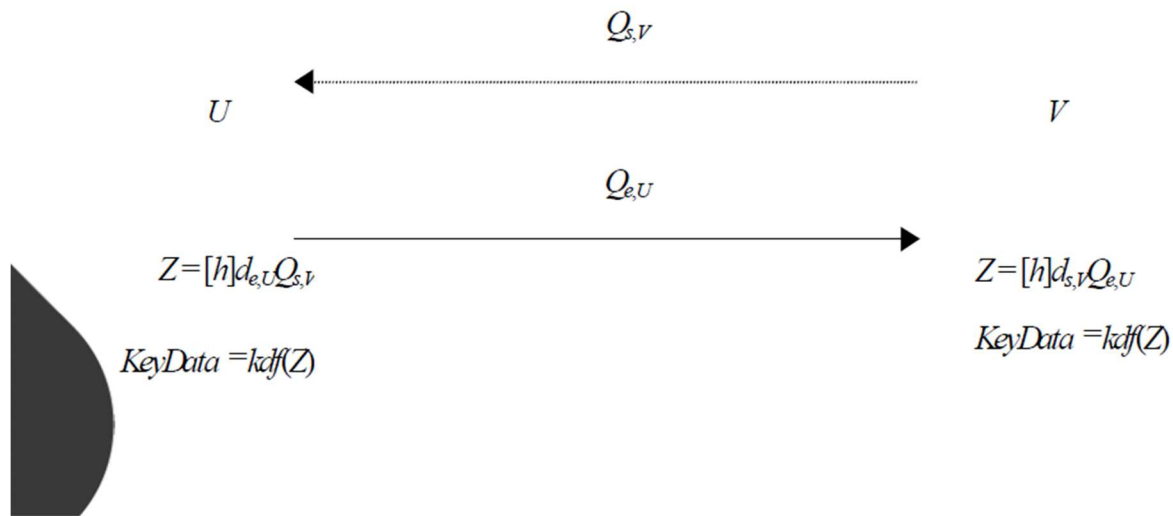
- b. **Element 1(a): storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key;**

86. In my opinion, Nakhjiri-Bradley-Jeong teaches Element 1(a). 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. *See, e.g.*, Ex-1033 (Boyd-Mathuria), 18; Ex-1014. For notational consistency, this public key (Q), private key (d) notation is used below. For example, the ANSI X9.63 Overview uses this notation to describe a Diffie-Hellman key exchange, as shown in the figure below (Ex-1014, 12), which illustrates an exchange between entities U and V.

ANSI X9.63 - 1-Pass DH



(1) A first module private key

87. Nakhjiri discloses a first module private key, d_m^{1st} . 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:

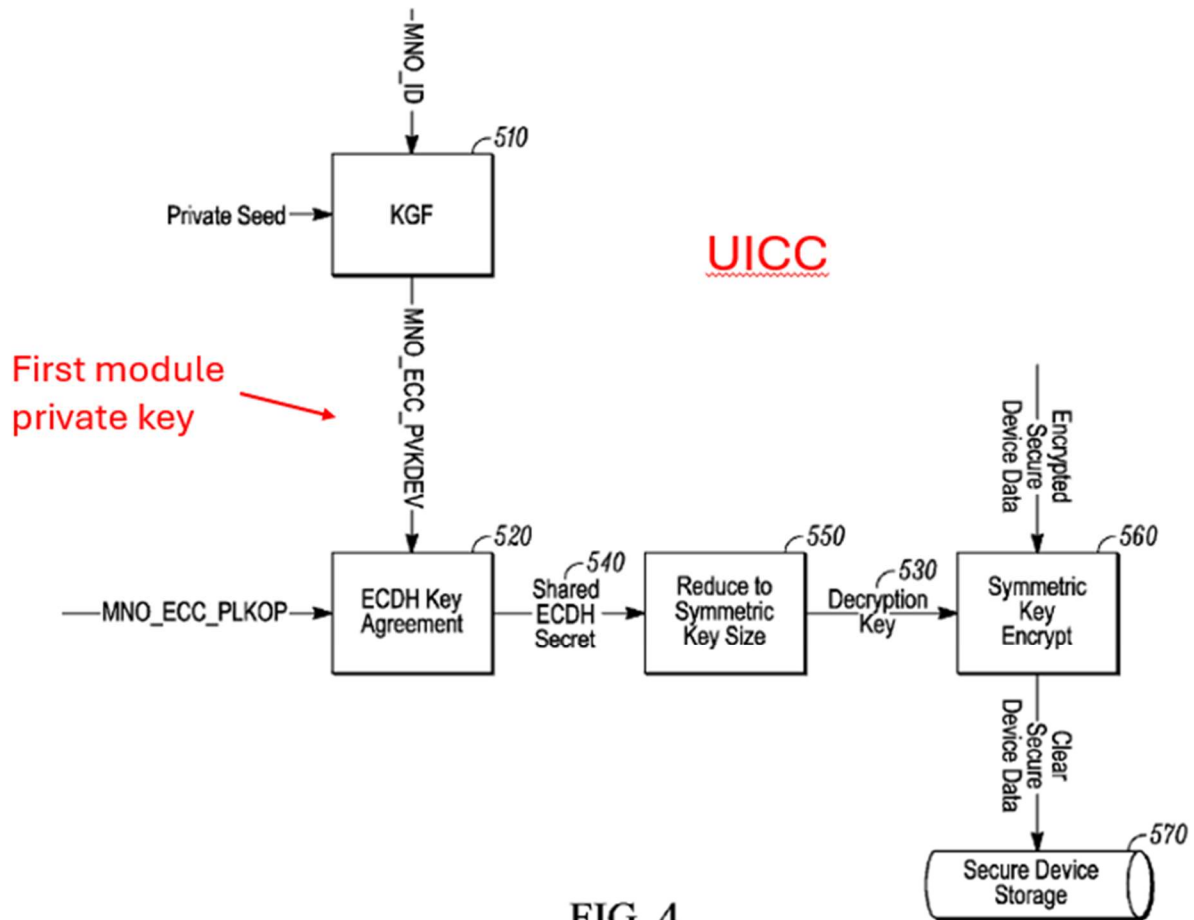


FIG. 4

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

(2) A corresponding first module public key

88. 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: $MNO_ECC_PLKDEV = MNO_ECC_PVKDEV * G$ 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.

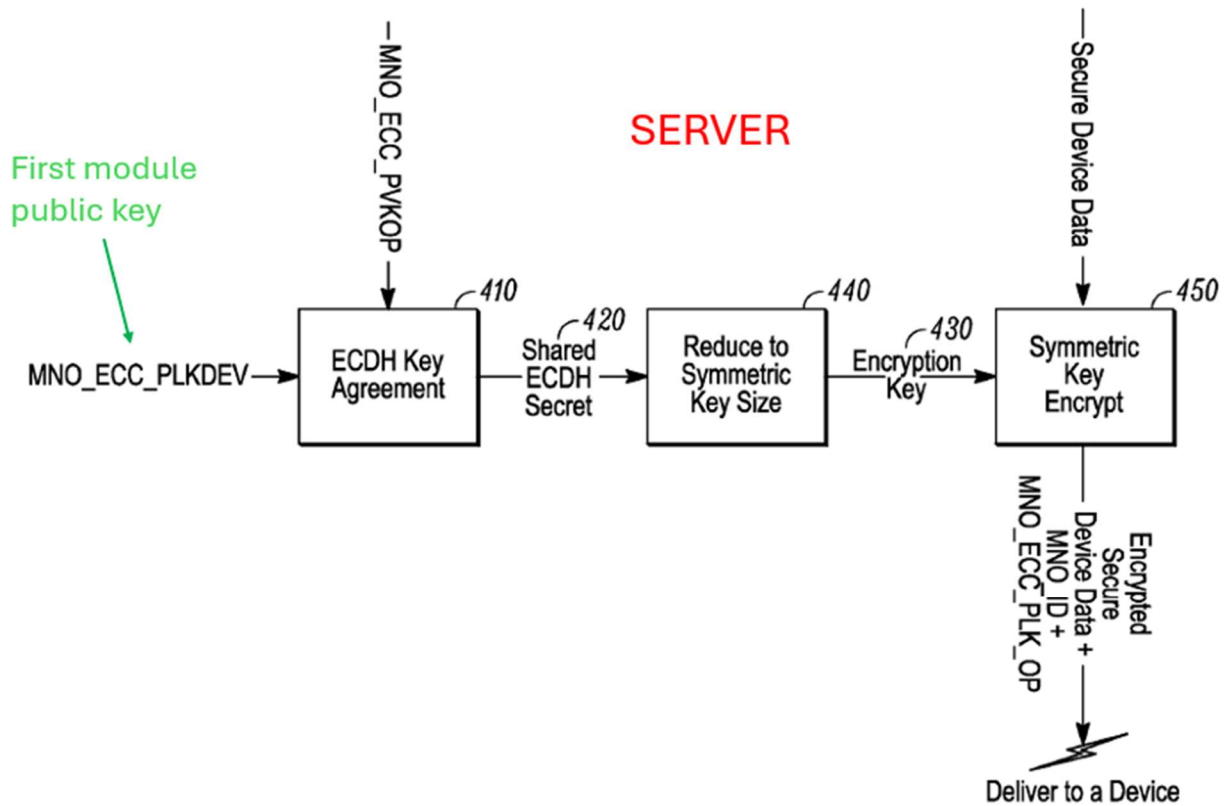


FIG. 3

Thus, $Q_m^{1s} = MNO_ECC_PLKDEV$.

(3) A network public key

89. 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:

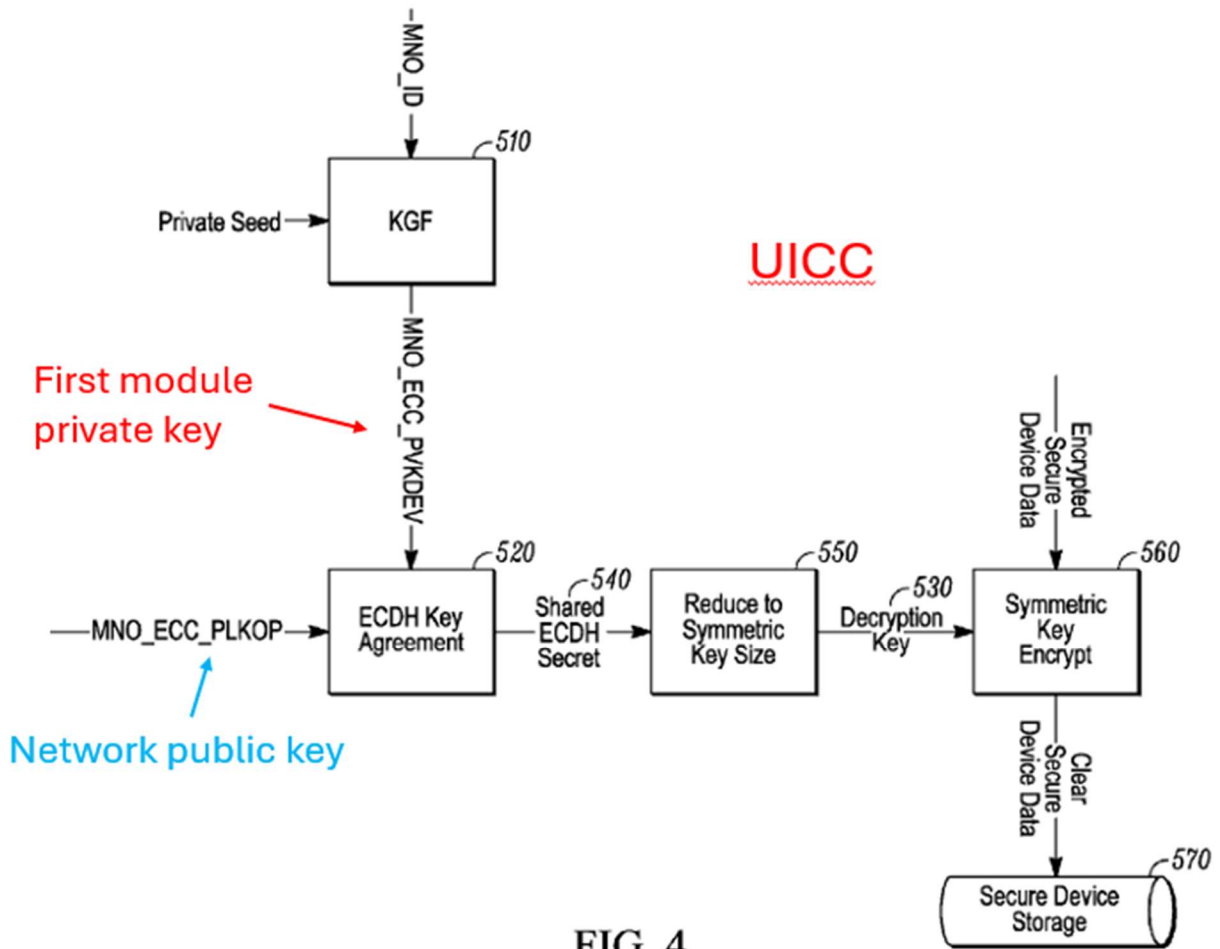


FIG. 4

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

(4) Storing the keys in an eUICC

90. 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). 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 these 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.

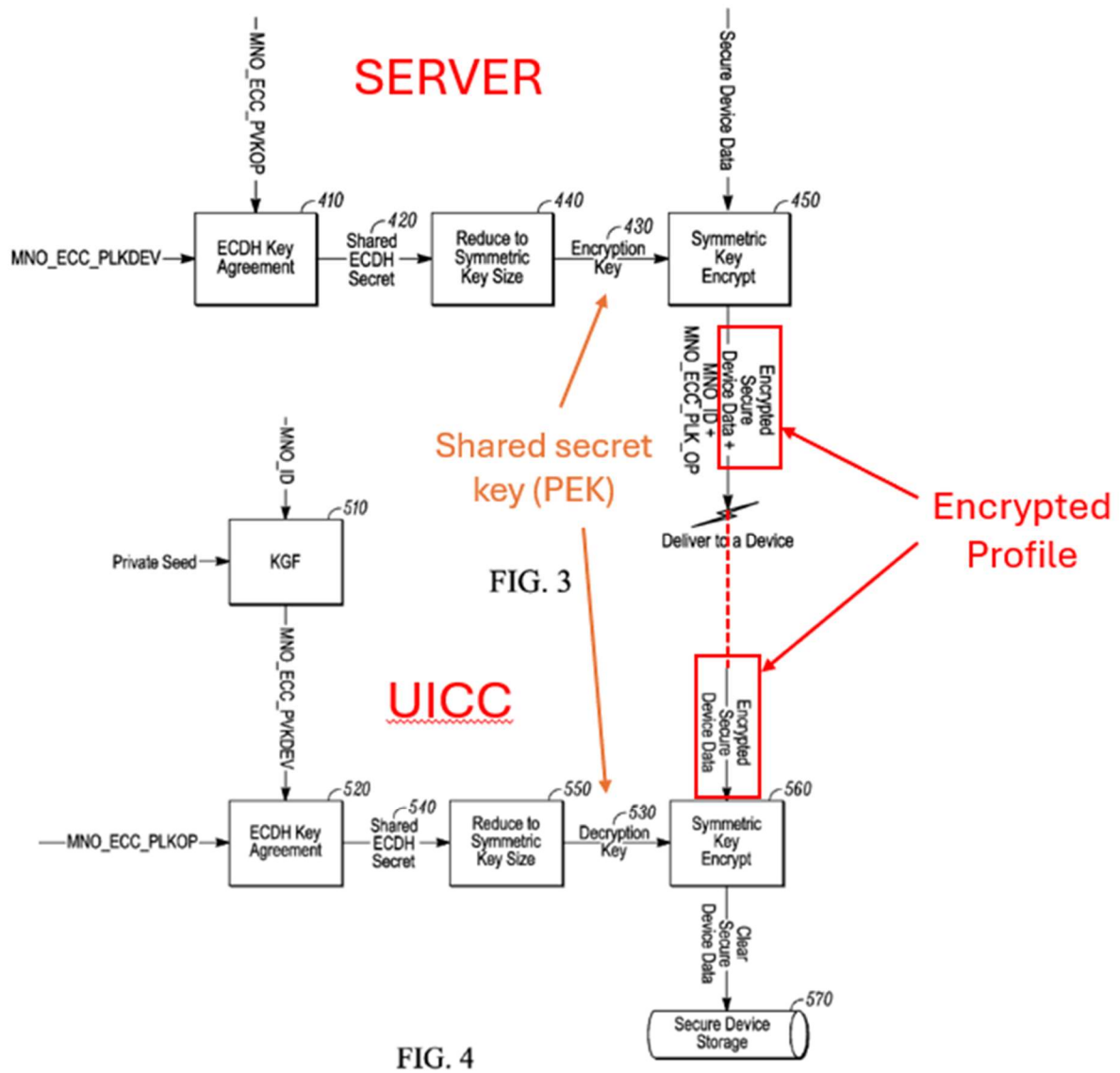
Claim element	Nakhjiri	Bradley	Jeong
First module private key, d_m^{1st}	MNO_ECC_PVKDEV		
First module public key, Q_m^{1st}	MNO_ECC_PLKDEV		
Network public key, Q_n	MNO_ECC_PLKOP		

- 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;**

91. In my opinion, Nakhjiri-Bradley-Jeong teaches Element 1(b).

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

92. 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. 3-4, below:



Nakhjiri’s PEK is the shared secret key key_{ssk} .

93. 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.”

(2) Encrypted profile comprises cryptographic parameters

94. 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).⁵

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

95. 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. *See, e.g.*, 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

⁵ 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.

least two module identities—the IMSI (international mobile subscriber ID) and an ICCID (integrated circuit card identification number).

96. Bradley teaches that “relevant subscription information [includes] the *IMSI*, *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.

97. 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. 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.

98. 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. 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 XI.A.1.

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;**

99. In my opinion, Nakhjiri-Bradley-Jeong teaches Element 1(c).

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 ECDH shared secret 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.

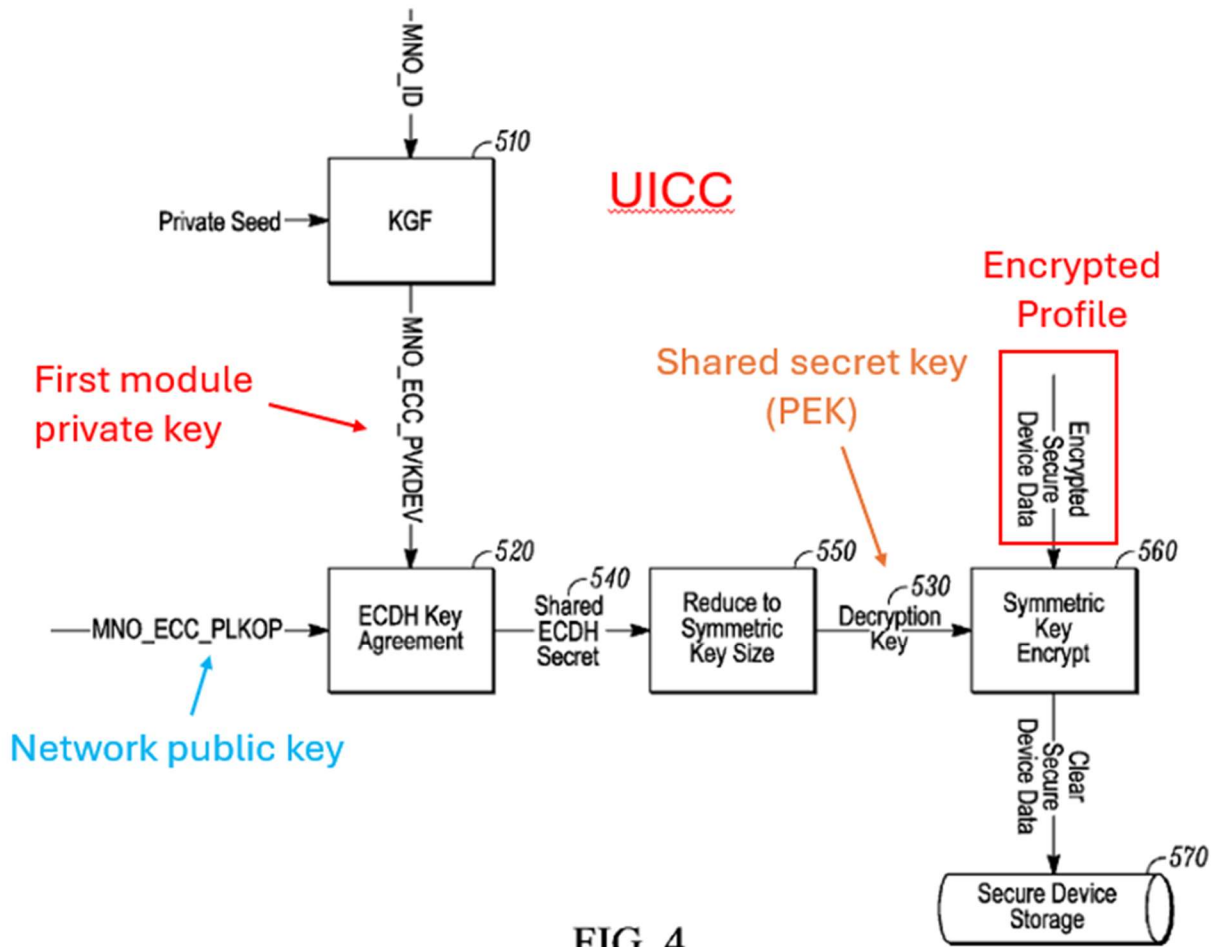


FIG. 4

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.

101. 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-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 and network public key.

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;**

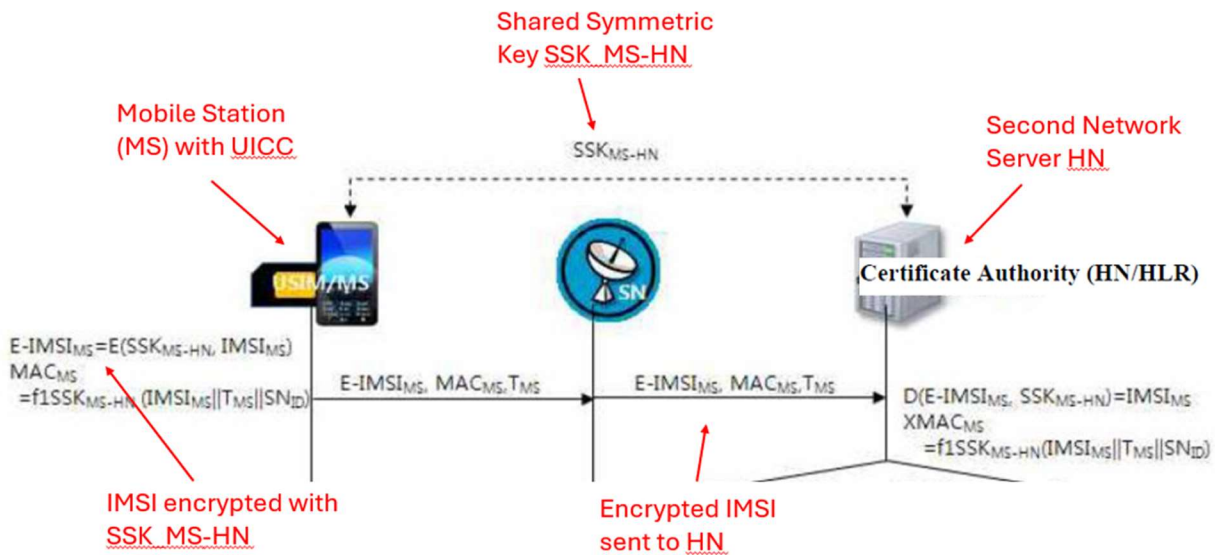
102. In my opinion, Nakhjiri-Bradley-Jeong teaches Element 1(d).

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 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;**

104. 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 key (what is claimed as “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”).



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.

105. 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 XI.A.1, it was well known in the art (as exemplified in 1(a)-(c)) to use ECDH to generate a shared secret. In claim 1(g), this second ECDH exchange results in “a symmetric key” or key_{SSK}^{2nd} .⁶

106. In my opinion, 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.

107. 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

⁶ 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-SSKMS-SN. It would have been obvious to a POSITA that the ECDH key agreement between MS and HN would proceed the same way it does between MS and SN. Thus, claim Elements 1(e), 1(f), and 1(g), below are described with reference to the ECDH exchange that takes place between MS and SN, understanding that the ECDH exchange between MS and HN would follow the same procedure.

would generate a public / private key pair (d_{MS} / Q_{MS}) for the ECDH exchange with HN. 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.

108. 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. Indeed, Jeong 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.* §4.1.3.⁷

⁷ 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.

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}

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

109. In my opinion, Nakhjiri-Bradley-Jeong teaches Element 1(f).

110. A POSITA would have understood that after generating its public/private key pair, MS would send its public key to the authentication server HN to continue the ECDH derivation process by generating its own copy of the second shared secret key, key_{SSK}^{2nd} (i.e., recited “symmetric key”).⁸ As Jeong

⁸ 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).

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.

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

111. In my opinion, Nakhjiri-Bradley-Jeong teaches Element 1(g).

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.⁹

113. Indeed, Jeong discloses “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. 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

⁹ Analogously, Jeong describes that for the MS-SN exchange, MS derives the SSK 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 (“ $SSK_{MS-SN} = EC-DH (P, MS, SNP)$ ”).

§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). A POSITA would have understood that “the initial point” P is a cryptographic parameter of the ECDH algorithm.

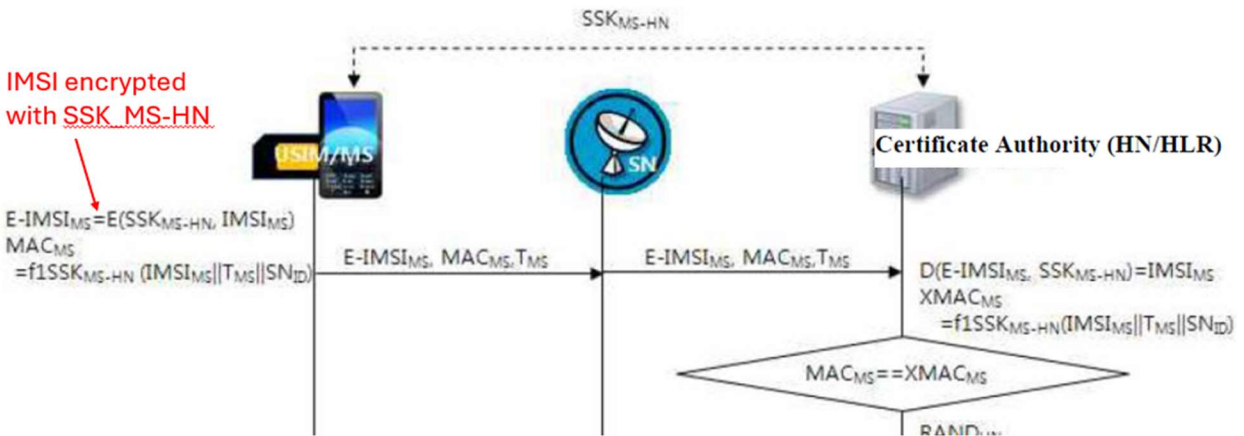
114. Thus, the “symmetric key” key_{SSK}^{2nd} would correspond to SSK_{MS-HN} .

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		
Shared secret key, key_{SSK}	Profile encrypted by PEK, includes curve ID and base point G	ICCID, IMSI, 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**

115. In my opinion, Nakhjiri-Bradley-Jeong teaches Element 1(h).

116. As shown in the excerpt of Figure 6 below, Jeong teaches that the MS prepares module encrypted data $E\text{-IMSI}_{MS} = E(SSK_{MS\text{-}HN}, IMSI_{MS})$, where the IMSI of MS is encrypted, “E(),” using $SSK_{MS\text{-}HN}$. 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 $SSK_{MS\text{-}HN}$* and transmitting it to the certificate authority.” Ex-1007 §4.1.2. Thus, Jeong discloses using the symmetric key $SSK_{MS\text{-}HN}$ to prepare module encrypted data comprising IMSI, the module identity.

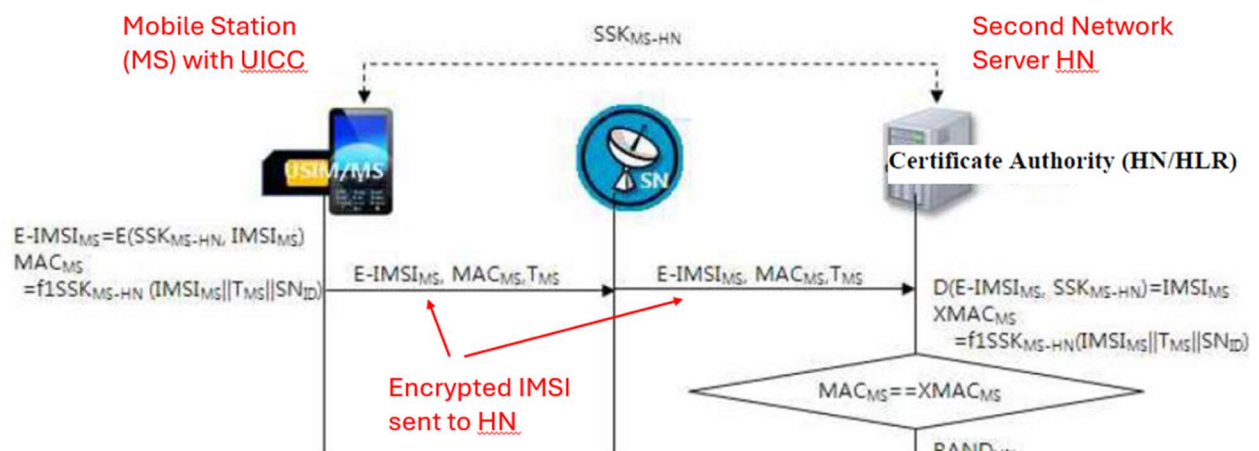


Claim element	Nakhjiri	Bradley	Jeong
First module public key, Q_m^{1st}	MNO_ECC_PVKDEV		
Network public key, Q_n	MNO_ECC_PLKDEV		
Encrypted profile with cryptographic parameters, ID, and key K	MNO_ECC_PLKOP		
Shared secret key, key_{SSK}	Profile encrypted by PEK, includes curve ID and base point G	ICCID,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

	and cryptographic keys		
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.

117. In my opinion, Nakhjiri-Bradley-Jeong teaches Element 1(i) for the reasons described in the previous section. 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:



118. 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.

119. Thus, in my opinion, 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).

120. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 2.

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.

122. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 3.

123. Bradley teaches that the module identity comprises a permanent identifier for the mobile device. Bradley teaches that “Device X is touched against

NFC token Y,” which “contains the ICCID and preferably also the ICCID’s activation code.” Ex-1006 ¶30. Bradley further teaches that “Device X reads the ICCID from token Y as well as (preferably) the ICCID’s secret activation code which is unique (this code prevents brute-force guessing of ICCID requests to the provisioning centre).” Ex-1006 ¶30. Device X 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 ¶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. For example, US 2021/0135491 to Bhuyan notes that a “unique identifier for the mobile device” is the “IMSI (international mobile subscriber identity.” Ex-1027 ¶59; *see also* US 2013/0012168 to Rajadurai, Ex-1008 ¶22; Ex-1025 (Semple) ¶26 (“[t]he IMSI is *a unique number* that is associated with an MT 102 in the network”); Ex-1026 (Wang) ¶15 (mobile device (WTRU) stores a user ID in the form of an IMSI); Ex-1028 (CSMG), 16 (“a SIM Card can have three identification data fields, each with its own specific purpose. These are *IMSI* (the ID of the card that is used for identification with the network), the MSISDN (the telephone number that is used to route incoming calls to the device) and the *ICCID*,

which is the serial number for that SIM card, often also physically printed onto the outside of the SIM card itself.”).

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

124. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 4.

125. 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.” *See, e.g.*, Ex-1025 (Semple) ¶¶33, 48; Ex-1024 (Gouget) ¶¶42-45. This is also taught by Bradley.

126. Bradley teaches that upon verifying the validity of the ICCID/secret activation code pairing, 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.

127. 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).

- 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.**

128. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 7.

129. 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

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

Calculated by MNO: Shared DH

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

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.

- 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.**

130. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 9.

131. As explained for Element 1[h], the Nakhjiri-Bradley-Jeong combination teaches generating the module encrypted data with the symmetric key. 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.

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

132. In my opinion, Nakhjiri-Bradley-Jeong Claim 10.

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 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 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.

134. While Jeong does not specify whether the symmetric key is used to encrypt the module data including IMSI (step h) before or after sending the second module public key to the second server (step f), it would have been a simple matter of design choice regarding whether to encrypt IMSI and then send the second module public key or to first send the second module public key and then encrypt IMSI.

However, it may have made more sense to first encrypt IMSI (step h) and then send MSP to the second server (step f) because the encrypted IMSI is also sent to the second server and it would make sense to send them in the same message to minimize communication transactions.

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

135. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 11.

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.

137. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 12.

138. 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.”

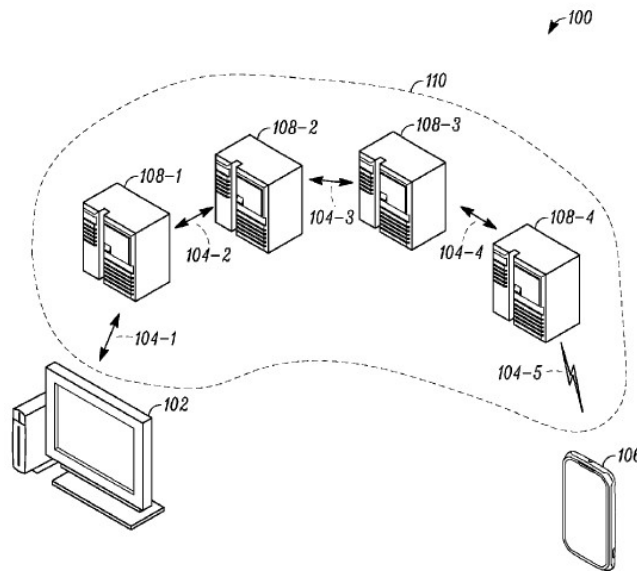


FIG. 1

- 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.**

139. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 13.

140. 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. “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.

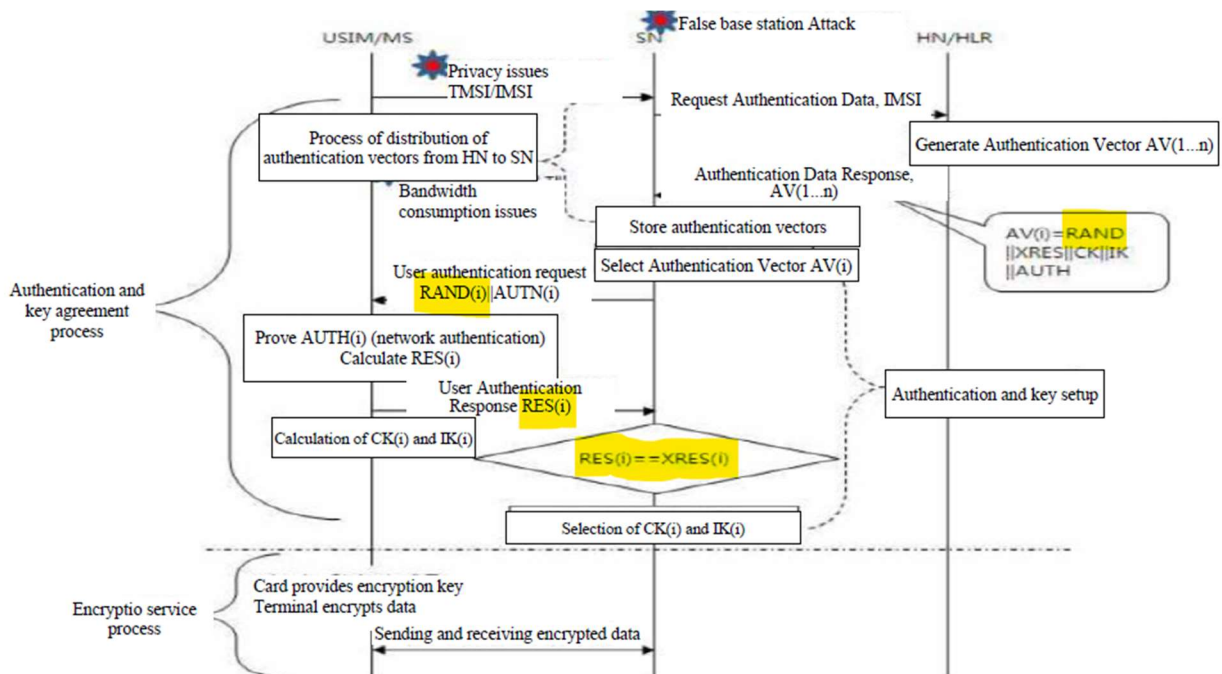


Figure 2. 3GPP-AKA Mutual Authentication Flow [10]

141. 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.

- 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.**

142. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 14.

143. 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. 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.¹⁰ Thus, Nakhjiri-Bradley-Jeong renders Claim 14 obvious.

¹⁰ 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

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.

144. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 16.

145. 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

per se; it proposes an alternative (key list secrecy). Selecting certificate-based verification for a smaller operator set remains an obvious, expressly taught option.

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.

146. As explained for 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.*”).

147. 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.

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

148. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 17.

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.

150. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 18.

151. 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.”¹¹ 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

¹¹ 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.

POSITA would have understood these parameters to be base points or starting points for an elliptic curve used in the ECDH algorithm.

- 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.**

152. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 19.

153. 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.**

154. In my opinion, Nakhjiri-Bradley-Jeong teaches Claim 20.

155. 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.

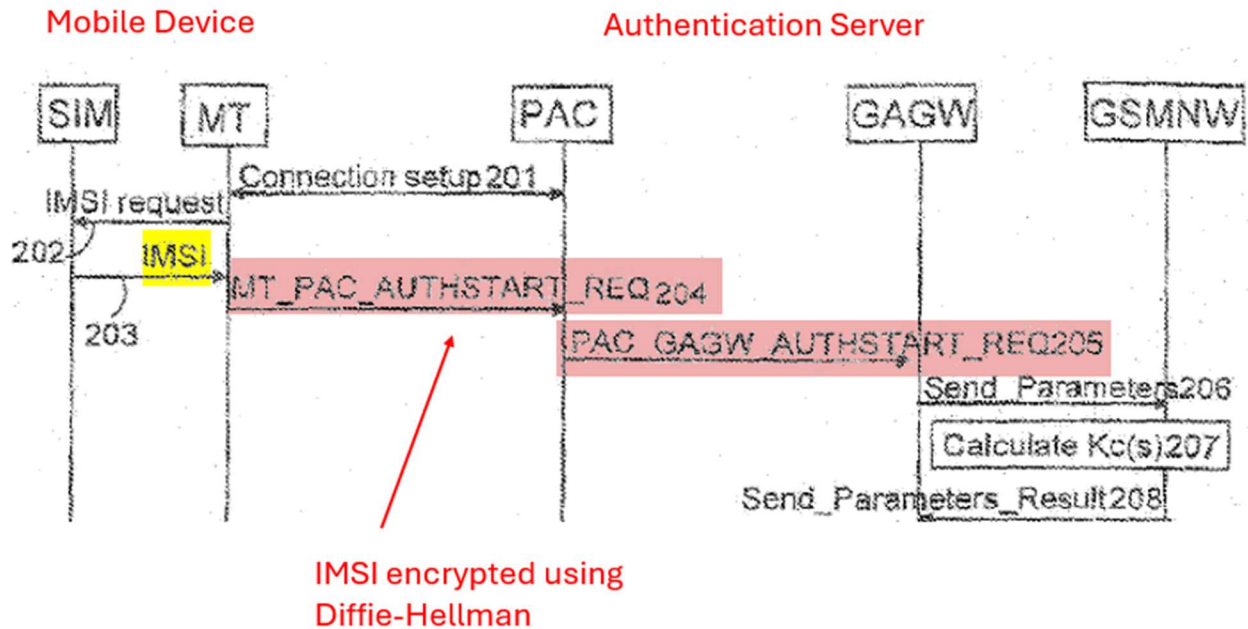
- B. Ground 2: Claims 1-4, 7, 9-14, and 16-20 are obvious over Nakhjiri in view of Bradley and Ala-Laurila**

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

156. A POSITA would have been motivated to combine Nakhjiri-Brdley’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 are complementary, well-understood steps within the same problem space (securing subscriber credentials and identifiers over untrusted links), and apply the same DH/ECDH mechanism to two adjacent phases of the lifecycle. Each reference expressly targets secure delivery/authentication of subscriber credentials in mobile environments and uses DH/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-1013 ¶¶22–26, 28.

157. As described above for Ground 1, Nakhjiri-Bradley teach 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.



158. Ala-Laurila teaches that the message from the MT is an authentication start request that includes a network access identifier NAI, which “comprises the IMSI identifier obtained from the identity module SIM.” Ex-1013 ¶26. Ala-Laurila further teaches that the request “is preferably sent *in ciphered form* to the PAC *using the Diffie-Hellman algorithm.*” Ex-1013 ¶26. Ala-Laurila thus teaches sending an authentication message including the IMSI encrypted with a Diffie-Hellman key, as recited in steps 1(e)-1(i).

2. Independent Claim 1

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

159. In my opinion, 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.

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

160. In my opinion, Nakhjiri-Bradley-Ala-Laurila teaches Element 1(e).

161. 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").

162. 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. Specifically, a POSITA would have understood, at least from Nakhjiri's ECDH key exchange

teachings, that for the mobile device and authentication server to derive a module public/private key pair, the mobile device (UICC) would send the module public key to the authentication server, and would use its own module private key (and the authentication server public key) to generate the Diffie-Hellman symmetric key. Thus, in the Nakhjiri-Bradley-Ala-Laurila combination, Nakhjiri's process where "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)" 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 (using instead the authentication server ID) for mutual authentication with the PAC/GAGW servers, as taught by Ala-Laurila.

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

163. In my opinion, Nakhjiri-Bradley-Ala-Laurila teaches Element 1(f) for the reasons described in the previous limitation.

164. 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” that 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 ¶¶22-26. The PAC and GAGW performs authentication and corresponds to the recited “second server.” In the Nakhjiri-Bradley-Ala-Laurila combination, Nakhjiri’s Diffie-Hellman key exchange process would be modified 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.

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

165. In my opinion, Nakhjiri-Bradley-Ala-Laurila teaches Element 1(g) for the reasons described for Elements 1(e)-1(f). A POSITA would have used Nakhjiri’s ECDH procedure to create the symmetric key Ala-Laurila uses to encrypt IMSI. Ex-1013 ¶¶22-23, 25-26. Specifically, a POSITA would have understood from Nakhjiri’s Diffie-Hellman key exchange teachings to generate the Diffie-Hellman symmetric key with the second module private key and the cryptographic parameters. 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

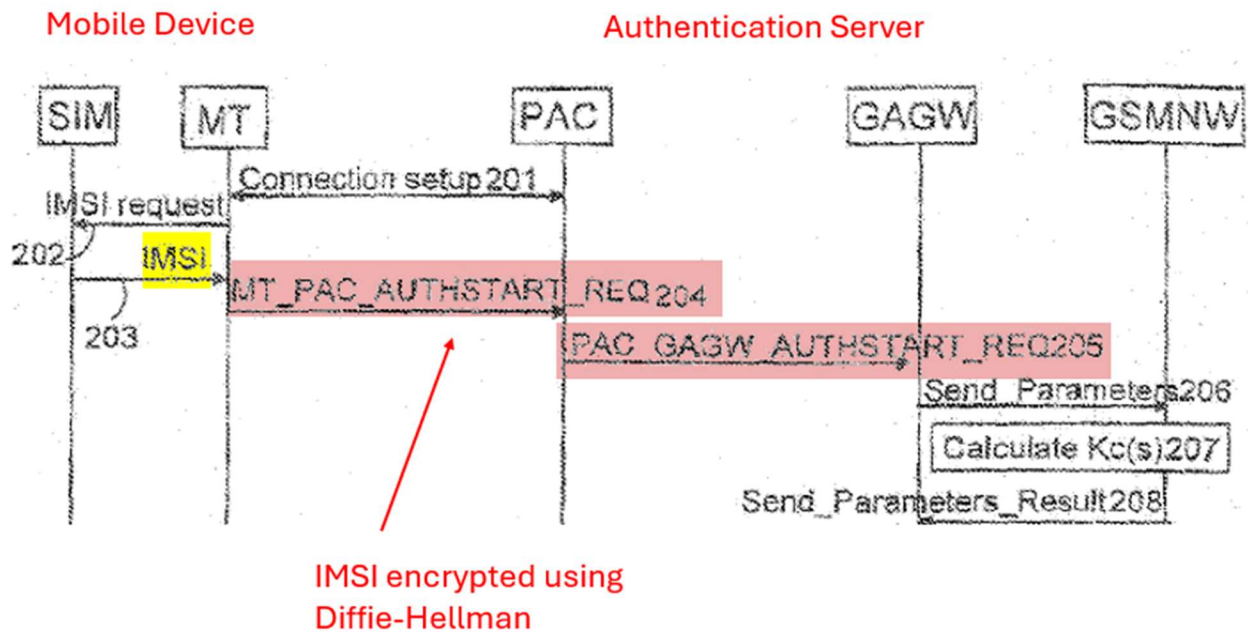
authentication server, as taught by Ala-Laurila, (instead of the MNO provisioning server, as taught by Nakhjiri), using the same elliptic curve Diffie-Hellman process. Using the same ECC parameters (curve/base point G) as provided in the profile (Ex-1005, 4:51–56) satisfies ‘cryptographic parameters’; the ECDH yields the symmetric key used for subsequent encryption. Ex-1013 ¶26.

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

166. In my opinion, Nakhjiri-Bradley-Ala-Laurila teaches Element 1(h).

167. 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. Ala-Laurila teaches that “[t]he 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.” 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 limitations 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. In the Nakhjiri-Bradley-Ala-Laurila combination, the IMSI sent from the MT to the PAC (and GAGW) would be encrypted using the symmetric key derived using the elliptic curve Diffie-Hellman process described above, as taught by Ala-Laurila and Nakhjiri. Ex-1013, Fig. 2.



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

168. In my opinion, Nakhjiri-Bradley-Ala-Laurila teaches Element 1(i) for the reasons described in the previous section. 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.

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

170. In my opinion, 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.

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

171. In my opinion, Nakhjiri-Bradley-Ala-Laurila teaches Claim 10.

172. 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. For example, SEC1 contemplates ephemeral ECDH keys and precomputation. Ex-1011, §§3.3, 3.6 (pp. 31–33, 56–57); *see also* Ex-1014, 12 (showing ephemeral key generation). Applying that to authentication yields steps (g) and (h) before sending (f).

173. 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. 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.

- 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.**

174. In my opinion, Nakhjiri-Bradley-Ala-Laurila teaches Claim 13.

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.

176. In my opinion, Nakhjiri-Bradley-Ala-Laurila teaches Claim 16.

177. 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 XI.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. 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.

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’s teachings

with X9.63-Overview’s teachings and would have had a reasonable expectation of success.

178. 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* Section XI.A.1.

179. 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)¹² (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. 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 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. 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

¹² 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.

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.

180. 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.

181. 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. 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* Section XI.A.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.

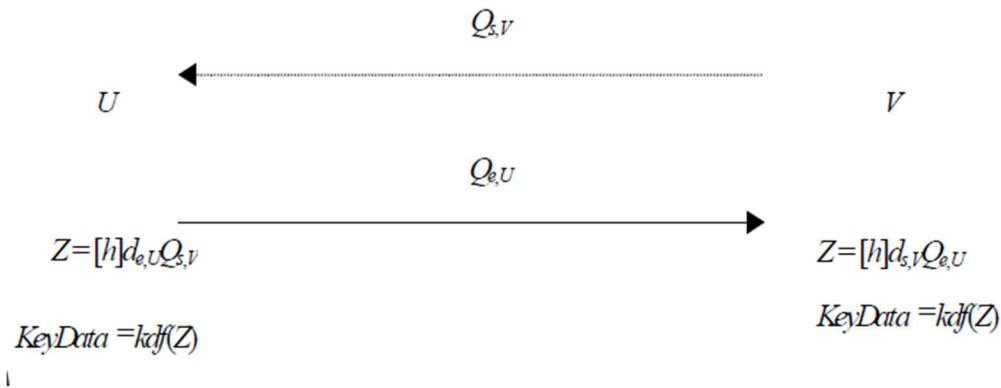
2. Dependent Claims 5-6

- 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.**

182. In my opinion, Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila in view of X9.63-Overview teaches Claim 5.

183. 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. 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).

184. 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.

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.

185. In my opinion, Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila with X9.63-Overview teaches Claim 6.

186. As explained in Grounds 1 and 2 for Element 1(g), the Jeong and Ala-Laurila teach deriving a symmetric key using a second ECDH exchange with a

second (authentication) server. 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.

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.**

187. 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.

188. 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.

189. A POSITA would have had a reasonable expectation of success Nakhjiri-Bradley-Jeong or Nakhjiri-Bradley-Ala-Laurila with Pierce. All describe methods for securing wireless communications using authentication and key agreement mechanisms. *See* Section XI.A.1 and XI.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.

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.**

190. 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. 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.

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

191. 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.

192. 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.

XII. CONCLUSION

193. For the reasons above, it is my opinion that Claims 1-20 of the '869 Patent are obvious based on each of the grounds specified in my Declaration.

194. I declare that all statements made in my Declaration of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: November 20, 2025



Dr. Sundeep Rangan