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. IPR2026-00119
U.S. Patent No. 11,916,893

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,916,893

TABLE OF CONTENTS

Page

I. INTRODUCTION 1
II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8 1
III. FEE AUTHORIZATION 3
IV. GROUNDS FOR STANDING 3
V. PRECISE RELIEF REQUESTED 3
VI. THE CHALLENGED PATENT 4
VII. PROSECUTION HISTORY OF THE '893 PATENT 8
VIII. LEVEL OF ORDINARY SKILL IN THE ART 9
IX. PRIORITY DATE 9
X. CLAIM CONSTRUCTION 10
XI. BRIEF DESCRIPTION OF THE APPLIED PRIOR ART 10
A. Park (Ex-1005) 10
B. GlobalPlatform (Ex-1006) 12
C. AbiChar (Ex-1007) 15
D. X9.63-Overview (Ex-1008) 15
E. Haggerty (Ex-1012) 17
F. Pierce (Ex-1013) 18
G. Konstantinou (Ex-1014) 18
H. Nix175 (Ex-1016) 19
XII. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS 19
A. Ground 1: Claims 1, 3, 6-11, 13-17 are obvious over Park in view of GlobalPlatform and AbiChar 19
1. A POSITA would have been motivated to combine Park's teachings with GlobalPlatform's and AbiChar's teachings and would have had a reasonable expectation of success 19

TABLE OF CONTENTS
(continued)

Page

a. A POSITA would have turned to GlobalPlatform for implementation-level details of Park's security requirements. 20

b. A POSITA would have understood that Abi-Char's elliptic curve Diffie-Hellman key agreement could be implemented within Park's SPA to provide an efficient asymmetric key-exchange mechanism.....23

2. Independent Claim 1 26

a. 1[pre]: A mobile device for communicating with a wireless network, the mobile device comprising: 26

b. 1[a]: a first memory configured to store an embedded universal integrated circuit card (eUICC) identity; 28

c. 1[b]: a random number generator operably connected to a processor connected to a second memory configured to generate a random number for an eUICC private key corresponding to an eUICC public key; 31

d. 1[c]: a radio including one or more transmit antennas and one or more receiving antennas configured to: 34

e. 1[c][1]: a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and.....35

f. 1[c][2]: b. receive, from the subscription manager, i) an eUICC profile comprising network parameters, a key K, and a subscriber identity and ii) a symmetric key; andA 37

g. 1[d]: an eUICC associated with the eUICC identity and configured to 41

h. 1[d][1]: a. derive a profile key using an elliptic curve Diffie-Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key; 41

TABLE OF CONTENTS
(continued)

Page

i. 1[d][2]: b. decrypt a first portion of the eUICC profile using the profile key; 43

j. 1[d][3]: c. receive the symmetric key from a network application operating in the mobile device;.....44

k. 1[d][4]: d. decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising the key K and the subscriber identity, wherein the first portion and the second portion are distinct; and 45

l. 1[d][5]: e. generate a response value for authentication of the mobile device with the wireless network using the key K.....47

3. Dependent Claims 3, 6-11, 13-17 48

a. Claim 3: The mobile device of claim 1, wherein the eUICC operates within a universal integrated circuit card within the mobile device. 48

b. Claim 6: The mobile device of claim 1, wherein the network application is configured to communicate with i) the wireless network and ii) the eUICC in the mobile device using a system bus.....48

c. Claim 7: The mobile device of claim 1, wherein the eUICC comprises computer executable instructions for a processor in the mobile device, and wherein the computer executable instructions are stored within the memory. 49

d. Claim 8: The mobile device of claim 1, wherein the eUICC comprises a package soldered onto a circuit board of the mobile device. 50

TABLE OF CONTENTS
(continued)

Page

e. Claim 9: The mobile device of claim 1, further comprising a user interface configured to receive user identification information before the mobile device receives the symmetric key. 50

f. Claim 10: The mobile device of claim 1, wherein the first portion of the eUICC profile includes the network parameters, the network parameters comprising a list of numbers associated with a mobile network operator. 51

g. Claim 11: The mobile device of claim 1, wherein the network parameters comprise a mobile country code (MCC) and a mobile network code (MNC) associated with the wireless network. 52

h. Claim 13: The mobile device of claim 1, wherein the subscriber identity comprises an International Mobile Subscriber Identity (IMSI). 52

i. Claim 14: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, a ciphertext for the symmetric key, wherein the mobile device is configured to decrypt the ciphertext using at least the eUICC private key. 52

j. Claim 15: The mobile device of claim 1, wherein the mobile device further comprises at least one of a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a tracking device, and a circuit board with the radio. 53

k. Claim 16: The mobile device of claim 1, wherein the second memory is the same memory as the first memory. 54

l. Claim 17: The mobile device of claim 1, wherein the one or more receiving antennas are the one or more transmit antennas. 55

TABLE OF CONTENTS
(continued)

Page

B. Ground 2: Claims 1, 3, 6-11, 13-17 are obvious over Park in view of GlobalPlatform and X9.63-Overview 55

1. A POSITA would have been motivated to combine Park's teachings with GlobalPlatform's and X9.63-Overview's teachings and would have had a reasonable expectation of success. 55

2. Independent Claim 1 57

a. 1[pre]-1[a], 1[c], 1[c][2]-1[d], 1[d][2]-1[d][5]: 57

b. 1[b]: a random number generator operably connected to a processor connected to a second memory configured to generate a random number for an eUICC private key corresponding to an eUICC public key; 57

c. 1[c][1]: a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and 59

d. 1[d][1]: a. derive a profile key using an elliptic curve Diffie-Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key; 60

3. Dependent Claims 3, 6-11, 13-17 61

C. Ground 3: Claims 2 and 12 are obvious over Grounds 1 or 2 in view of Haggerty 61

1. A POSITA would have been motivated to add Haggerty to Park-GlobalPlatform-AbiChar or Park-GlobalPlatform-X9.63-Overview and would have had a reasonable expectation of success. 61

2. Claim 2: The mobile device of claim 1, wherein the eUICC is further configured to receive a profile identity for the eUICC profile as a plaintext. 64

3. Claim 12: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, the eUICC profile using transport layer security.

TABLE OF CONTENTS
(continued)

Page

.....65

D. Ground 4: Claims 4-5 are obvious over Grounds 1 or 2 in view of Pierce.....65

1. A POSITA would have been motivated to add Pierce to Park-GlobalPlatform-AbiChar, or Park-GlobalPlatform-X9.63-Overview and would have had a reasonable expectation of success.....65

2. Claim 4: The mobile device of claim 1, wherein the random number generator is configured to generate the random number in response to input from at least one of a clock and a sensor. 67

Claim 5: The mobile device of claim 1, wherein the random number generator is configured to generate the random number from a seed value, wherein the seed value comprises data from at least one of a sensor, the radio, a bus, a clock, a physical interface, the memory, and an operating system. 67

E. Ground 5: Claims 10-11 are obvious over Grounds 1 or 2 in view of Konstantinou 67

1. A POSITA would have been motivated to add Konstantinou to Park-GlobalPlatform-AbiChar, or Park-GlobalPlatform-X9.63-Overview, and would have had a reasonable expectation of success.....67

2. Claim 10: The mobile device of claim 1, wherein the first portion of the eUICC profile includes the network parameters, the network parameters comprising a list of numbers associated with a mobile network operator.....68

Claim 11: The mobile device of claim 1, wherein the network parameters comprise a mobile country code (MCC) and a mobile network code (MNC) associated with the wireless network.....68

F. Ground 6: Claims 1-17 are obvious over Nix175 in view of Park and GlobalPlatform 68

TABLE OF CONTENTS
(continued)

Page

1. A POSITA would have been motivated to combine Nix175, Park, and GlobalPlatform and would have had a reasonable expectation of success.....68
2. Independent Claim 1 75
   a. 1[pre]: A mobile device for communicating with a wireless network, the mobile device comprising: 75
   b. 1[a]: a first memory configured to store an embedded universal integrated circuit card (eUICC) identity; 76
   c. 1[b]: a random number generator operably connected to a processor connected to a second memory configured to generate a random number for an eUICC private key corresponding to an eUICC public key; 76
   d. 1[c]: a radio including one or more transmit antennas and one or more receiving antennas configured to: 78
   e. 1[c][1]: a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and.....78
   f. 1[c][2]: b. receive, from the subscription manager, i) an eUICC profile comprising network parameters, a key K, and a subscriber identity and ii) a symmetric key; and 79
   g. 1[d]: an eUICC associated with the eUICC identity and configured to 83
   h. 1[d][1]: a. derive a profile key using an elliptic curve Diffie-Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key; 83
   i. 1[d][2]: b. decrypt a first portion of the eUICC profile using the profile key; 84

TABLE OF CONTENTS
(continued)

Page

j. 1[d][3]: c. receive the symmetric key from a network application operating in the mobile device;.....85

k. 1[d][4]: d. decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising the key K and the subscriber identity, wherein the first portion and the second portion are distinct; and.....86

l. 1[d][5]: e. generate a response value for authentication of the mobile device with the wireless network using the key K.....88

3. Dependent Claims 2-17.....89

a. Claim 2: The mobile device of claim 1, wherein the eUICC is further configured to receive a profile identity for the eUICC profile as a plaintext. 89

b. Claim 3: The mobile device of claim 1, wherein the eUICC operates within a universal integrated circuit card within the mobile device. 90

c. Claim 4: The mobile device of claim 1, wherein the random number generator is configured to generate the random number in response to input from at least one of a clock and a sensor.....91

Claim 5: The mobile device of claim 1, wherein the random number generator is configured to generate the random number from a seed value, wherein the seed value comprises data from at least one of a sensor, the radio, a bus, a clock, a physical interface, the memory, and an operating system. 91

d. Claim 6: The mobile device of claim 1, wherein the network application is configured to communicate with i) the wireless network and ii) the eUICC in the mobile device using a system bus.....91

TABLE OF CONTENTS
(continued)

Page

e. Claim 7: The mobile device of claim 1, wherein the eUICC comprises computer executable instructions for a processor in the mobile device, and wherein the computer executable instructions are stored within the memory. 92

f. Claim 8: The mobile device of claim 1, wherein the eUICC comprises a package soldered onto a circuit board of the mobile device. 92

g. Claim 9: The mobile device of claim 1, further comprising a user interface configured to receive user identification information before the mobile device receives the symmetric key. 92

h. Claim 10: The mobile device of claim 1, wherein the first portion of the eUICC profile includes the network parameters, the network parameters comprising a list of numbers associated with a mobile network operator. Claim 11: The mobile device of claim 1, wherein the network parameters comprise a mobile country code (MCC) and a mobile network code (MNC) associated with the wireless network. 93

i. Claim 12: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, the eUICC profile using transport layer security. 94

j. Claim 13: The mobile device of claim 1, wherein the subscriber identity comprises an International Mobile Subscriber Identity (IMSI). 94

a. Claim 14: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, a ciphertext for the symmetric key, wherein the mobile device is configured to decrypt the ciphertext using at least the eUICC private key. 94

TABLE OF CONTENTS
(continued)

Page

b. Claim 15: The mobile device of claim 1, wherein the mobile device further comprises at least one of a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a tracking device, and a circuit board with the radio. 95

c. Claim 16: The mobile device of claim 1, wherein the second memory is the same memory as the first memory. 95

d. Claim 17: The mobile device of claim 1, wherein the one or more receiving antennas are the one or more transmit antennas. 96

XIII. CONCLUSION 96

LIST OF EXHIBITS[1]

Ex. No.	Description
Ex-1001	U.S. Patent No. 11,916,893 ("the '893 Patent)
Ex-1002	Declaration of Dr. Paul S. Min
Ex-1003	Curriculum Vitae of Dr. Paul S. Min
Ex-1004	Prosecution History of U.S. Patent No. 11,916,893
Ex-1005	Jaemin Park et al., Secure Profile Provisioning Architecture for Embedded UICC, Int'l Conference on Availability, Reliability & Security 297 (2013) ("Park")
Ex-1006	GlobalPlatform Card Specification, Version 2.2.1, Public Release (Jan. 2011) ("GlobalPlatform")
Ex-1007	Pierre E. Abi-Char et al., A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications, Int'l Conference on Next Generation Mobile Applications, Services and Technologies (2007) ("AbiChar")
Ex-1008	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000) ("X9.63-Overview")
Ex-1009	INTENTIONALLY LEFT BLANK
Ex-1010	INTENTIONALLY LEFT BLANK
Ex-1011	GlobalPlatform Card Secure Channel Protocol '11' Card Specification v2.2 – Amendment F, Version 1.0 (May 2015) ("SCP11")

[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-1012	U.S. Patent Pub. No. 2013/0227646 to Haggerty ("Haggerty")
Ex-1013	U.S. Patent Pub. No. 2009/0323967 to Pierce ("Pierce")
Ex-1014	U.S. Patent Pub. No. 2010/0267383 to Konstantinou ("Konstantinou")
Ex-1015	Declaration of Simon Blake-Wilson, author of ANSI X9.63-Overview
Ex-1016	U.S. Patent No. 9,100,175 ("Nix175")
Ex-1017	INTENTIONALLY LEFT BLANK
Ex-1018	Declaration of Tono Aspinall of GlobalPlatform, Inc.
Ex-1019	Declaration of Gordan MacPherson of IEEE
Ex-1020	Claim Mapping Table
Ex-1021	Colin Boyd and Anish Mathuria, "Protocols for Authentication and Key Establishment" (Springer, 2003) ("Boyd & Mathuria")
Ex-1022	Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, 22 IEEE Trans. Info. Theory 644 (1976)
Ex-1023	NIST, SP 800-57, Recommendation for Key Management: Part 1 — General (Rev. 3) (July 2012)
Ex-1024	NIST, SP 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping (Dec. 2012).
Ex-1025	NIST, SP 800-56A, Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (May 2013)
Ex-1026	GlobalPlatform Card Technology, Secure Channel Protocol 03, Card Specification v 2.2 – Amendment D, Version 1.0 (Apr. 2009)

Ex. No.	Description
Ex-1027	Reprogrammable SIMs: Technology, Evolution and Implications, Final Report, Ofcom (Sept. 25, 2012)
Ex-1028	ETSI TS 103 383 v12.1.0, "Smart Cards; Embedded UICC; Requirements Specification (Release 12)," (June 2013)
Ex-1029	Network-1's Infringement Contentions for the '893 Patent, filed on September 30, 2025, as Exhibit C to Network-1 Technologies, Inc.'s P.R. 3-1 Disclosure of Asserted Claims and Infringement Contentions

I. INTRODUCTION

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Petitioner") request *inter partes* review ("IPR") of Claims 1-17 of U.S. Patent No. 11,916,893 ("the '893 Patent") (Ex-1001), currently assigned to Network-1 Technologies, Inc. ("PO").

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

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

Related Matters: PO has asserted the '893 Patent against Petitioner in *Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd. et al.*, No. 2:25-cv-00667 (E.D. Tex.) ("Samsung litigation").

Lead and Back-Up Counsel:

- Lead Counsel:

  William M. Fink (Reg. No. 72,332)
  O'Melveny & Myers LLP
  1625 Eye Street, NW
  Washington, DC 20006
  Telephone: (202) 383-5300
  Fax: (202) 383-5414
  Email: tfink@omm.com

- Back-Up Counsel:

  Benjamin M. Haber (Reg. No. 67,129)
  O'Melveny & Myers LLP
  400 South Hope Street, 19th Floor
  Los Angeles, CA 90071

Telephone: (213) 430-6000
Fax: (213) 430-6407
Email: bhaber@omm.com

Marc J. Pensabene (Reg. No. 37,416)
O'Melveny & Myers LLP
1301 Avenue of the Americas, Suite 1700
New York, NY 10019
Telephone: (212) 326-2000
Fax: (212) 326-2061
Email: mpensabene@omm.com

Brian Cook (Reg. No. 59,356)
O'Melveny & Myers LLP
400 South Hope Street, 19th Floor
Los Angeles, CA 90071
Telephone: (213) 430-6000
Fax: (213) 430-6407
Email: bcook@omm.com

Caitlin P. Hogan (Reg. No. 61,515)
O'Melveny & Myers LLP
1301 Avenue of the Americas, Suite 1700
New York, NY 10019
Telephone: (212) 326-2000
Fax: (212) 326-2061
Email: chogan@omm.com

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

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

III. FEE AUTHORIZATION

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

IV. GROUNDS FOR STANDING

Petitioner certifies that the '893 Patent is available for review, and Petitioner is not barred or estopped from requesting review.

V. PRECISE RELIEF REQUESTED

Petitioner requests review and cancellation of Claims 1-17 as unpatentable based on the following grounds, supported by a declaration from Dr. Paul S. Min. Ex-1002 ¶¶1-83; Ex-1003.

Ground	Summary
1	Claims 1, 3, 6-11, and 13-17 are obvious over Park (Ex-1005) in view of GlobalPlatform (Ex-1006) and AbiChar (Ex-1007)
2	Claims 1, 3, 6-11, and 13-17 are obvious over Park in view of GlobalPlatform and X9.63-Overview (Ex-1008)
3	Claims 2 and 12 are obvious over Grounds 1 or 2 in view of Haggerty (Ex-1012)
4	Claims 4-5 are obvious over Grounds 1 or 2 in view of Pierce (Ex-1013)
5	Claims 10-11 are obvious over Grounds 1 or 2 in view of Konstantinou (Ex-1014)
6	Claims 1-17 are obvious over Nix175 (Ex-1016) in view of Park and GlobalPlatform

VI. THE CHALLENGED PATENT

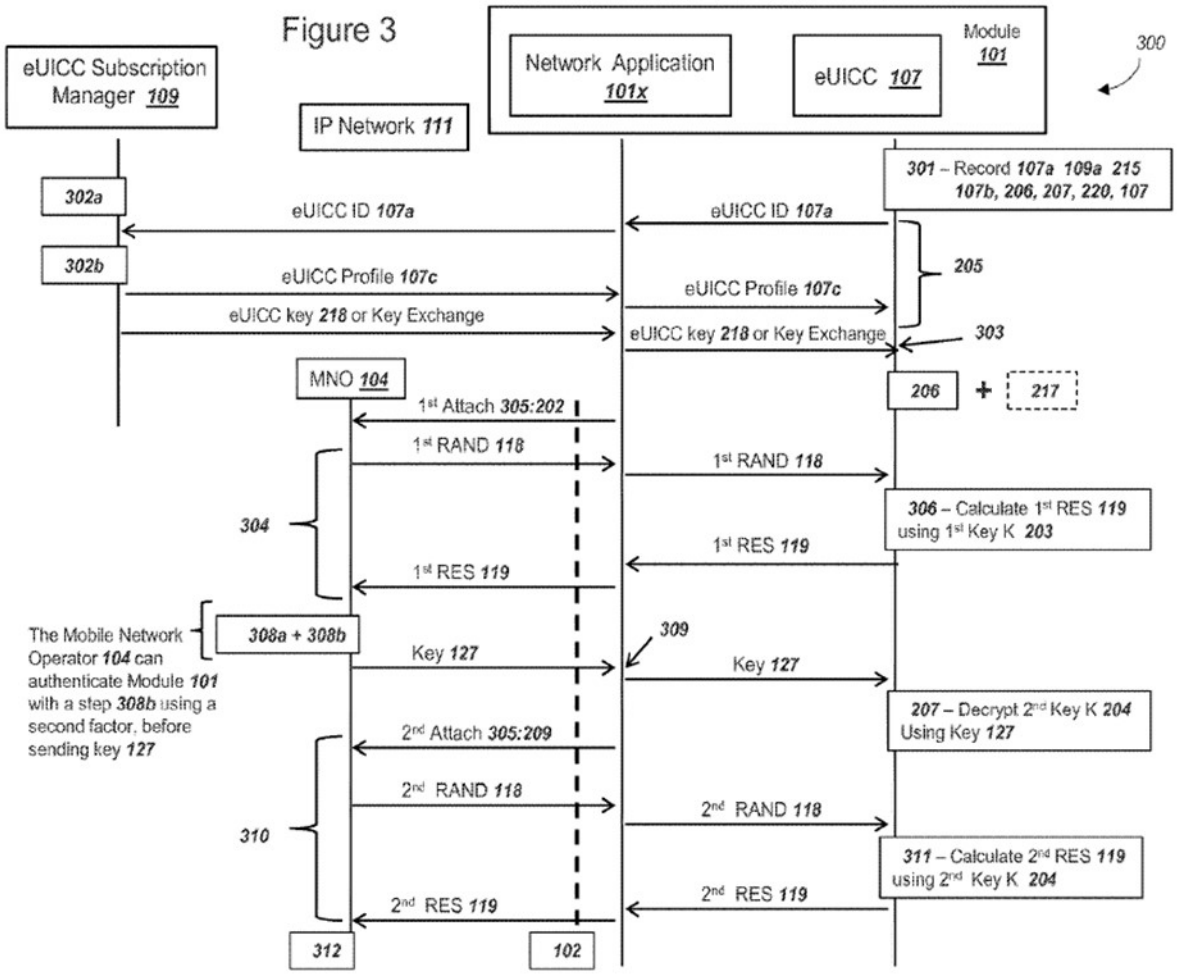
The '893 Patent describes provisioning an embedded universal integrated circuit card (eUICC) with a profile containing network access credentials. Ex-1001, 3:55-67.

As the '893 Patent explains, mobile devices traditionally relied on a "subscriber identity module (SIM) card" or "universal integrated circuit card (UICC)" to access a wireless network. Ex-1001, 2:34-45. Each card was supplied by a mobile network operator (MNO) and contained "a pre-shared secret key K in addition to a set of parameters for a mobile phone or user equipment to connect with the wireless network operated by the MNO." Ex-1001, 2:45-49. Because each card only allowed access to the network of its associated MNO, changing networks required "swapping the UICC card," the cost of which "could be prohibitive." Ex-1001, 3:1-15. This led the industry "to consider an embedded UICC" (eUICC), onto which new MNO network access credentials could be transferred, without physically swapping out the UICC. Ex-1001, 3:16-20.

The '893 Patent purports to address a security concern with this new provisioning system, where the distribution and release of the profile (including decryption of a secret key K) is under the control of the SM—and not the MNO, which thus loses control over ensuring its secret key K is only provided to authorized devices. Ex-1001, 3:59-64, 35:38-49. To address this issue, the '893 Patent describes

a multi-stage provisioning process illustrated in Figure 3, below, splitting control between the SM (for profile delivery) and the MNO (for decryption of secret key K).

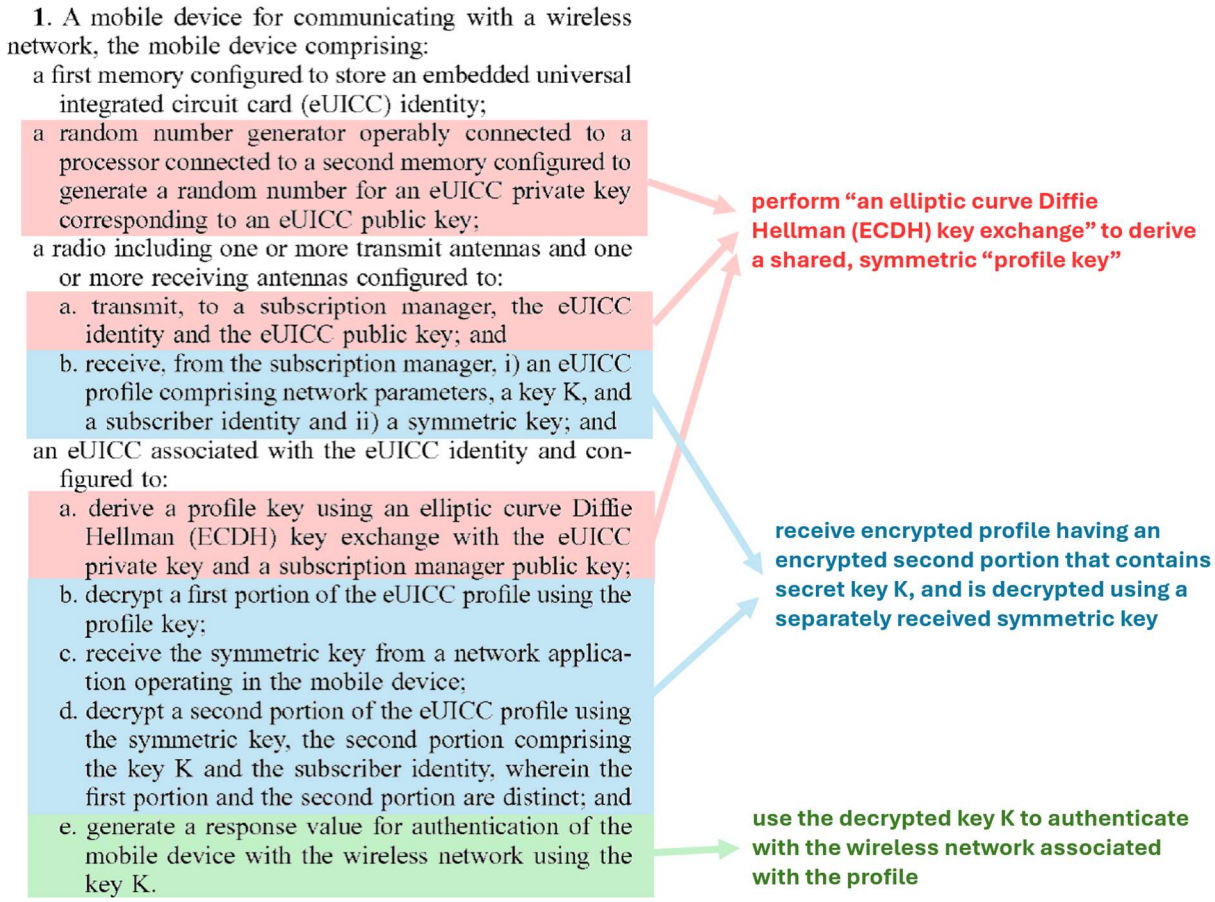
Figure 3



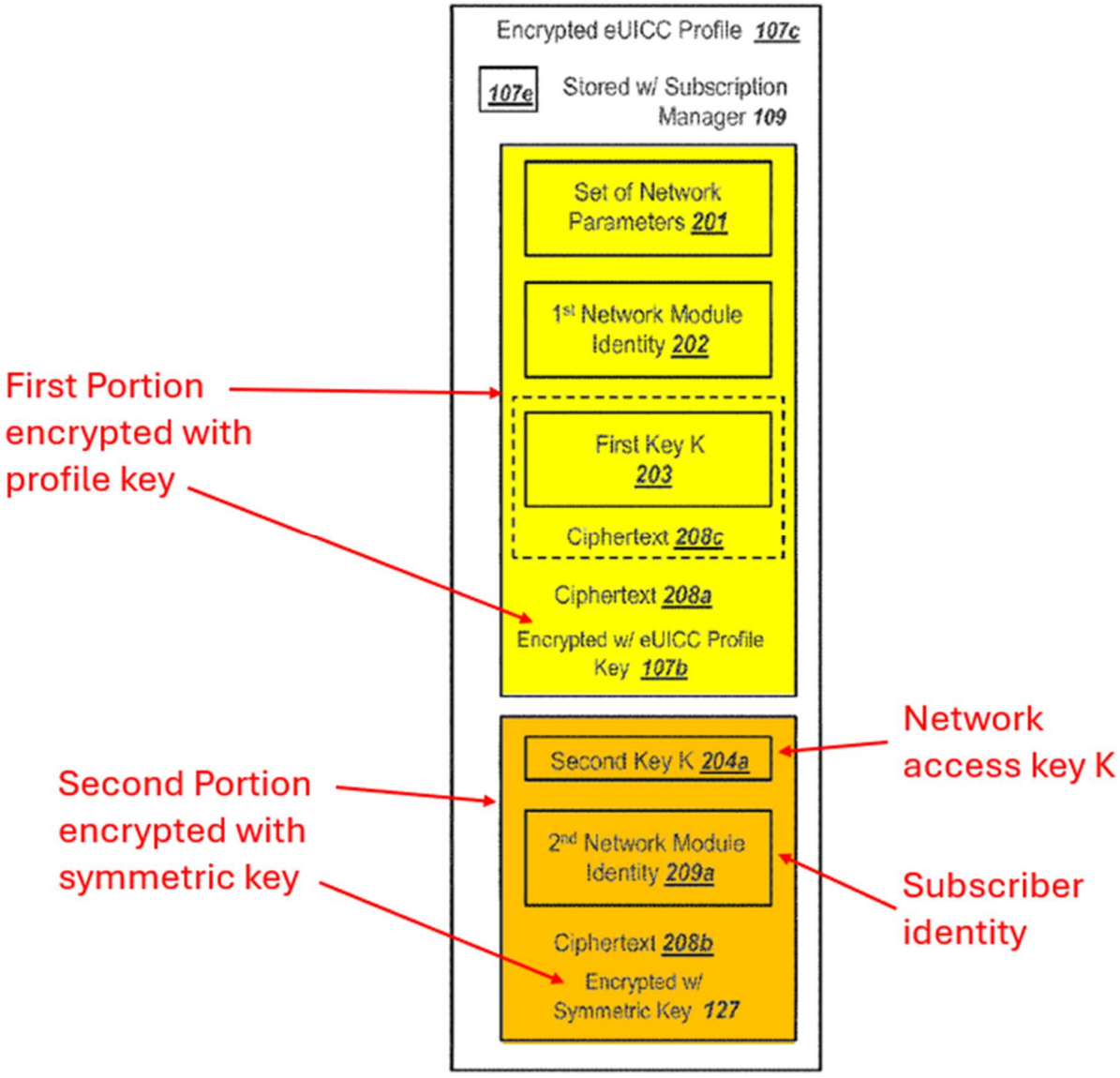
The profile 107c delivered to the eUICC by the SM includes two portions—a first portion including a 1st Key K, and a second portion including a 2nd Key K that is encrypted under a symmetric key. *Id*., 5:35-42, 6:40-42. The profile from the SM is encrypted under a "profile key" known to the SM and the eUICC. *Id*., 5:33-40. After decrypting a first portion of the profile using the profile key, the eUICC can

perform a two-factor authentication with the MNO (*id*., 5:45-62; Fig. 3, 308a, 308b), after which the MNO transmits the symmetric key needed to decrypt the second portion of the profile. *Id*., 6:30-32. Using this symmetric key, the eUICC completes the profile decryption, thereby recovering the second key K, which it can use to gain full access to the network. *Id*., 6:53-67.

Thus, the purpose of the '893 Patent is its two-stage provisioning process, which ensures that the network operator—not the subscription manager—is in control of the final release of network credentials. However, Claim 1 (reproduced below) is drafted quite differently, reciting an eUICC performing three conventional processes: (1) participating in an elliptic curve Diffie-Hellman key exchange to generate a shared "profile key" for use in encrypting/decrypting a profile; (2) receiving and decrypting an encrypted profile where the profile is encrypted by two separate keys—the ***profile key*** encrypting a first portion of the profile, and a ***symmetric key*** encrypting a network access key K and subscriber identity within a second portion of the profile; and (3) using the network access key K to authenticate with the network. Ex-1001, Cl. 1; Ex-1002 ¶¶84-88.



The annotated excerpt of Figure 2a, below, illustrates the two portions of the profile encrypted by two different keys:



VII. PROSECUTION HISTORY OF THE '893 PATENT

The '893 Patent was filed December 10, 2021, and claims priority through a chain of 5 continuation applications (now issued patents), the earliest of which was filed December 6, 2013. During prosecution, the Examiner did not issue any substantive prior art rejections, but only Section 112 rejections, which the Applicant

overcame by amending Claim 1 to recite structure for the claimed "radio" and "random number generator." Ex-1004.

VIII. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art at the relevant time ("POSITA") would have had at least a bachelor's degree in electrical engineering, computer engineering, computer science, or a similar field, and 2-3 years of experience with cellular/WLAN security and mobile devices. Ex-1002 ¶¶25-27.

IX. PRIORITY DATE

The '893 Patent claims a priority date of December 6, 2013. However, the claims of the '893 Patent include new matter not disclosed in any of the earlier patents, to which the '893 Patent claims priority. Ex-1002 ¶¶91-94.

In particular, the common specification makes clear that it is the ***MNO*** that sends the symmetric key to the eUICC, to ensure that the ***SM*** does ***not*** have control over the release of network access key K. *See, e.g.*, Ex-1001, 6:30-32, 35:13-38, 35:49-55, 41:48-42:6, 59:37-48,59:55-65. However, the claims of the '893 Patent recite that the source of the claimed "symmetric key" is the "***subscription manager***" or ***SM***.

Because none of the applications in the '893 Patent's priority chain provides any written description support for this claim limitation, the '893 Patent is entitled to a priority date no earlier than its filing date: December 10, 2021. *See, e.g.*, *X2Y*

Attenuators, LLC v. ITC, 757 F.3d 1358, 1365 (Fed. Cir. 2014) ("[A] claim is entitled to the priority date of an earlier application only if the earlier specification provides sufficient written support for the full scope of the claim.").

Ground 6 assumes this later priority date, while the references relied upon or added in Grounds 1-5 are prior art under either priority date.

X. CLAIM CONSTRUCTION

Petitioner interprets the claims according to *Phillips*. 37 C.F.R. §42.100(b). To resolve this Petition, Petitioner does not believe that any term requires express construction.[2] CTPG, 44; Ex-1002 ¶95.

XI. BRIEF DESCRIPTION OF THE APPLIED PRIOR ART

A. Park (Ex-1005)

Park was published in the Proceedings of the 2013 International Conference on Availability, Reliability and Security, Regensburg, Germany (297-303), cataloged by IEEE, and was publicly available by at least November 7, 2013. Ex-1019; Ex-1002 ¶¶96-98. Park is prior art to the '893 Patent under 35 U.S.C. §102(a)(1).

[2] The Samsung litigation is in its infancy and no claim construction proceedings have begun. Petitioner respectfully reserves all rights to raise claim construction and other arguments in district court and will request leave to submit the district court's claim construction as soon as it becomes available. Additionally, should PO raise express or implied claim construction arguments in its Preliminary Response, Petitioner will respectfully seek a Preliminary Reply to respond. Consolidated Trial Practice Guide (CTPG), 44-45.

Park teaches a secure architecture for remotely provisioning MNO profiles onto eUICCs. Ex-1005, 297. Under ETSI/GSMA's eUICC provisioning model (illustrated in Figure 1, below), the SM was divided into two roles: "SM-DP (Data Preparation)" for generating and encrypting the operator profile, and "SM-SR (Secure Routing)" for transporting and installing the encrypted profile onto the eUICC. *Id*., 297.

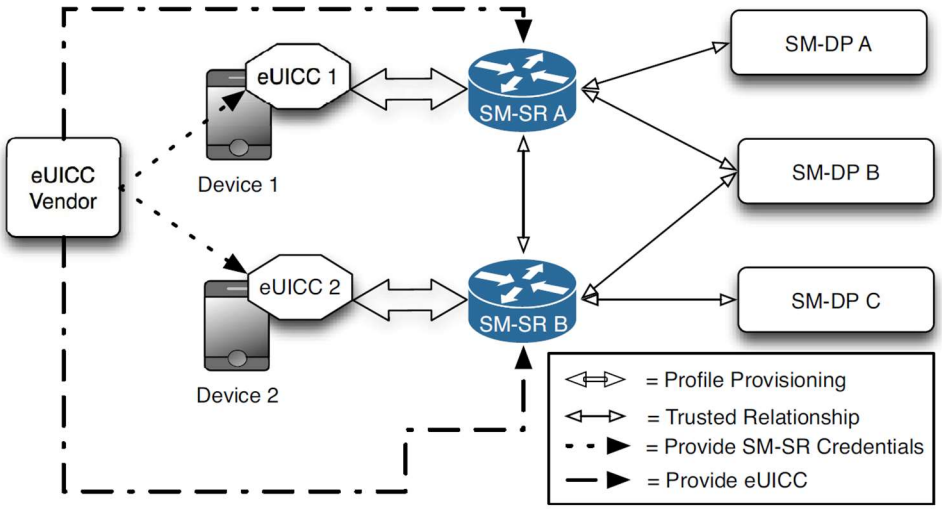


Fig. 1. eUICC Profile Ecosystem

This architecture introduced a new trust boundary: because the SM-SR may be operated by an entity distinct from the SM-DP or MNO, it should not be trusted with access to sensitive profile contents. *Id*. To mitigate, Park introduces a Key Agreement Module (KAM), enabling the eUICC and the SM-DP to negotiate mutually compatible profile encryption keys directly, without exposing them to the SM-SR or other intermediaries. *Id*., 299–301.

B. GlobalPlatform (Ex-1006)

GlobalPlatform (GlobalPlatform Card Specification Version 2.2.1) was published in January 2011 and made available that month on the GlobalPlatform Digital Library website and is prior art to the '893 Patent under 35 U.S.C. §102(a)(1). Ex-1018; Ex-1002 ¶¶99-103.

GlobalPlatform defines a standardized architecture for smart card security including Secure Channel Protocols (SCPs) to protect communications between the card and an off-card entity, ensuring authentication, integrity, and confidentiality. Ex-1006, 19-20, 28, 112.

GlobalPlatform's Secure Channel Protocol 10 ("SCP10"), uses "a Public Key Infrastructure (PKI)" for authentication. *Id*., 116. Under PKI, each participant has a pair of keys—a private key kept secret and a public key shared with others. Ex-1002 ¶101. During authentication, each party sends the other a random challenge, which the receiving party signs with its private key and returns to the sender. Ex-1006, 246-47, 266-68, 271. The sender then verifies that signature using the responder's public key. *Id*. Successful verification proves that the responder is the legitimate holder of the private key and therefore authentic, as shown in Figure F-9, below. *Id*., 234.

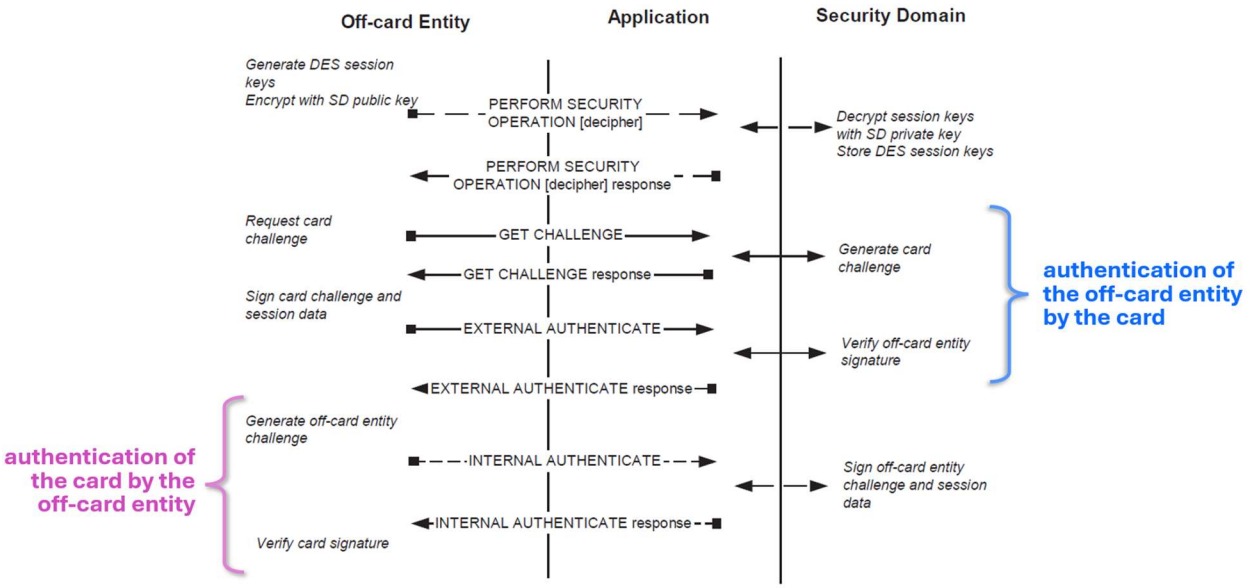


Figure F-9: Entity Authentication Flow

For confidentiality, a "Secure Channel session key" encrypts all message data transmitted to and from the card, as illustrated in Figure F-11. *Id.*, 258-59.

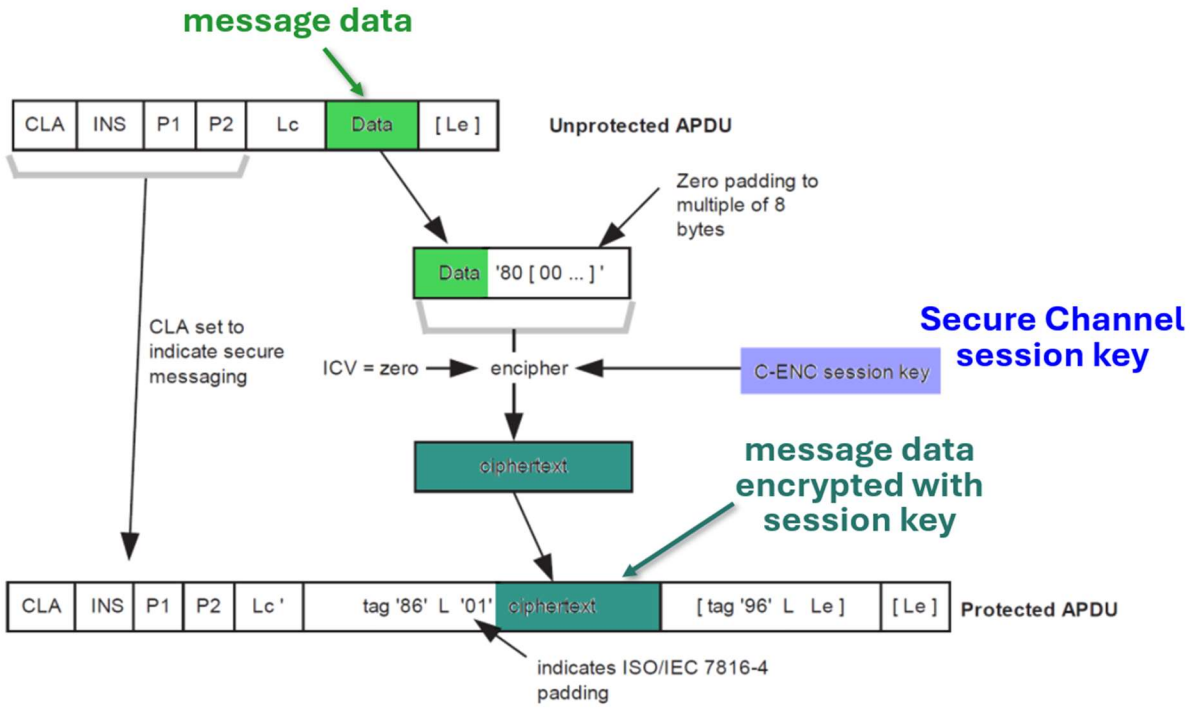


Figure F-11: Secure Messaging: Command message protected for confidentiality

GlobalPlatform imposes an additional level of protection for sensitive data, explaining that "[a] further level of security applies to sensitive data (e.g. secret keys) that shall always be transmitted as confidential data." *Id.*, 112. This additional encryption "is over and beyond the Current Security Level required for the Secure Channel." *Id.*, 264. Thus, when "transmitting sensitive data to and form the card"—including "all keys transmitted to a card"—the sensitive data is first encrypted "us[ing] the relevant data encryption session key (DEK)" and the entire message is then further encrypted with the Secure Channel session key, providing layered protection for these highly sensitive materials. *Id.*, 264.

C. AbiChar (Ex-1007)

AbiChar was published in the Proceedings of the 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007), was cataloged and made publicly available by IEEE by at least October 8, 2007, and is prior art to the '893 Patent under 35 U.S.C. §102(a)(1). Ex-1018; Ex-1002 ¶¶104-05.

AbiChar teaches a fast and secure elliptic-curve-based authenticated key agreement protocol (EC-SAKA) for low-power mobile communications. Ex-1007, 1. But as a starting point, AbiChar uses the standard "Diffie-Hellman key exchange based on EC," (or ECDH), which AbiChar describes as follows:

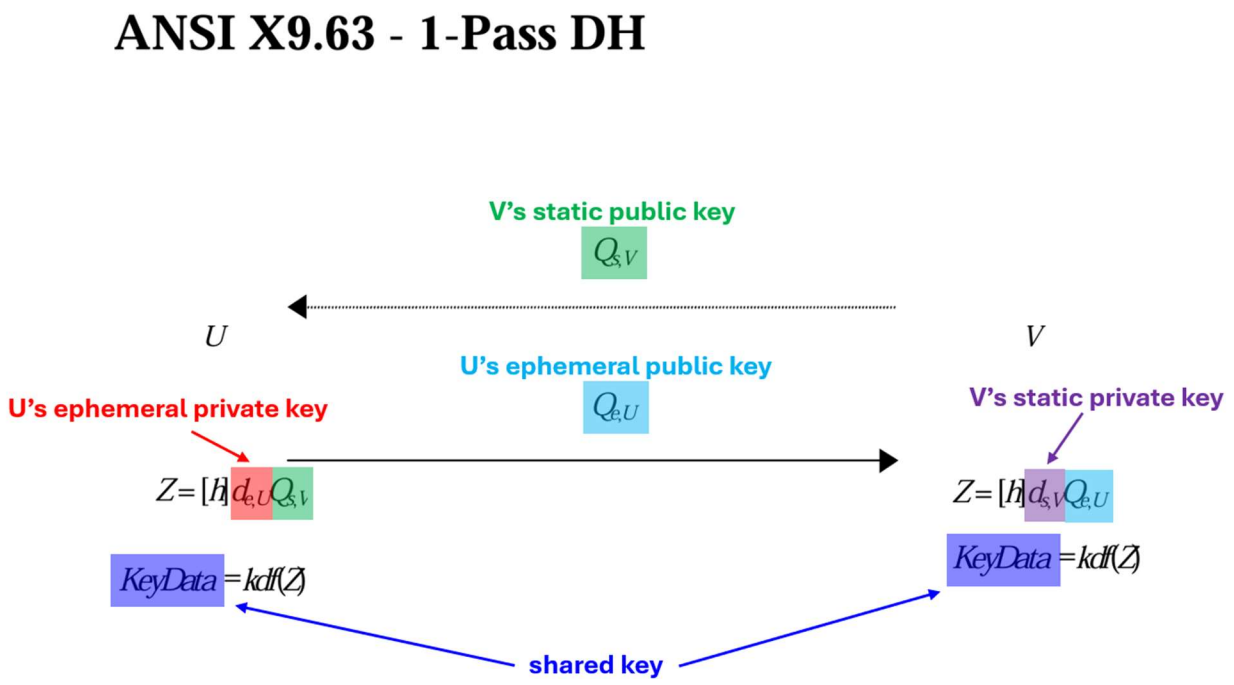
> Alice selects a random number n_a and computes $Y_a = n_a B$, she sends Y_a to Bob. Similarly Bob computes $Y_b = n_b B$ and sends Y_b to Alice. Alice and Bob generate the same key $K = n_a Y_b = n_b Y_a = n_a n_b B$.

Ex-1007, 3. The derived key K in AbiChar corresponds to the profile key derived in Claim 1 of the '893 Patent. Ex-1002 ¶105.

D. X9.63-Overview (Ex-1008)

X9.63-Overview (ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography) was authored by Simon Blake-Wilson in 1999, was publicly available in 2000, and is prior art to the '893 Patent under 35 U.S.C. §102(a)(1). Ex-1015; Ex-1002 ¶¶106-07.

X9.63-Overview "[s]pecifies key agreement and key transport schemes using elliptic curve cryptography" (Ex-1008, 3), including the one-pass Diffie-Hellman key-agreement protocol, illustrated below:



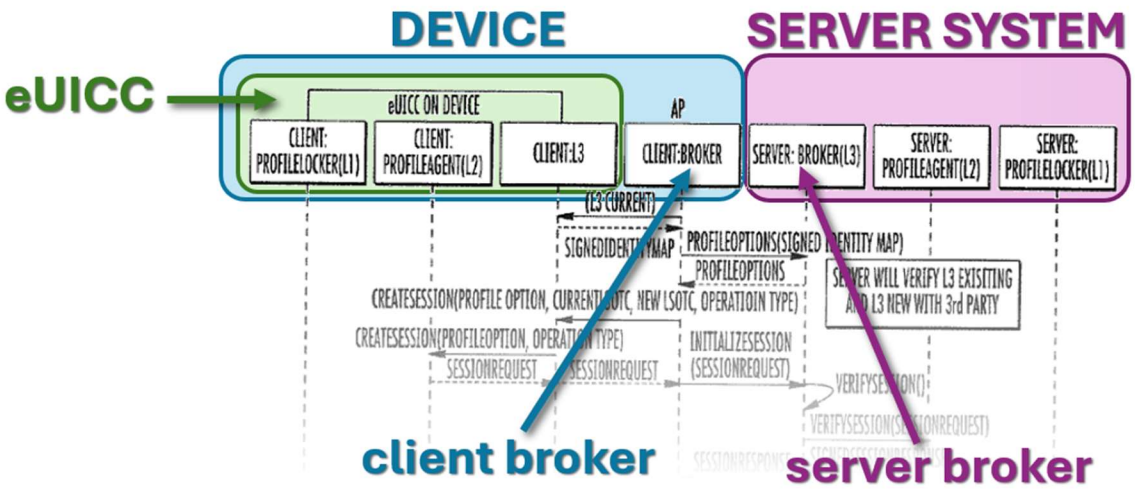
Id., 12. Here, entity U generates an ephemeral public/private key pair ($Q_{e,U}$, $d_{e,U}$) (*id.*), by randomly selecting an ephemeral private key ($d_{e,U}$) (*id.*, 7). Entity U then sends its ephemeral public key ($Q_{e,U}$) to entity V. *Id.*, 12. Each entity then computes a shared secret Z using 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.* That shared secret is then input into a key-derivation function (KDF) to produce a **shared key (*KeyData*)**. *Id.* **KeyData** is substantially similar to AbiChar's K and the "profile key" derived in Claim 1.

E. Haggerty (Ex-1012)

Haggerty (U.S. Patent Pub. No. 2013/0227646) filed February 14, 2013, published August 29, 2013, and is prior art to the '893 Patent under 35 U.S.C. §102(a)(1). Ex-1002 ¶¶108-111.

Haggerty teaches methods for secure large-scale distribution of eSIMs that are to be stored on eUICCs. Haggerty explains that, although eSIM data are encrypted, certain metadata fields remain in plaintext for operational use, such as the Integrated Circuit Card Identifier ("ICCID"). Ex-1012, ¶84. These plaintext identifiers allow devices and servers to identify and manage profiles without decrypting the full payload. Ex-1012, ¶¶54, 105; Ex-1002 ¶109.

In Haggerty's system, the eUICC device includes a "device broker" for sending provisioning requests to a "server broker" that relays them to a profile agent. Ex-1012, ¶¶97, 104-05, 108; Fig. 9 (below).



The "communication between the device broker and the server broker" may use a "a security protocol (e.g., transport layer security (TLS))" to "prevent capture and replay attacks." Ex-1012, ¶100.

F. Pierce (Ex-1013)

Pierce (U.S. Patent Pub. No. 2009/0323967) published December 31, 2009, and is prior art to the '893 Patent under 35 U.S.C. §102(a)(1). Ex-1002 ¶¶112-13.

Pierce teaches "producing cryptographic keys for use by an embedded processing device" using a "pseudo random number generator" (PRNG). Ex-1013, Abstract. As Pierce explains, generating "strong cryptographic keys typically involves the use of random data that cannot be later discerned or uncovered," and are thus preferably based on "entropy data." Ex-1013, ¶3. Accordingly, Pierce teaches collecting entropy data from sources that are naturally available to embedded devices, such as sensor outputs, timing data (e.g., GPS time), unique identifiers, and/or transient events on the communication bus, to generate seed values for the PRNG. Ex-1013 ¶¶35–38, Fig. 3.

G. Konstantinou (Ex-1014)

Konstantinou (U.S. Patent Pub. No. 2010/0267383) published October 21, 2010 and is prior art to the '893 Patent under 35 U.S.C. §102(a)(1). Ex-1002 ¶¶114-15. Konstantinou teaches that UICC profile network parameters include mobile

country code (MCC) and mobile network code (MNC) values. Ex-1014 ¶¶31, 158, 162.

H. Nix175 (Ex-1016)

Nix175 (U.S. Patent No. 9,100,175) was filed on December 6, 2013 and published on August 4, 2015. If the challenged patent is not entitled to its priority claim as discussed in Section IX, Nix175 is prior art to the '780 Patent under 35 U.S.C. §102(a)(1). Ex-1016, cover; Ex-1002 ¶116. Nix175 shares a specification with the challenged patent.

XII. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS

A. Ground 1: Claims 1, 3, 6-11, 13-17 are obvious over Park in view of GlobalPlatform and AbiChar

1. A POSITA would have been motivated to combine Park's teachings with GlobalPlatform's and AbiChar's teachings and would have had a reasonable expectation of success.

A POSITA would have been motivated to combine Park's secure profile provisioning architecture (SPA) with GlobalPlatform's procedures for sensitive data encryption, and AbiChar's elliptic curve Diffie-Hellman (ECDH) key agreement protocol, to yield a complete, secure, and efficient architecture for eUICC profile provisioning, as detailed below. Ex-1002 ¶117.

a. A POSITA would have turned to GlobalPlatform for implementation-level details of Park's security requirements.

Park's Secure Profile Provisioning Architecture (SPA) defines an architectural framework for secure eUICC profile provisioning but intentionally leaves some implementation-level details to the practitioner. Ex-1005, 299-303. Park generates profiles and securely delivers them from the SM-DP to the eUICC, noting "diverse key agreement protocols, secure communication protocols and cryptographic algorithms can be applied depending on the circumstances around the eUICC." *Id*., 303. Moreover, Park recognizes the GlobalPlatform Card Specification (GP) and its Secure Channel Protocol (SCP) as the "de facto standard for profile provisioning," and presents its SPA as extending GlobalPlatform. Ex-1005, 299. Park's SPA's fundamental security requirements—mutual SM-DP/eUICC authentication and profile confidentiality—are derived directly from GlobalPlatform. Park explains that SPA's security requirements "should be guaranteed in accordance with the requirements in [5]," where reference [5] corresponds to GlobalPlatform. *Id*., 299, 303.

Thus, a POSITA would have looked to GlobalPlatform to understand how to implement Park's security requirements. Ex-1002 ¶¶118-19. GlobalPlatform's SCPs were well-known, widely deployed mechanisms for providing mutual authentication and confidentiality in smart-card provisioning. Ex-1002 ¶¶68-75, 119. Accordingly,

incorporating GlobalPlatform's encryption procedures into Park's architecture, would (1) directly satisfy Park's stated requirements, (2) align with the standard that Park's SPA builds upon, and (3) leverage mature, well-tested, and industry-accepted methods. Ex-1002 ¶119.

In Park's SPA, the eUICC's Key Agreement Module (KAM) is used to generate a shared "SM-DP credential ($key_{SM\text{-}DP}$)" for encrypting and decrypting the profile transmitted from the SM-DP to the eUICC. Ex-1005, 300, 302. In the combined Park-GlobalPlatform system, $key_{SM\text{-}DP}$ serves the same function as GlobalPlatform's Secure Channel session key—providing confidentiality for data exchanged between an off-card entity and the card. Ex-1005, 302; Ex-1006, 258-59; Ex-1002 ¶¶75, 120. As Park explains, the SM-DP uses $key_{SM\text{-}DP}$, together with "selected cryptographic algorithms" agreed upon by the parties, to encrypt the profile that it sends to the eUICC. Ex-1005, 300. GlobalPlatform provides those established encryption procedures. Ex-1002 ¶120.

When transmitting message data that includes sensitive data, such as secret/private keys, SPC10 first encrypts the sensitive data "us[ing] the relevant data encryption session key (DEK)" and then further encrypts the message data with the secure channel session key, providing layered protection for these highly sensitive materials. Ex-1006, 264, 258 (explaining that the session key, C-ENC, is used to encrypt "the command data field of the command message being transmitted to the

card," which "includes any data within the data field that has already been protected for another purpose ***e.g. secret or private keys encrypted with the data encryption session key***"). This configuration is illustrated below in annotated Figure F-11.

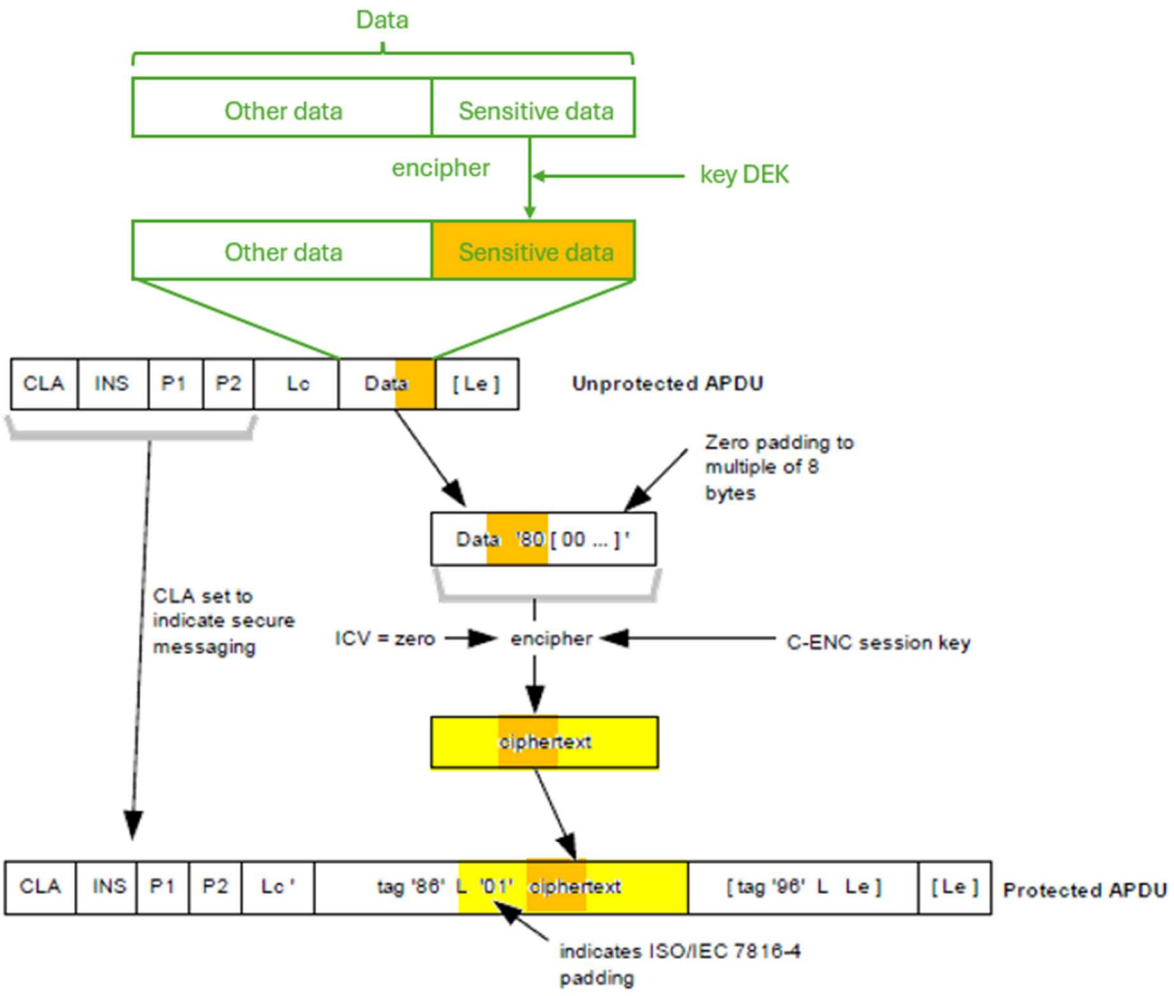


Figure F-11: Secure Messaging: Command message protected for confidentiality

Park similarly explains that eUICC profiles contain "security-sensitive information," including "keys" used for accessing a mobile network. Ex-1005, 297. A POSITA would have recognized that applying GlobalPlatform's DEK-based inner

encryption to these elements of Park's profile would provide an additional layer of protection for the most sensitive data within the profile, ensuring that even if the outer session-key encryption were compromised, the critical key materials could remain protected. Ex-1002 ¶¶40-41, 55-56, 121-22. Thus, Park-GlobalPlatform sends profiles from the SM-DP to the eUICC that include an inner layer of encryption for sensitive materials like keys (using GlobalPlatform's DEK), as well as an outer layer of encryption using Park's $key_{SM\text{-}DP}$/GlobalPlatform's session key. Ex-1002 ¶122.

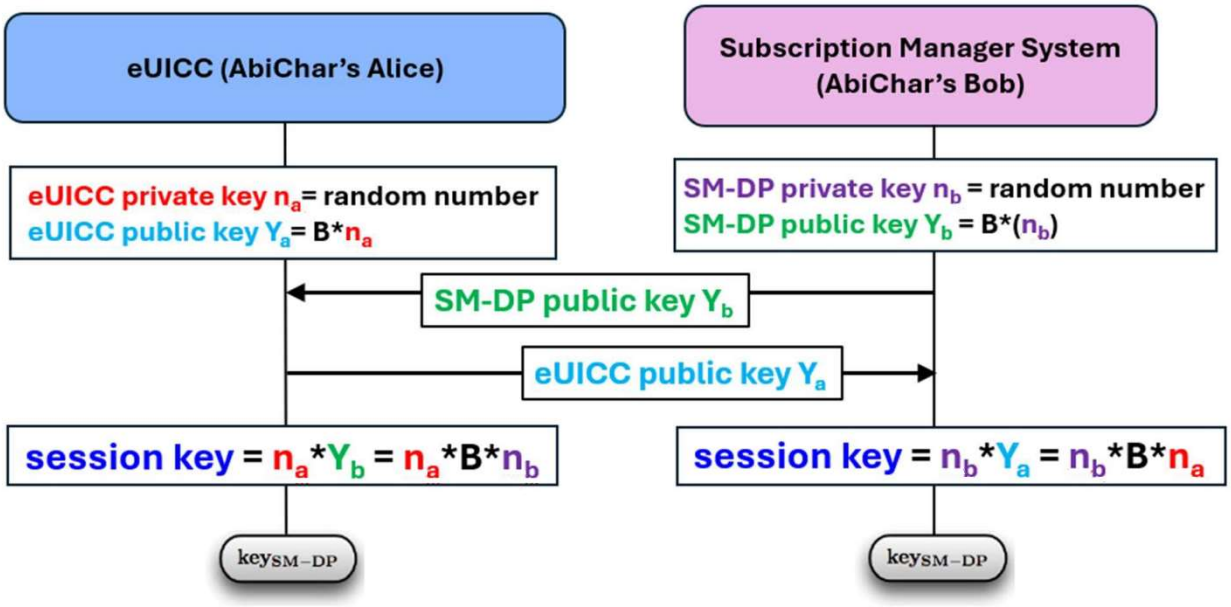
b. A POSITA would have understood that Abi-Char's elliptic curve Diffie-Hellman key agreement could be implemented within Park's SPA to provide an efficient asymmetric key-exchange mechanism

Park's Key Agreement Module (KAM) "provides the asymmetric algorithm-based key agreement protocol" used to derive $key_{SM\text{-}DP}$ for encrypting the eUICC profile. Ex-1005, 301. But Park does not specify a particular algorithm, instead explaining that "diverse key agreement protocols … can be applied depending on the circumstances around the eUICC." Ex-1005, 303.

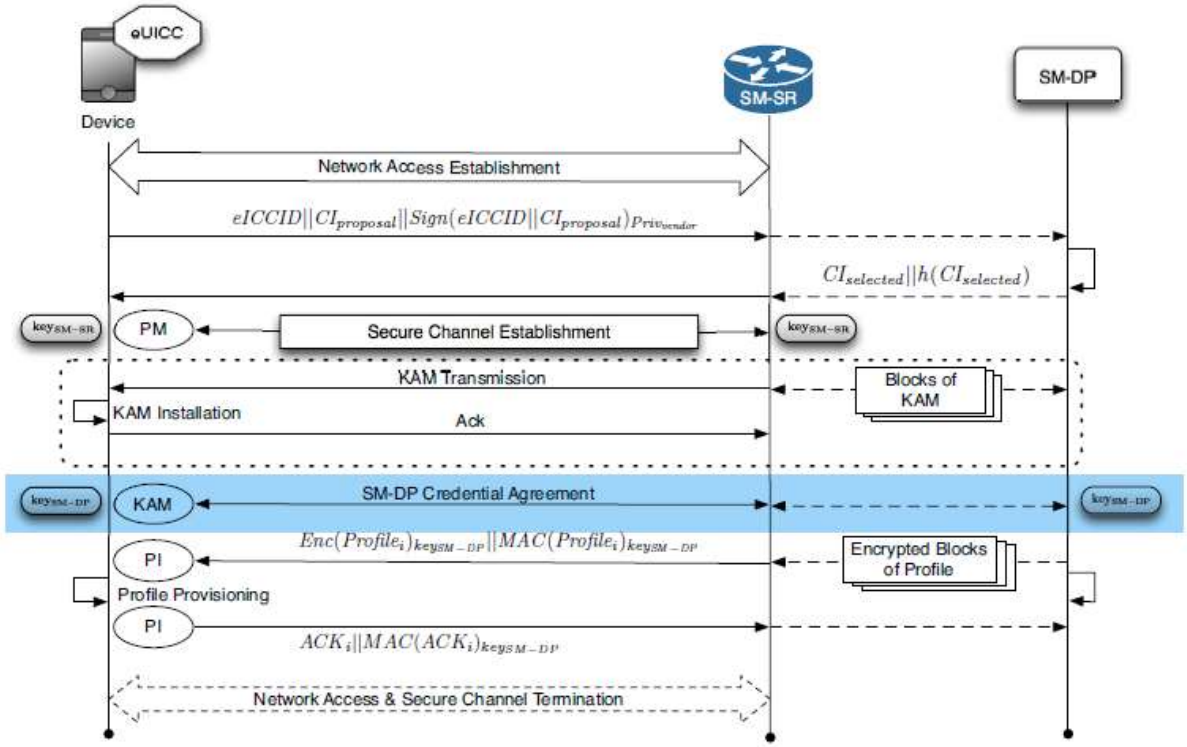
A POSITA would have recognized that the elliptic-curve-Diffie-Hellman key agreement protocol described in AbiChar provides an efficient asymmetric key exchange technique suitable for Park's architecture. Ex-1002 ¶¶42-48, 123-24. AbiChar explains elliptic-curve cryptography "can significantly reduce the

computation and storage overhead" of public-key operations, making it particularly well-suited for mobile and smart-card devices with limited processing resources. Ex-1007, 1. AbiChar describes an elliptic-curve Diffie–Hellman (ECDH) key-agreement exchange wherein each party generates random private keys (n_a and n_b respectively), generates public keys ($Y_a = n_aB$ and $Y_b = n_bB$, respectively), and then exchanges public keys. *Id*., 3. Each party then calculates a shared key using its private key and the other party's public key ($K = n_aY_b = n_bY_a = n_an_bB$). *Id*.

A POSITA would have incorporated AbiChar's ECDH protocol within Park's flexible, asymmetric framework, to provide a secure, lightweight, and computationally efficient mechanism for establishing $key_{SM\text{-}DP}$ between the eUICC and the SM-DP. Ex-1002 ¶¶45-48, 124. By mapping AbiChar's "Alice" to the eUICC and "Bob" to the SM-DP, the ECDH key exchange between the eUICC and SM-DP is illustrated as follows:



The ECDH exchange occurs in the Park-GlobalPlatform combination after the KAM transmission and installation (which would include ECDH parameters, such as the elliptic curve) and result in the establishment of keySM-DP in the "SM-DP Credential Agreement" step:



Ex-1002 ¶126.

2. Independent Claim 1

a. 1[pre]: A mobile device for communicating with a wireless network, the mobile device comprising:

Park, GlobalPlatform, and AbiChar ("Park-GlobalPlatform-AbiChar") teaches[3] the preamble, to the extent it is limiting. Ex-1002 ¶¶127-130.

Park teaches a "secure profile provisioning architecture" for "[e]mbedded UICC (hereafter eUICC)," which Park explains is "a new form of UICC (Universal

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

Integrated Circuit Card)" that is "soldered into a device during manufacturing." Ex-1002, 297. As illustrated in Figure 5, below, the device housing the eUICC may be a mobile device, such as a smartphone:

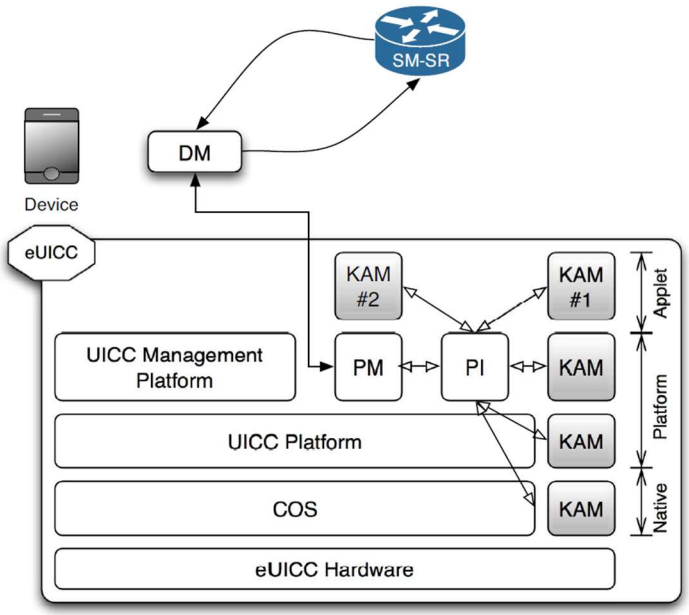


Fig. 5. Internal Architecture of eUICC

As Park explains, unlike a traditional UICC that is pre-provisioned by a single MNO, an eUICC must download a profile from a Subscription Manager in order to access an MNO's cellular network. Ex-1005, 297-98. Downloading a new profile is performed via wireless communications between Park's eUICC-installed device and the subscription manager. Ex-1005, Fig. 4:

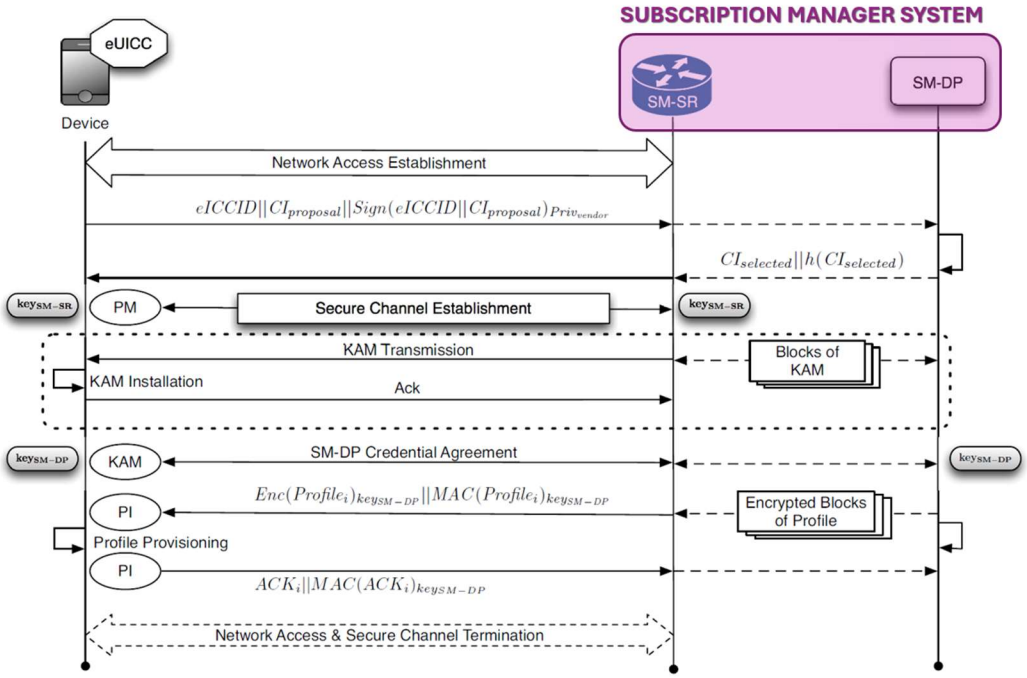


Fig. 4. Secure Profile Provisioning Procedure

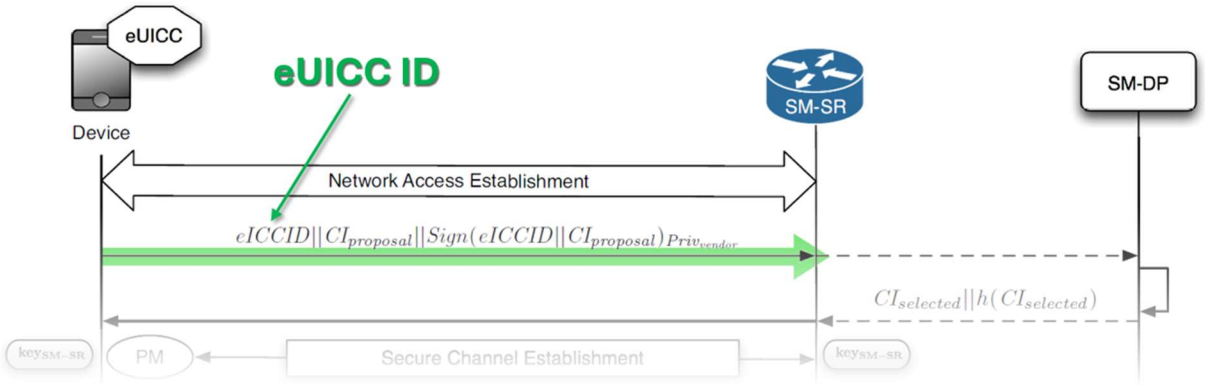
The eUICC wirelessly communicates with the SM-SR either by: (1) accessing a mobile network "using [a] Provisioning Profile" that was pre-provisioned on the eUICC; (2) "access[ing] SM-SR via WiFi"; or (3) using an already "provisioned profile for accessing [a] mobile network." Ex-1005, 300. Thus, Park teaches "[a] mobile device for communicating with a wireless network," as claimed. Ex-1002 ¶130.

b. 1[a]: a first memory configured to store an embedded universal integrated circuit card (eUICC) identity;

Park-GlobalPlatform-AbiChar teaches 1[a]. Ex-1002 ¶¶131-34.

(1) eUICC "identity"

Park teaches that eUICC and SM-DP negotiate (via the SM-SR) to establish the key exchange protocol to be used by the parties. Ex-1005, 301. The eUICC sends a message to the SM-SR that includes "the eUICC ID (*eICCID*)," as illustrated in Figure 4, excerpted below. Ex-1005, 300.



(2) "a first memory" storing the eUICC ID

The eUICC includes "eUICC Hardware," together with "software running in the eUICC," as illustrated in Figure 5, below. Ex-1005, 299.

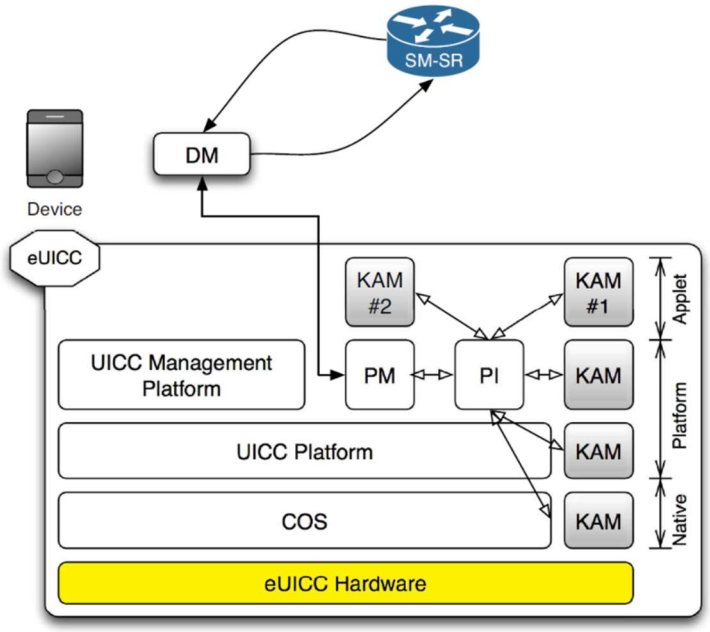


Fig. 5. Internal Architecture of eUICC

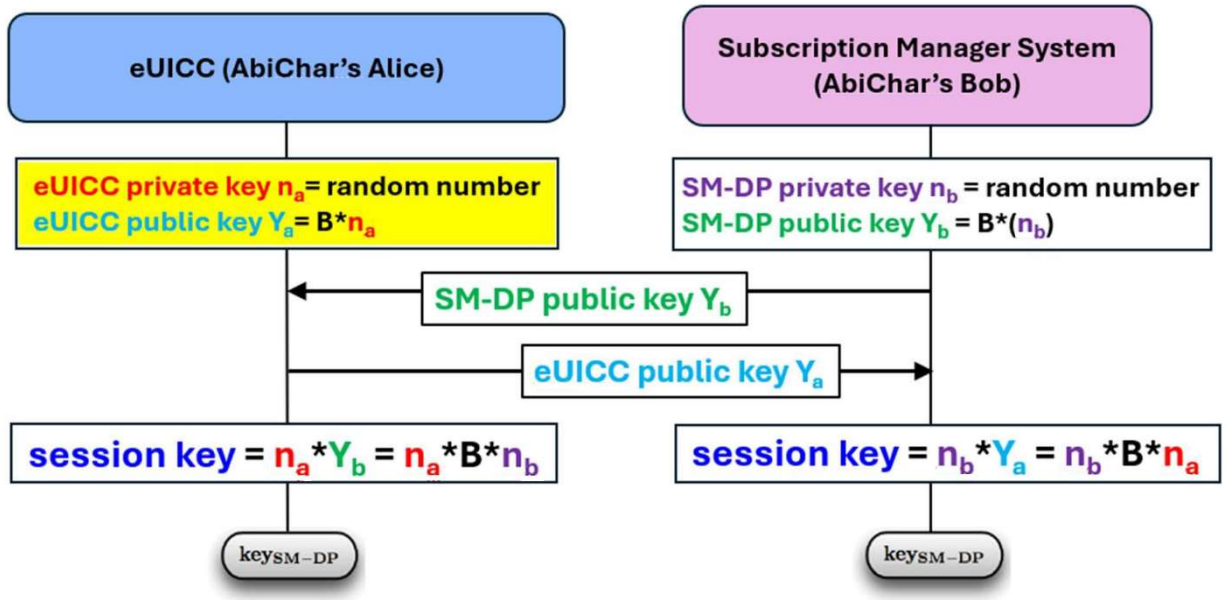
A POSITA would have understood that this "eUICC Hardware" includes memory. Ex-1002 ¶134. Indeed, Park notes that different eUICC "can be different from each other with respect to … ***available memory capacities***." *Id*., 301. A POSITA would have recognized that the eUICC ID would be stored in this eUICC memory (claimed "first memory"), so that it can be retrieved by the eUICC and used during the provisioning process, as illustrated in Figure 4, above. Ex-1005, 300; Ex-1002 ¶134. Moreover, a POSITA would have preferred that this first memory be non-volatile so the eUICC ID is retained through power cycles. Ex-1002 ¶134.

c. 1[b]: a random number generator operably connected to a processor connected to a second memory configured to generate a random number for an eUICC private key corresponding to an eUICC public key;

Park-GlobalPlatform-AbiChar teaches 1[b]. Ex-1002 ¶¶135-140.

(1) generating "a random number for an eUICC private key corresponding to an eUICC public key" using a "random number generator"

During Park's profile-provisioning procedure, the eUICC and SM-DP engage in an "asymmetric algorithm-based key agreement protocol" to each "dynamically [] generate the SM-DP Credentials ($key_{SM\text{-}DP}$)." Ex-1005, 300-301. The combined system would use AbiChar's ECDH key agreement for this protocol, resulting in the key exchange illustrated below:



Ex-1002 ¶136.

In the combined Park-GlobalPlatform-AbiChar system, the eUICC generates **private key n_a (claimed "eUICC private key")** as a random number. Ex-1007, 3. The eUICC then calculates a **corresponding public key $Y_a = B*n_a$ (claimed "second eUICC public key")** from **private key n_a**, using elliptic-curve scalar multiplication, with elliptic curve point *B*. Ex-1007, 3; Ex-1002 ¶137. A POSITA would have understood that the eUICC would include a random number generator—e.g., within, or coupled to, Park's KAM software—for use in generating the random number for **private key n_a**. Ex-1002 ¶137.

(2) the random number generator "operably connected to a processor connected to a second memory"

Park teaches that the eUICC includes "eUICC Hardware," together with "software running in the eUICC," which includes the "Key Agreement Module (KAM)," as illustrated in Figure 5, below. Ex-1005, 299.

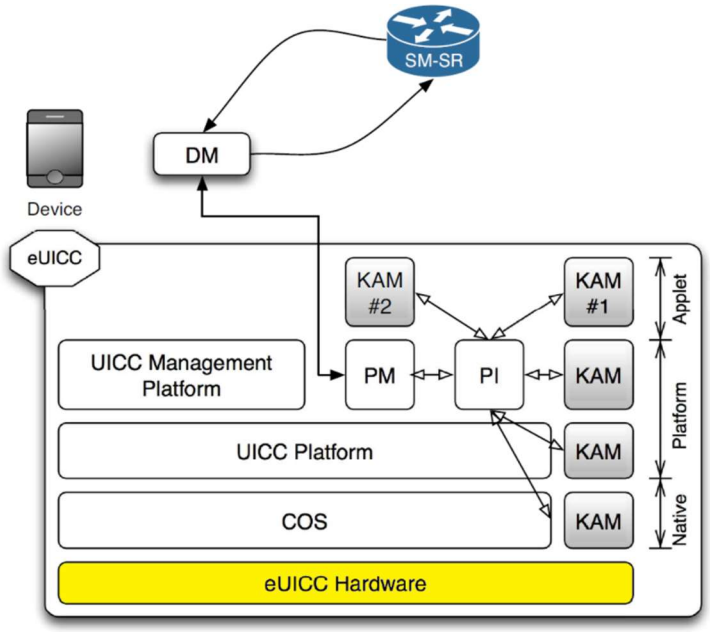


Fig. 5. Internal Architecture of eUICC

A POSITA would have understood that the KAM software, together with the random number generator it employs, would execute within the secure environment provided by the eUICC, on one or more processors included within the eUICC hardware—i.e., the random number generator would be "operably connected" to these processor(s), as claimed. Ex-1002 ¶139. Indeed, Park specifically identifies an "(e)UICC" offered by STMicroelectronics that includes a "Crypto Co-Processor," which a POSITA would have recognized as a well-known component used to execute cryptographic functions, including random number generation, within secure elements such as an eUICC. Ex-1005, 302-03; Ex-1002 ¶139.

As explained for 1[a], Park also teaches that the eUICC hardware includes memory. While the first memory for storing the eUICC ID (as discussed for 1[a],

above, is likely non-volatile memory, it may be preferable that the random number used to generate the private key n_a not be retained through power cycles to reduce the risk of compromise, in which case, the memory would be a second (volatile) memory, separate from that used to store the eUICC ID. Ex-1002 ¶140. A POSITA would have understood that the random number generator would be connected to that second memory because the random numbers it produces—including random **private key *n_a***, generated during the key agreement process—must be stored at least temporarily so that they can be used by the KAM. Ex-1002 ¶140.

d. 1[c]: a radio including one or more transmit antennas and one or more receiving antennas configured to:

Park-GlobalPlatform-AbiChar teaches 1[c]. Ex-1002 ¶¶141-43.

As explained for 1[pre], Park teaches that the eUICC wirelessly communicates with the SM-SR during the profile provisioning process, using a "mobile" or "WiFi" network and describes "profiles being ***transmitted*** to eUICC." Ex-1005, 299-300. The eUICC includes a "Device Module (DM)"—"software running in the Device to perform the roles of the intermediator between eUICC and SM-SR," as illustrated in Figure 5, below. Ex-1005, 299.

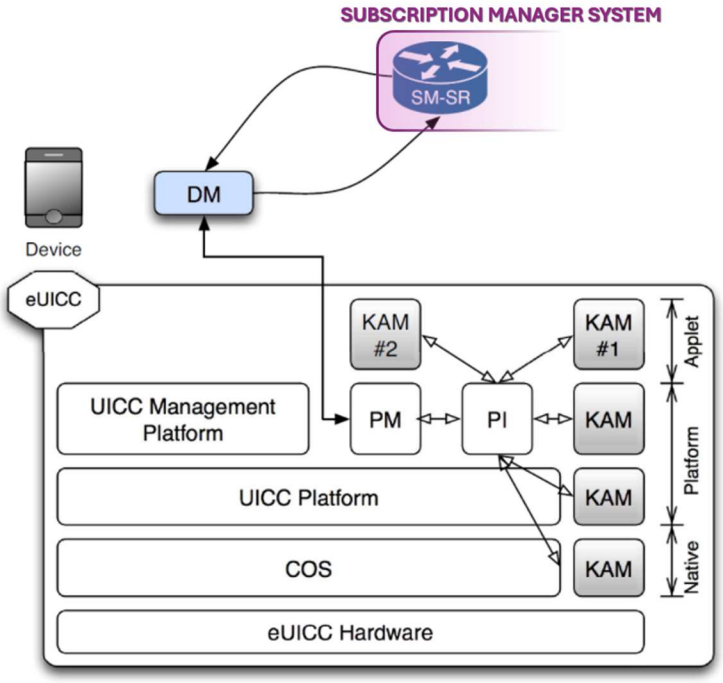


Fig. 5. Internal Architecture of eUICC

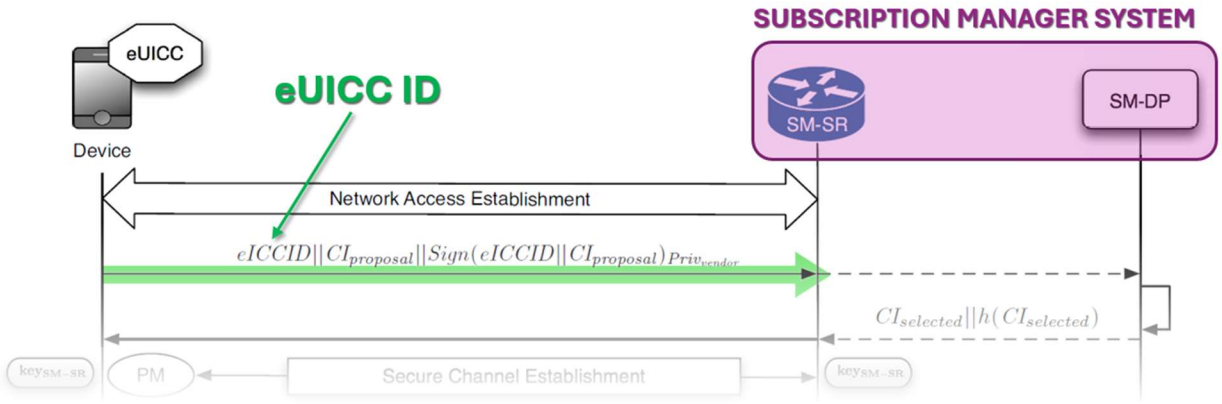
A POSITA would have understood that Park's DM would necessarily interface with transmit and receive antenna(s) to enable those wireless communications with the SM-SR. Ex-1002 ¶143. Indeed, conventional smartphones—such as the one illustrated in Park's Figure 5, above—include integrated transmit/receive antenna(s) for wireless communications over cellular and WiFi networks. *Id*.

e. 1[c][1]: a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and

Park-GlobalPlatform-AbiChar teaches 1[c][1]. Ex-1002 ¶¶144-46.

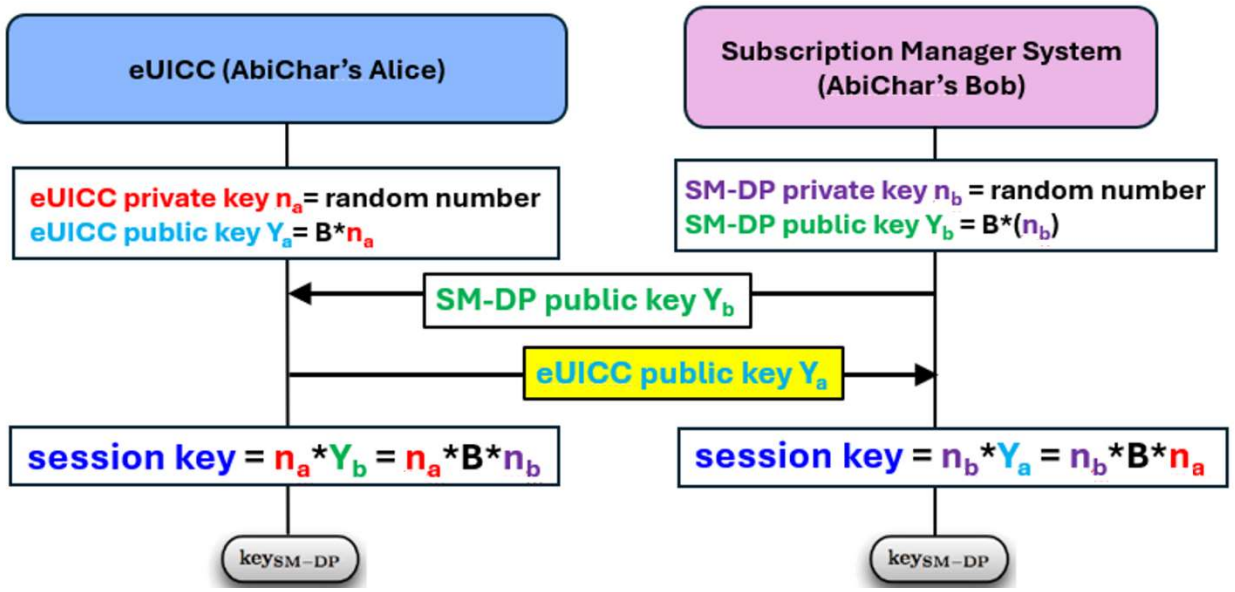
(1) transmit the eUICC identity to a subscription manager

As explained for 1[a], the eUICC transmits its eUICC ID to subscription manager in the initial capability negotiation message, as illustrated in Figure 4, excerpted below. Ex-1005, 300.



(2) transmit the eUICC public key to the subscription manager

As explained for 1[b], in the combined system, the KAM in Park's eUICC uses AbiChar's ECDH key agreement protocol to generate a private key n_a and a **corresponding public key Y_a (claimed "eUICC public key")**. Ex-1007, 3. That public key is then sent to the SM-DP (via SM-SR), as illustrated below, so that it can be combined with a private key n_b generated by the SM-DP, to generate Park's $key_{SM\text{-}DP}$. *Id*. As Park notes, $key_{SM\text{-}DP}$ can be generated by asymmetric key agreement (*id*.) of which ECDH is one of the most common choices. Ex-1002 ¶146.

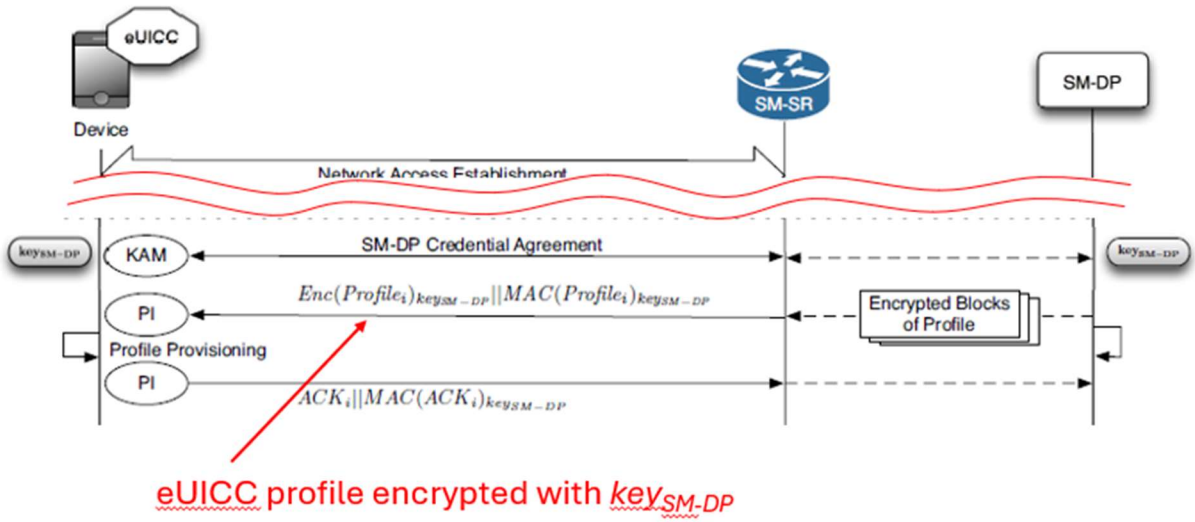


f. 1[c][2]: b. receive, from the subscription manager, i) an eUICC profile comprising network parameters, a key K, and a subscriber identity and ii) a symmetric key; andA

Park-GlobalPlatform-AbiChar teaches 1[c][2]. Ex-1002 ¶¶147-154.

(1) eUICC profile

After performing AbiChar's key agreement to generate key_{SM-DP}, Park teaches that SM-DP encrypts a profile "[u]sing the agreed SM-DP Credentials [key_{SM-DP}] and the selected cryptographic algorithms," and then "sends the protected profile blocks to the eUICC." Ex-1005, 300; Fig. 4 (excerpted below).



The profile includes "the MNO's data and applications … such as ***NAA (Network Access Application)*** [] with related data (e.g. ***IMSI (International Mobile Subscriber Identity)***, ***keys***, authentication algorithm, etc.)." Ex-1005, 297 (describing profiles in the context of traditional UICCs, and explaining that MNOs must be able to remotely provision those same profiles onto eUICCs). A POSITA would have understood that the NAA defines network parameters for enabling an eUICC to attach to, authenticate with, and communicate over the MNO's network. Ex-1002 ¶149.

(2) a symmetric key

Park teaches that the eUICC profile "includes [] security-sensitive information." Ex-1005, 299. A POSITA would have recognized that such sensitive information includes the keys (claimed "key K") and IMSI (claimed "subscriber identity") within the profile. Ex-1005, 297; Ex-1002 ¶150. GlobalPlatform teaches

that, when transmitting messages that include sensitive data, such as "secret or private keys," an additional layer of protection is provided "over and beyond the security level required for the Secure Channel," by first encrypting the sensitive data with a Data Encryption Key (DEK), and then encrypting the entire message (including the encrypted sensitive data) using the session key, as illustrated below. Ex-1006, 255, 258, 260, 264; Fig. F-11 (annotated). DEK is the recited "symmetric key," as explained below.

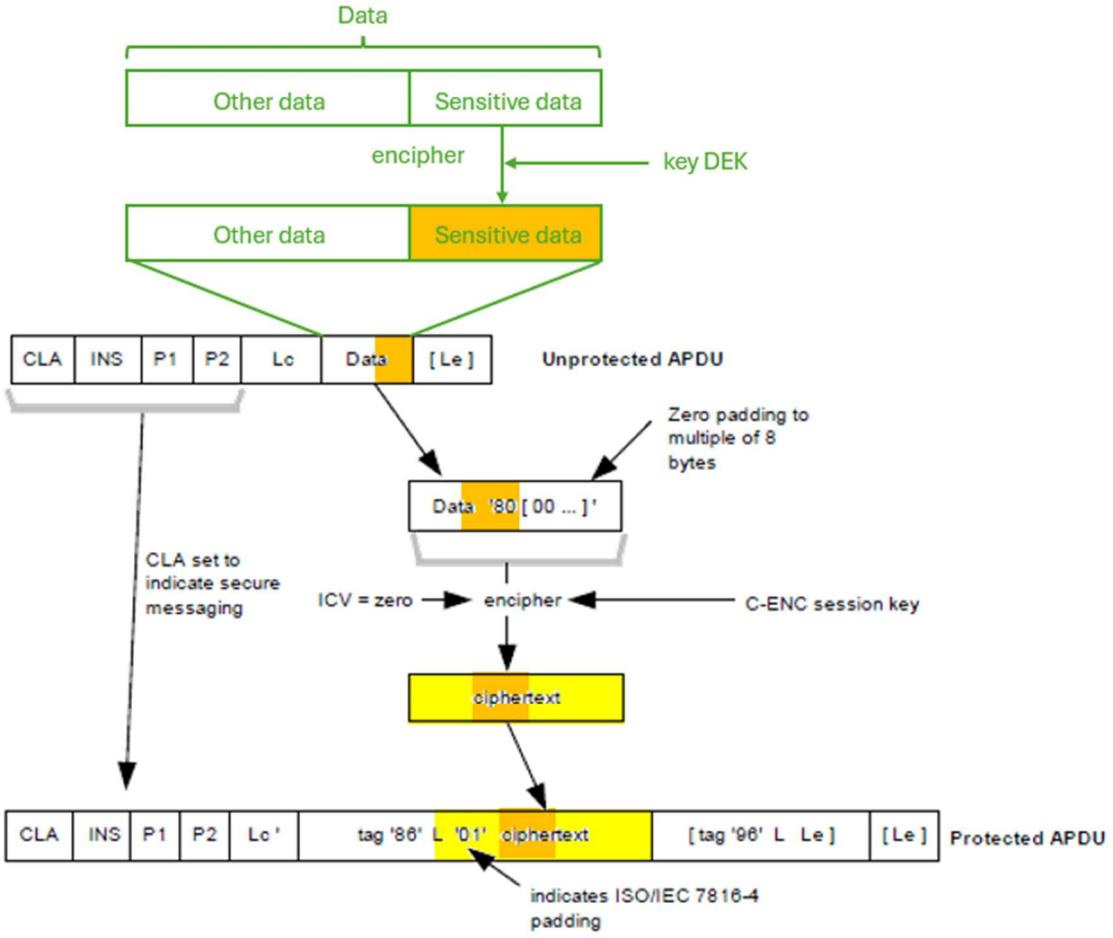
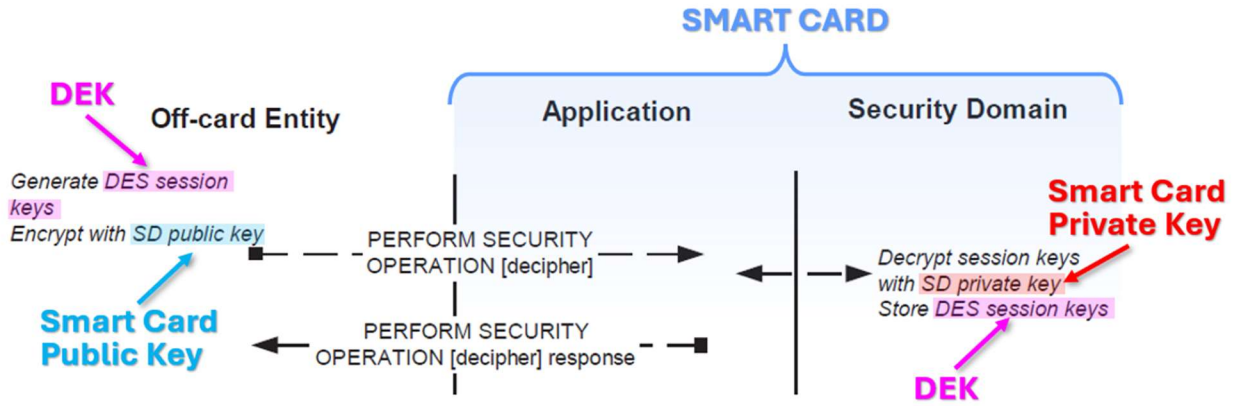


Figure F-11: Secure Messaging: Command message protected for confidentiality

A POSITA would have recognized that encrypting the sensitive data in Park's profile using DEK is required by GlobalPlatform to add an separate layer of protection. Ex-1002 ¶¶40-41, 151.

GlobalPlatform explains that encryption with the DEK "uses DES" (Ex-1006, 264), and that "[t]he Data Encryption Standard (DES) is a symmetric cryptographic algorithm that requires the use of the same secret key to encrypt and decrypt data." *Id*., 174. Thus, GlobalPlatform's symmetric DEK (claimed "symmetric key") is used to encrypt the sensitive data (e.g., secret keys, IMSI) included within Park's profile. Ex-1002 ¶¶33-35, 152.

Because the DEK is a symmetric key, in order for the eUICC to decrypt a key K encrypted with the DEK, the eUICC must have its own copy of the DEK. Ex-1002 ¶¶33-35, 153. GlobalPlatform teaches a "key transport option" that may be used by an off-card entity to send the DEK to a smart card. Ex-1006, 251-52. The DEK is sent to the card using the "PERFORM SECURITY OPERATION [decipher] command." Ex-1006, 255-56 (explaining that the PERFORM SECURITY OPERATION [decipher] command includes "control reference templates" that "contain the actual key values," with "control reference template 'B8'" used to transmit the DEK). GlobalPlatform further teaches that keys sent to smart card using the key transport option are encrypted using the card's public key. Ex-1006, 247, 275-76. This is illustrated in Figure F-9, excerpted below:



Ex-1006, Fig. F-9 (excerpted)

A POSITA would have recognized that in the combined Park-GlobalPlatform system, the SM-DP would send the DEK (claimed "symmetric key") to the eUICC, encrypted with the eUICC's public key (enabling the eUICC to decrypt it using its corresponding private key). Ex-1002 ¶¶40-41, 154. Thus, Park-GlobalPlatform-AbiChar teaches that the eUICC-installed device receives a "symmetric key" from the "subscription manager," as claimed.

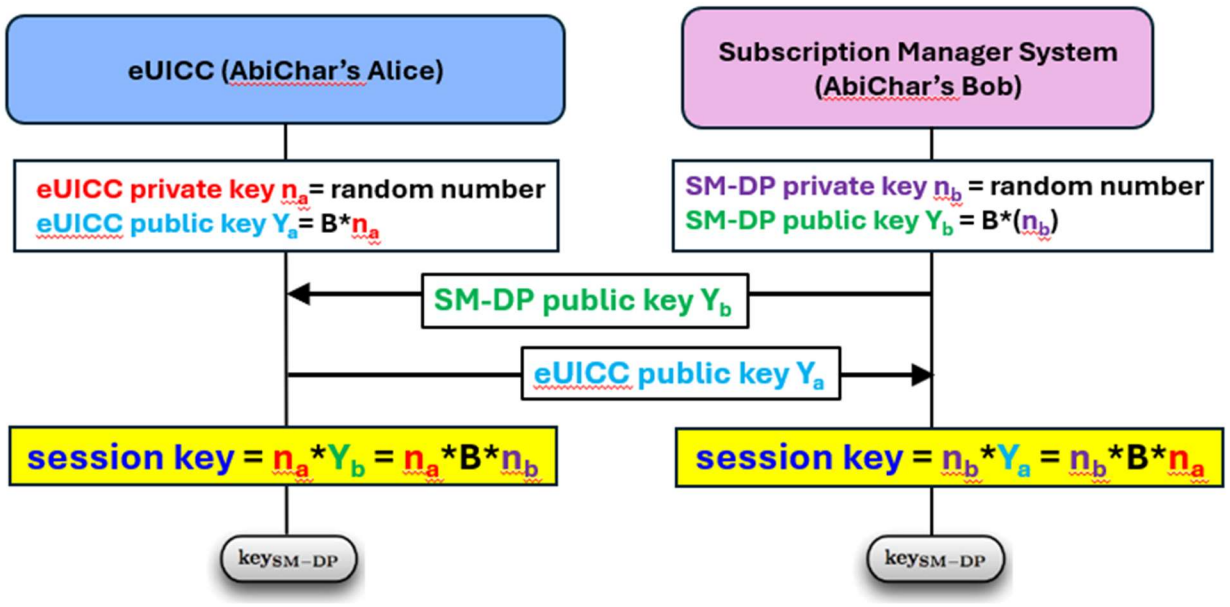
g. 1[d]: an eUICC associated with the eUICC identity and configured to

Park-GlobalPlatform-AbiChar teaches 1[d]. Ex-1002 ¶155. As explained for 1[a], Park teaches an eUICC associated with "the eUICC ID (*eICCID*)." Ex-1005, 300.

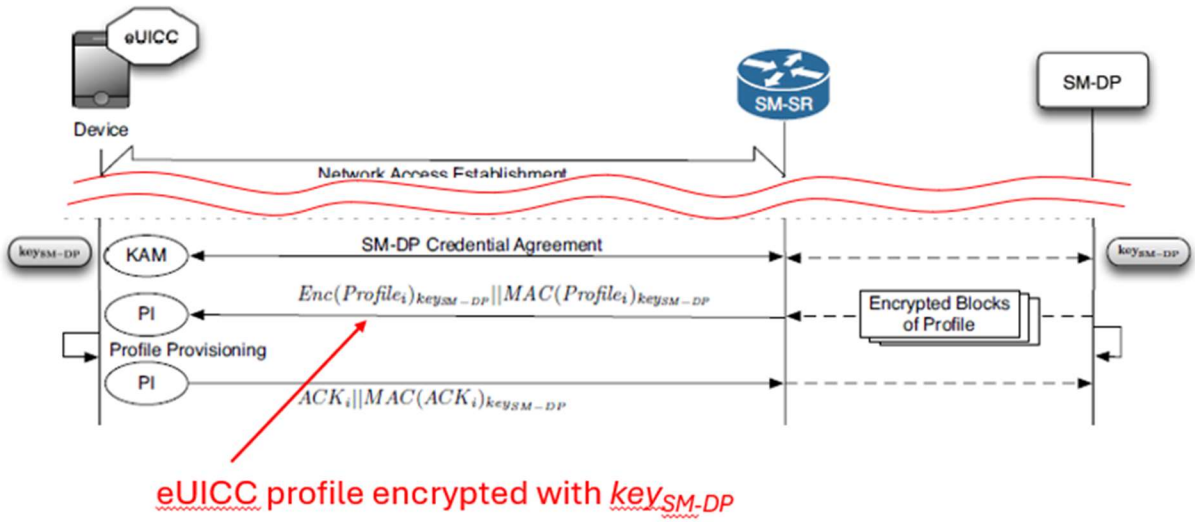
h. 1[d][1]: a. derive a profile key using an elliptic curve Diffie-Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key;

Park-GlobalPlatform-AbiChar teaches 1[d][1]. Ex-1002 ¶¶156-58.

As explained for 1[b], Park's eUICC and SM-DP engage in AbiChar's elliptic curve Diffie-Hellman (ECDH) key exchange to each generate a copy of Park's key_{SM-DP}/AbiChar's session key, as illustrated below. Ex-1007, 3; Ex-1005, 300.



In particular, the eUICC calculates ***key_{SM-DP}*/session key (claimed "profile key")** using its **private key n_a (claimed "eUICC private key")**, together with the **SM-DP public key Y_b (claimed "subscription manager public key)** that it received from the SM-DP. Ex-1007, 3. Park's ***key_{SM-DP}*** results from the KAM (applying AbiChar's ECDH algorithm) and is used to encrypt the eUICC profile as shown below. Ex-1005, Fig. 4 (excerpt).



i. 1[d][2]: b. decrypt a first portion of the eUICC profile using the profile key;

Park-GlobalPlatform-AbiChar teaches 1[d][2]. Ex-1002 ¶¶159-160.

Park teaches that, upon receiving the encrypted profile 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-1005, 300, Table1 ("Profile Installer (PI) | The software running in the eUICC to perform the decryption and verification of the protected profile blocks from SM-DP"). Because the SM-DP and eUICC both share ***key*$_{SM-DP}$ (claimed "profile key")**, a POSITA would have understood that ***key*$_{SM-DP}$** is a symmetric key—i.e., one that can be used for both encryption and decryption. Ex-1002 ¶¶33-35, 160. Thus, a POSITA would understood that decrypting each profile block, as performed by the eUICC, would involve using ***key*$_{SM-DP}$ (claimed "profile key")**. *Id*.

j. 1[d][3]: c. receive the symmetric key from a network application operating in the mobile device;

Park-GlobalPlatform-AbiChar teaches 1[d][3]. Ex-1002 ¶¶161-62.

As explained for 1[c][2], Park-GlobalPlatform-AbiChar teaches that the eUICC-installed device receives GlobalPlatform's symmetric key DEK (claimed "symmetric key") from the SM-DP. As illustrated in Figure 5, below, messages sent to the eUICC are received using Park's Device Module (DM), which is "software running in the Device to perform the roles of the intermediator between eUICC and SM-SR." Ex-1005, 299. Park's DM corresponds to the claimed "network application."

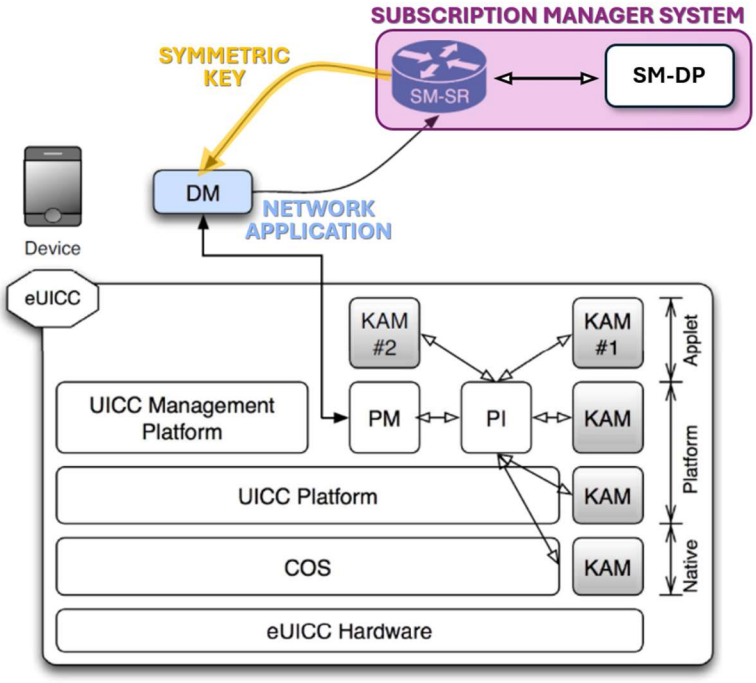


Fig. 5. Internal Architecture of eUICC

k. 1[d][4]: d. decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising the key K and the subscriber identity, wherein the first portion and the second portion are distinct; and

Park-GlobalPlatform-AbiChar teaches 1[d][4]. Ex-1002 ¶¶163-67.

As explained for 1[c][2], in the combined system, GlobalPlatform's DEK (claimed "symmetric key") would be used to encrypt the "security-sensitive information" within the profile (Ex-1005, 299), before the entire profile is wrapped under $key_{SM\text{-}DP}$. The sensitive information encrypted with DEK (claimed "symmetric key") would include Park's keys (claimed "key K") and IMSI (claimed "subscriber identity"), because disclosure of the keys could compromise network authentication and disclosure of the IMSI could allow cloning of the subscriber's identity. Ex-1002 ¶164.

GlobalPlatform teaches that, in response to receiving such encrypted "sensitive data," a smart card will perform a "decryption" process that "is the exact opposite" of the encryption process. Ex-1006, 264. Thus, in the combined Park-GlobalPlatform system, once the eUICC has decrypted the outer layer using $key_{SM\text{-}DP}$, it would use the DEK to decrypt the inner ciphertext containing the key K and IMSI. Ex-1002 ¶165.

Park teaches that the profile also includes a "Network Access Application" (NAA). Ex-1005, 297. As explained for 1[c][2], a POSITA would have understood

that the NAA includes network parameters used to establish network connectivity. A POSITA would have understood that such network parameters would include non-security-sensitive information—e.g., configuration data shared across all subscribers of the same MNO and/or MNO service. Ex-1002 ¶166. Encrypting and decrypting such information with GlobalPlatform's DEK would add unnecessary computational overhead to the system. *Id*. Accordingly, in the combined system, the inner layer of encryption with GlobalPlatform's DEK (claimed "symmetric key") would only be applied to a subset of Park's profile (claimed "second portion of the eUICC profile"), while the outer layer of encryption with Park's $key_{SM\text{-}DP}$ (claimed "profile key") would be applied to the entire profile (claimed "first portion of the eUICC profile"). Ex-1002 ¶166. Thus, Park-GlobalPlatform-AbiChar teaches that "the first portion and the second portion" of the profile "are distinct," as claimed.

Alternatively, once the sensitive data portion (keys, IMSI) has been encrypted using DEK, it is not necessary to further encrypt that portion of the profile with $key_{SM\text{-}DP}$, and it would be a simple matter of design choice (computational complexity vs. cryptographic security) to encrypt the sensitive portion only with DEK and the non-sensitive portion only with $key_{SM\text{-}DP}$ since all of the profile would still be protected under at least one key and the sensitive portion would remain accessible only to an entity possessing the claimed "symmetric key" DEK. This would maintain the first and second portions as distinct. Ex-1002 ¶167.

l. 1[d][5]: e. generate a response value for authentication of the mobile device with the wireless network using the key K.

Park-GlobalPlatform-AbiChar teaches 1[d][5]. Ex-1002 ¶¶168-170.

Park teaches that, following successful decryption of the profile, "the profile blocks are provisioned inside the eUICC." Ex-1005, 300. The provisioned profile includes a "Network Access Application" "with related data," including "keys" (claimed "key K") and an "authentication algorithm." Ex-1005, 297; Ex-1002 ¶¶77, 169. A POSITA would have recognized that the key K and authentication algorithm in Park's profile would be used by the eUICC to authenticate with and gain access to the associated MNO's network. *Id*. In particular, a POSITA would have recognized that a well-known method for authentication involves demonstrating possession of a secret key K, by using that key to sign a random challenge issued by the authenticating entity. Ex-1002 ¶¶57-59, 169. For instance, GlobalPlatform teaches an authentication method in which the card and off-card entity authenticate one another by proving that they both have "knowledge of the same secret(s)," by generating and verifying cryptographic response values derived from those shared secret(s). Ex-1006, 209-11. And, in the standard 3GPP authentication and key agreement (AKA) process, the eUICC uses its stored secret key K and authentication algorithm (e.g., MILENAGE or COMP128) to compute a response value (RES) to a random challenge sent by the network. Ex-1002 ¶169.

Indeed, after describing that a profile includes "keys [and an] authentication algorithm," Park cites to a technical report on "Reprogrammable SIMs," which describes this well-known authentication procedure. Ex-1005, 297, 303; Ex-1027, 21-22 (explaining that, as part of the authentication process, a SIM "us[es] the RAND [received from the network] and its own copy of Ki and the A3 algorithm … to generate the signed response (called SRES) and passes this to the network").

Thus, Park-GlobalPlatform-AbiChar renders obvious Claim 1.

3. Dependent Claims 3, 6-11, 13-17

a. Claim 3: The mobile device of claim 1, wherein the eUICC operates within a universal integrated circuit card within the mobile device.

Park-GlobalPlatform-AbiChar teaches Claim 3. Ex-1002 ¶171. Park teaches that the eUICC "is a new form of UICC (Universal Integrated Circuit Card) [], soldered into a device during manufacturing." Ex-1005, 297.

b. Claim 6: The mobile device of claim 1, wherein the network application is configured to communicate with i) the wireless network and ii) the eUICC in the mobile device using a system bus.

Park-GlobalPlatform-AbiChar teaches Claim 6. Ex-1002 ¶¶172-74.

As illustrated in Figure 5, below, Park's DM (claimed "network application") communicates with both the SM-SR and the eUICC:

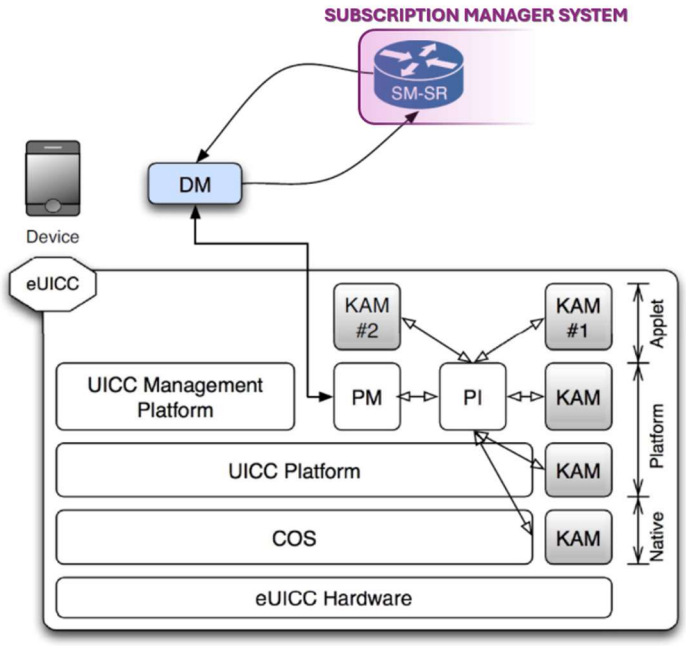


Fig. 5. Internal Architecture of eUICC

As explained for 1[c], a POSITA would have understood that Park's DM would interface with the device's radio—including its transmit and receive antenna(s)—to enable the wireless communications between the DM and the SM-SR. Ex-1002 ¶174. A POSITA would further have understood that the device processor executing the DM would communicate with the eUICC and the radio over a system bus. *Id*. Indeed, it was well-known to use a system bus to enable communications between hardware components in a mobile device. *Id*.

c. Claim 7: The mobile device of claim 1, wherein the eUICC comprises computer executable instructions for a processor in the mobile device, and wherein the computer executable instructions are stored within the memory.

Park-GlobalPlatform-AbiChar teaches Claim 7. Ex-1002 ¶¶175-76.

Park teaches that the eUICC includes "eUICC Hardware," together with a "software running in the eUICC," such as the "Key Agreement Module (KAM)," "Profile Installer (PI)," and "Profile Manager (PM)." Ex-1005, 299. A POSITA would have understood that the eUICC's software modules correspond to machine-readable instructions stored in the eUICC's memory, that are executed by the eUICC's processor(s) (claimed "processor in the mobile device") to perform the described operations, such as key agreement and profile installation. Ex-1002 ¶176.

d. Claim 8: The mobile device of claim 1, wherein the eUICC comprises a package soldered onto a circuit board of the mobile device.

Park-GlobalPlatform-AbiChar teaches Claim 8. Ex-1002 ¶177. Park teaches that the eUICC "is a new form of UICC (Universal Integrated Circuit Card) [], soldered into a device during manufacturing." Ex-1005, 297.

e. Claim 9: The mobile device of claim 1, further comprising a user interface configured to receive user identification information before the mobile device receives the symmetric key.

Park-GlobalPlatform-AbiChar teaches Claim 9. Ex-1002 ¶¶178-180.

GlobalPlatform teaches that secure element (such as an eUICC) may be protected by a "Global PIN" that provides "a mechanism for a Cardholder Verification Method," to prevent "access violations." Ex-1006, 71. A POSITA would have understood that this operation involves the eUICC being operably connected to a host module—such as a handset, terminal, or other interface device—

that provides a user interface (e.g., keypad or touchscreen) through which the user can enter the Global PIN (claimed "user identification information"). Ex-1002 ¶179.

A POSITA would have understood that requiring a user to enter the Global PIN before provisioning the eUICC with secret keys, such as the DEK (claimed "symmetric key"), would provide an additional layer of protection by ensuring that only an authorized user or operator could trigger a "PERFORM SECURITY OPERATION [decipher] command" (Ex-1006, 255-56) to load a new DEK onto the eUICC. Ex-1002 ¶180.

f. Claim 10: The mobile device of claim 1, wherein the first portion of the eUICC profile includes the network parameters, the network parameters comprising a list of numbers associated with a mobile network operator.

Park-GlobalPlatform-AbiChar teaches Claim 10. Ex-1002 ¶¶181-82.

As explained for 1[d][4], Park teaches that the first portion of the profile includes a "Network Access Application" (NAA) with network parameters associated with the MNO that issued the profile. It would have been well-known to a POSITA that such parameters would include a list of numbers. Ex-1002 ¶182. For instance, according to well-known 3GPP/ETSI standards, the network parameters would include the "Public Land Mobile Network" (PLMN) list—a list of MNO-preferred networks, in priority order, that the eUICC should connect to when roaming, each identified numerically using the operator's mobile country code

(MCC) and mobile network code (MNC). Ex-1002 ¶182. Indeed, the "Reprogrammable SIMs" technical report cited by Park highlights this PLMN list as being one of the pieces of information stored on a SIM profile. Ex-1027, 17 ("The Public Land Mobile Network (PLMN) selector is a list of MNO-preferred networks in priority order … [which] allows the MNO to control which visited networks to use (i.e. when roaming or coverage is lost).").

g. Claim 11: The mobile device of claim 1, wherein the network parameters comprise a mobile country code (MCC) and a mobile network code (MNC) associated with the wireless network.

Park-GlobalPlatform-AbiChar teaches Claim 11 for the reasons explained for Claim 10. Ex-1002 ¶183.

h. Claim 13: The mobile device of claim 1, wherein the subscriber identity comprises an International Mobile Subscriber Identity (IMSI).

Park-GlobalPlatform-AbiChar teaches Claim 13. Ex-1002 ¶184. As explained for 1[c][2], Park teaches that the profile provisioned to the eUICC includes an "IMSI (International Mobile Subscriber Identity)." Ex-1005, 297.

i. Claim 14: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, a ciphertext for the symmetric key, wherein the mobile device is configured to decrypt the ciphertext using at least the eUICC private key.

Park-GlobalPlatform-AbiChar teaches Claim 14. Ex-1002 ¶185. As explained for 1[c][2], in the combined system, the SM-DP would send the DEK (claimed

"symmetric key") to the eUICC, encrypted with the eUICC's public key. The encrypted DEK corresponds to the claimed "ciphertext." Ex-1002 ¶185. A POSITA would have understood that, under standard principles of public-key cryptography, data encrypted with a public key must be decrypted with the corresponding private key. *Id*. Thus, where the SM-DP encrypts the DEK using the eUICC's public key, the eUICC necessarily uses its private key to decrypt that ciphertext and recover the DEK. *Id*.

j. Claim 15: The mobile device of claim 1, wherein the mobile device further comprises at least one of a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a tracking device, and a circuit board with the radio.

Park-GlobalPlatform-AbiChar teaches Claim 15. Ex-1002 ¶¶186-88.

Park teaches that the field of use of the eUICC has extended to include "Consumer Electronic Devices." Ex-1005, 297. Indeed, as illustrated in Figure 5, below, Park illustrates its eUICC as being housed within a smartphone:

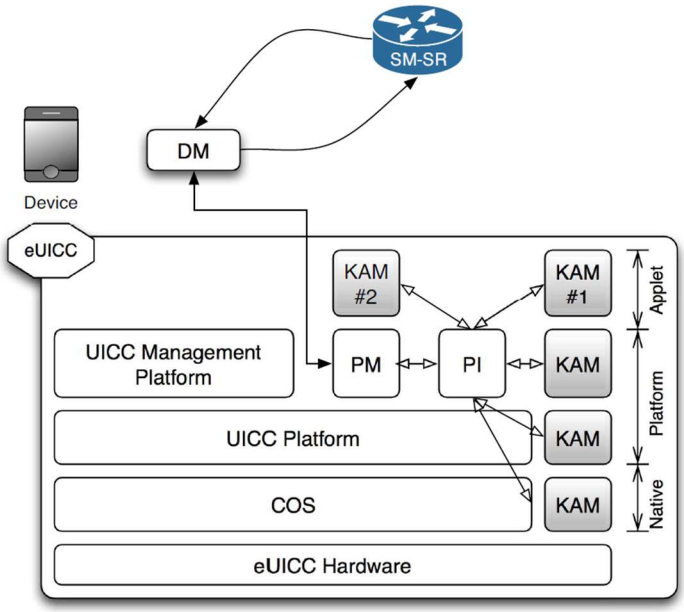


Fig. 5. Internal Architecture of eUICC

As explained for 1[c], A POSITA would have understood that Park's DM would interface with a radio on the device to enable wireless communications with the SM-SR. Ex-1002 ¶188. A POSITA would have recognized that such a radio would be included in a circuit board of the device. *Id*.

k. Claim 16: The mobile device of claim 1, wherein the second memory is the same memory as the first memory.

Park-GlobalPlatform-AbiChar teaches Claim 16. Ex-1002 ¶¶189-190.

A POSITA would have understood that the "first memory" for storing an eUICC identity (which would likely be nonvolatile) could also be the "second memory" used in conjunction with the random number generator, especially if the random eUICC private key n_a needs to be available through a power cycle. Ex-1002

¶190. A POSITA would have viewed this as being a simple matter of design choice. *Id*.

l. Claim 17: The mobile device of claim 1, wherein the one or more receiving antennas are the one or more transmit antennas.

Park-GlobalPlatform-AbiChar teaches Claim 17. Ex-1002 ¶191. It would have been well-known to a POSITA that the same antenna in a mobile device is commonly used for both transmitting and receiving signals over a wireless network. *Id*. Indeed, the "Reprogrammable SIMs" technical report cited by Park describes a handset with a single antenna. Ex-1027, 15 (explaining that "the SIM [] securely communicate[s] (via the handset and ***its antenna***) with the MNO's transmitters and servers").

B. Ground 2: Claims 1, 3, 6-11, 13-17 are obvious over Park in view of GlobalPlatform and X9.63-Overview

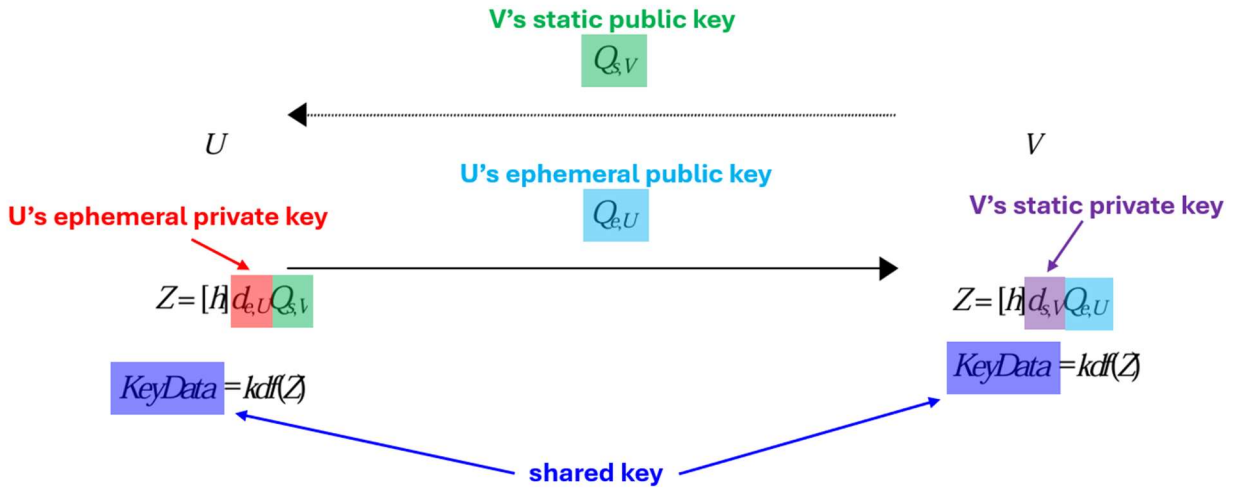
1. A POSITA would have been motivated to combine Park's teachings with GlobalPlatform's and X9.63-Overview's teachings and would have had a reasonable expectation of success.

A POSITA would have been motivated to combine Park's secure profile provisioning architecture (SPA) with GlobalPlatform's procedures for sensitive data encryption, for the same reasons as explained for Ground 1, above. A POSITA would further have been motivated to combine Park's SPA with X9.63-Overview's 1-pass Diffie-Hellman key agreement protocol, to implement a specific embodiment

of Park's asymmetric key-exchange mechanism that is well-suited for Park's architectural environment, in which eUICC's are considered "resource-constrain[ed]" devices, for which "overhead for the security-related operations" is undesirable." Ex-1005, 299. Ex-1002 ¶192.

As X9.63-Overview illustrates, the parties exchange public keys, Q_{sV} and Q_{eU}, and then each side combines the other side's public key with its own private key—for example, the eUICC uses its **random private key $d_{e,U}$** together with the **received public key $Q_{s,V}$**—to generate a shared secret:

ANSI X9.63 - 1-Pass DH



Ex-1008, 12. From that shared secret, each party can then derive the same symmetric key, **KeyData**, corresponding to the profile key. A POSITA would have understood that a one-pass DH exchange offers forward secrecy to the eUICC side of the

communication. Ex-1002 ¶193. In the one-pass approach, the eUICC generates a fresh ephemeral public/private key pair for each session, ensuring that even if its long-term private key were later compromised, previously provisioned profiles could not be decrypted. *Id*.

2. Independent Claim 1

a. 1[pre]-1[a], 1[c], 1[c][2]-1[d], 1[d][2]-1[d][5]:

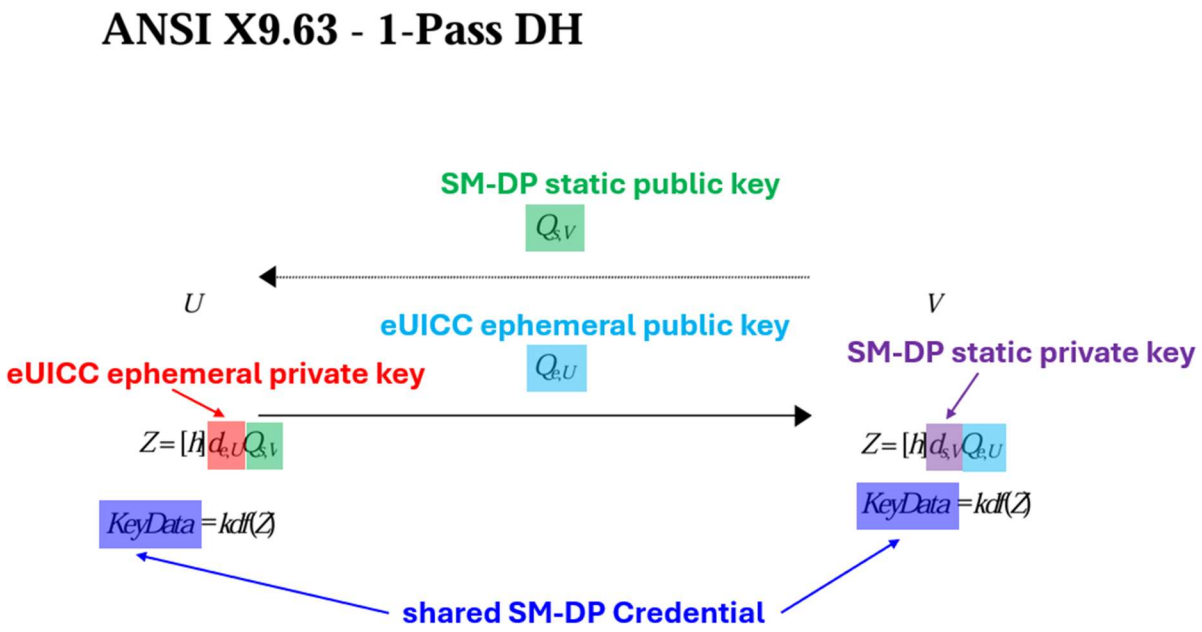
Park in view of GlobalPlatform and X9.63-Overview ("Park-GlobalPlatform-X9.63-Overview") teaches elements 1[pre]-1[a], 1[c], 1[c][2]-1[d], and 1[d][2]-1[d][5] for the same reasons as explained for Ground 1. Ex-1002 ¶194.

b. 1[b]: a random number generator operably connected to a processor connected to a second memory configured to generate a random number for an eUICC private key corresponding to an eUICC public key;

Park-GlobalPlatform-AbiChar teaches 1[b]. Ex-1002 ¶¶195-98.

(1) generating "a random number for an eUICC private key corresponding to an eUICC public key" using a "random number generator"

X9.63-Overview's 1-pass Diffie-Hellman key exchange is illustrated below:



Ex-1008, 12. In Park-GlobalPlatform-X9.63-Overview, the eUICC generates an **ephemeral private key $d_{e,U}$ (claimed "eUICC private key")**. *Id*. The eUICC then calculates a **corresponding ephemeral public key $Q_{e,U}$ (claimed "eUICC public key")**. Ex-1008, 12. X9.63-Overview teaches that **ephemeral private key $d_{e,U}$** is "selected randomly." *Id*., 7. A POSITA would have understood that the eUICC would include a random number generator—e.g., within, or coupled to, Park's KAM software—for use in generating the random number for **ephemeral private key $d_{e,U}$**. Ex-1002 ¶¶196-97.

(2) the random number generator "operably connected to a processor connected to a second memory"

Park teaches that the random number generator is operably connected to a processor connected to a second memory, for the same reasons explained for Ground 1. Ex-1002 ¶198.

c. 1[c][1]: a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and

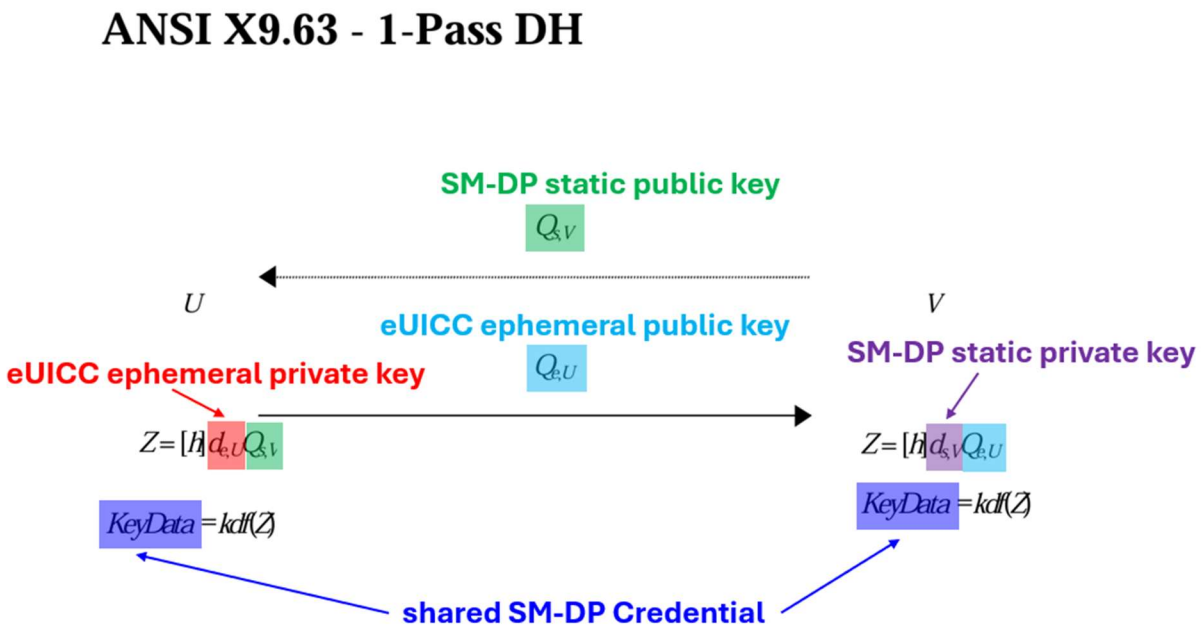
Park-GlobalPlatform-X9.63-Overview teaches 1[c][1]. Ex-1002 ¶¶199-201.

(1) transmit the eUICC identity to a subscription manager

Park teaches transmitting the eUICC identity to a subscription manager, for the same reasons explained for Ground 1. Ex-1002 ¶200.

(2) transmit the eUICC public key to the subscription manager

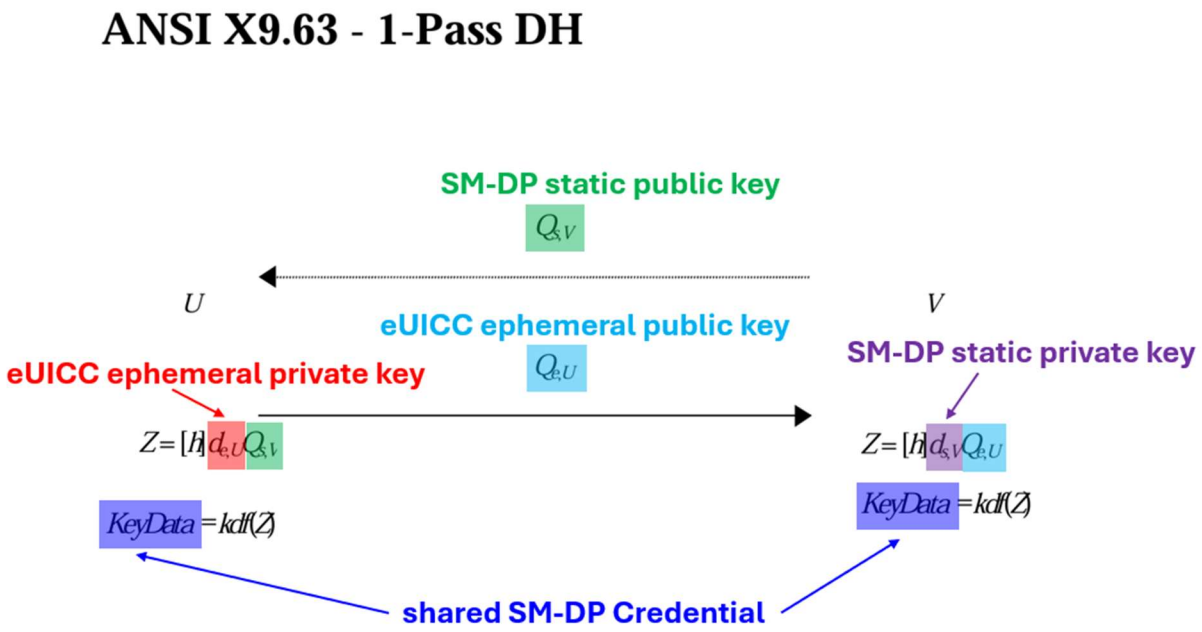
In the combined system, Park's KAM uses X9.63-Overview's 1-pass Diffie-Hellman key exchange to generate a private key $d_{e,U}$ and **corresponding public key $Q_{e,U}$ (claimed "eUICC public key")**. Ex-1008, 12. That public key is sent to the SM-DP (via SM-SR), as illustrated below, so that it can be combined with a private key $d_{s,V}$ generated by the SM-DP, to generate the shared SM-DP credential/$key_{SM\text{-}DP}$. *Id*.



d. 1[d][1]: a. derive a profile key using an elliptic curve Diffie-Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key;

Park-GlobalPlatform-X9.63-Overview teaches 1[d][1]. Ex-1002 ¶¶202-03.

As explained above for elements 1[b] and 1[c], Park's eUICC and SM-DP use X9.63-Overview's 1-pass Diffie-Hellman key exchange to each generate a copy of Park's shared SM-DP credential/$key_{SM\text{-}DP}$ as illustrated below. Ex-1008, 12; Ex-1005, 300.



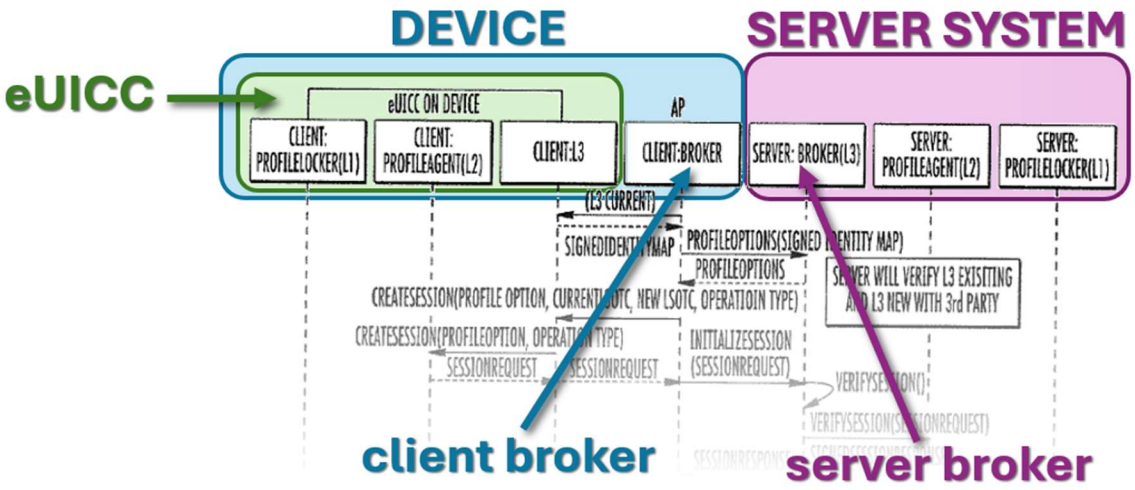
3. Dependent Claims 3, 6-11, 13-17

Park-GlobalPlatform-X9.63-Overview teaches Claims 3, 6-11, and 13-17 for the same reasons as explained for Ground 1. Ex-1002 ¶204.

C. Ground 3: Claims 2 and 12 are obvious over Grounds 1 or 2 in view of Haggerty

1. A POSITA would have been motivated to add Haggerty to Park-GlobalPlatform-AbiChar or Park-GlobalPlatform-X9.63-Overview and would have had a reasonable expectation of success.

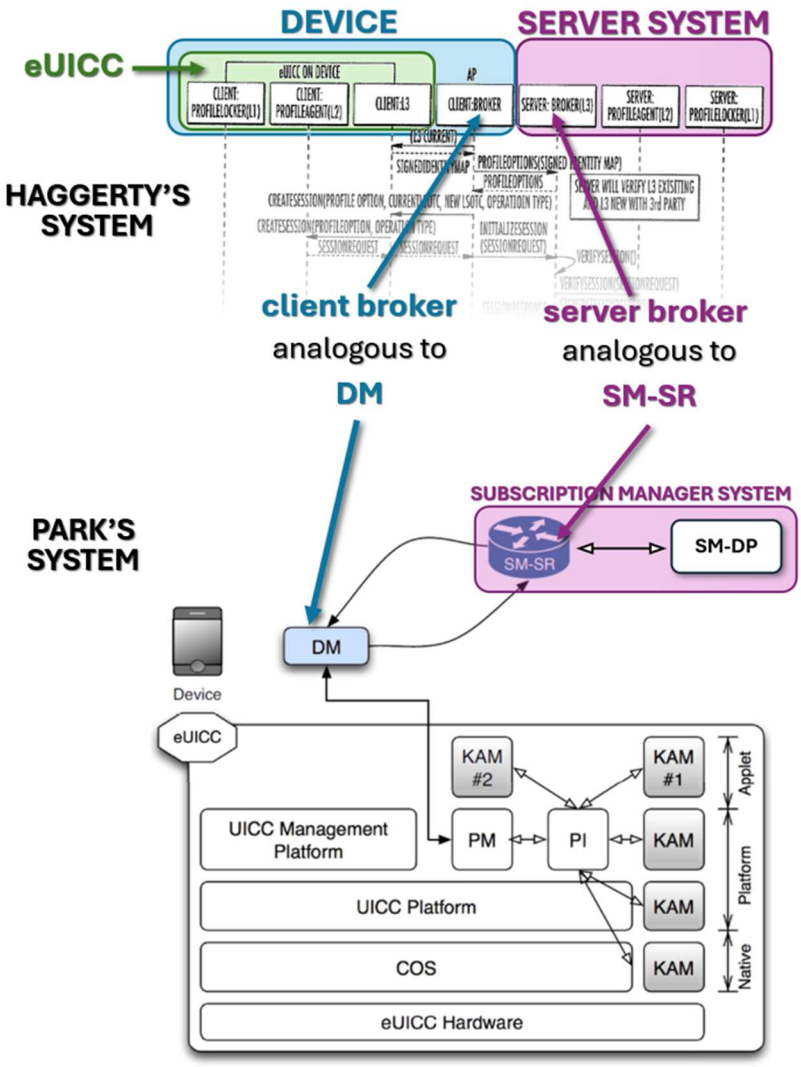
Haggerty teaches a broker-based architecture for secure eSIM provisioning in which communications between an eUICC and a backend provisioning server are mediated by two intermediary components—a device broker and a server broker, as illustrated in excerpted Figure 9, below.



Haggerty's device broker resides on the eUICC-containing device, and passes profile download requests, for example, to the provisioning infrastructure. Ex-1013, ¶¶97, 104. The server broker operates within the provisioning server system, and receives those requests, forwarding them to the "profile agent" or "profile locker." Ex-1013 ¶¶105, 108, Fig. 9. Communications between the two brokers are protected using a standard secure transport layer protocol, such as Transport Layer Security (TLS), to prevent interception or replay attacks. Ex-1013 ¶100.

Haggerty's architecture closely parallels that of Park. Ex-1002 ¶¶205-07. Haggerty's device broker is analogous to Park's Device Module (DM)—each serves as the intermediary on the device side, interfacing between the eUICC and the remote provisioning infrastructure. Likewise, Haggerty's server broker is analogous to Park's SM-SR—each is responsible for receiving provisioning requests from the

device, and routing them to the appropriate profile provisioning components. Ex-1002 ¶207.



Park teaches that the DM and SM-SR communicate over a "secure communication channel," but leaves implementation details to the designer. Ex-1005, 300. Haggerty teaches using TLS as the secure transport layer. Ex-1013 ¶100. A POSITA would have used Haggerty's TLS for Park's secure communication channel. Ex-1002 ¶208. TLS was a well-established, standardized protocol

providing confidentiality, integrity, and mutual authentication—exactly the security objectives Park seeks to achieve. *Id*.

Haggerty teaches that, when provisioning a profile, certain information, such as the ICCID, is kept in plaintext (Ex-1013, ¶84), enabling the provisioning servers to identify and manage the profile without decrypting its full eSIM payload. Ex-1013 ¶¶54, 105. A POSITA would have understood that incorporating Haggerty's teaching into Park's system would enable Park's SM-SR (analogous to Haggerty's server broker) to use the plaintext ICCID for profile identification and routing, while maintaining end-to-end encryption for the sensitive profile content. Ex-1002 ¶209. This would improve operational efficiency and scalability—allowing Park's SM-SR to handle multiple profiles—without compromising confidentiality. *Id*.

2. Claim 2: The mobile device of claim 1, wherein the eUICC is further configured to receive a profile identity for the eUICC profile as a plaintext.

Park-GlobalPlatform-AbiChar-Haggerty and Park-GlobalPlatform-X9.63-Overview-Haggerty teach Claim 2. Ex-1002 ¶¶210-11.

Haggerty teaches that, when encrypting an eSIM for delivery to an eUICC, certain metadata fields, including the Integrated Circuit Card Identifier ("ICCID"), should remain as plaintext. Ex-1012 ¶84. For example, Haggerty's batch descriptor contains "information for the eSIM" and includes "a plain text section … that consists of: an ICCID for each profile." *Id*. ¶85, Fig. 7. In other words, the plaintext

ICCID identifies each profile. Ex-1002 ¶210. In the combined systems, this would allow Park's SM-SRs and receiving devices to identify profiles without decrypting the full payload. Ex-1012, ¶¶54, 105; Ex-1002 ¶211.

3. Claim 12: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, the eUICC profile using transport layer security.

Park-GlobalPlatform-AbiChar-Haggerty and Park-GlobalPlatform-X9.63-Overview-Haggerty teach Claim 12. Ex-1002 ¶¶212-13.

Haggerty teaches that "a security protocol (e.g., transport layer security (TLS))" is used to protect communications between Haggerty's "device broker" (analogous to Park's DM) and "server broker" (analogous to Park's SM-SR, respectively). Ex-1013, ¶100. In the combined systems, Haggerty's TLS would be used to protect the profile delivered by the SM-SR to the device, to "prevent capture and replay attacks." Ex-1013, ¶100; Ex-1002 ¶213.

D. Ground 4: Claims 4-5 are obvious over Grounds 1 or 2 in view of Pierce

1. A POSITA would have been motivated to add Pierce to Park-GlobalPlatform-AbiChar, or Park-GlobalPlatform-X9.63-Overview and would have had a reasonable expectation of success.

Both AbiChar and X9.63-Overview teach the use of a random number generator (RNG) to generate private keys for use in an elliptic curve Diffie-Hellman

key exchange. Ex-1007, 3; Ex-1008, 7, 12. But none provides details about the RNG to be used. Ex-1002 ¶214.

Pierce teaches a method "for use by an embedded processing device within a manufactured product," to generate strong cryptographic keys using a "pseudo random number generator" (PRNG). Ex-1013, Abstract. Pierce teaches seeding a PRNG with entropy data from sources that are naturally available to such embedded devices, such as sensor outputs, timing data (e.g., GPS time), unique identifiers, and/or transient events on the communication bus, to generate seed values for the PRNG. Ex-1013 ¶¶35-38, Fig. 3. A POSITA would have recognized that incorporating Pierce's method would improve the security of the Park-GlobalPlatform-AbiChar and Park-GlobalPlatform-X9.63-Overview systems, by helping to ensure that the private keys used in their ECDH exchanges were derived from sufficiently random and unpredictable sources that were readily available to the eUICC-storing devices in these systems. Ex-1002 ¶215.

2. Claim 4: The mobile device of claim 1, wherein the random number generator is configured to generate the random number in response to input from at least one of a clock and a sensor.

Claim 5: The mobile device of claim 1, wherein the random number generator is configured to generate the random number from a seed value, wherein the seed value comprises data from at least one of a sensor, the radio, a bus, a clock, a physical interface, the memory, and an operating system.

Park-GlobalPlatform-AbiChar-Pierce, and Park-GlobalPlatform-X9.63-Overview-Pierce teach Claims 4-5. Ex-1002 ¶¶216-17.

Pierce teaches a random number generator configured to generate random numbers in response to receiving a seed value in the form of "entropy data" "from a sensor." Ex-1013 ¶36.

E. Ground 5: Claims 10-11 are obvious over Grounds 1 or 2 in view of Konstantinou

1. A POSITA would have been motivated to add Konstantinou to Park-GlobalPlatform-AbiChar, or Park-GlobalPlatform-X9.63-Overview, and would have had a reasonable expectation of success.

Park teaches procedures for remotely provisioning profiles onto eUICCs. Ex-1005, 297. While the profile includes NAAs (Ex-1005, 297), Park does not specify what those network access parameters include. Ex-1002 ¶218. Konstantinou fills that gap by teaching that according to "TIA/EIA/IS-683-D: Over-the-Air Service Provisioning of Mobile Stations," a profile's MSPL (Multi-mode System Priority List) includes "MCC [mobile country code] / MNC [Mobile Network Code]" entries.

Ex-1014 ¶¶31, 158, 163, 166. A POSITA would have turned to Konstantinou's detailed disclosure to determine what Park's network access parameters include. Ex-1002 ¶218.

2. Claim 10: The mobile device of claim 1, wherein the first portion of the eUICC profile includes the network parameters, the network parameters comprising a list of numbers associated with a mobile network operator.

Claim 11: The mobile device of claim 1, wherein the network parameters comprise a mobile country code (MCC) and a mobile network code (MNC) associated with the wireless network.

Park-GlobalPlatform-AbiChar-Konstantinou, and Park-GlobalPlatform-X9.63-Overview-Konstantinou teach Claims 10-11. Ex-1002 ¶¶219-220.

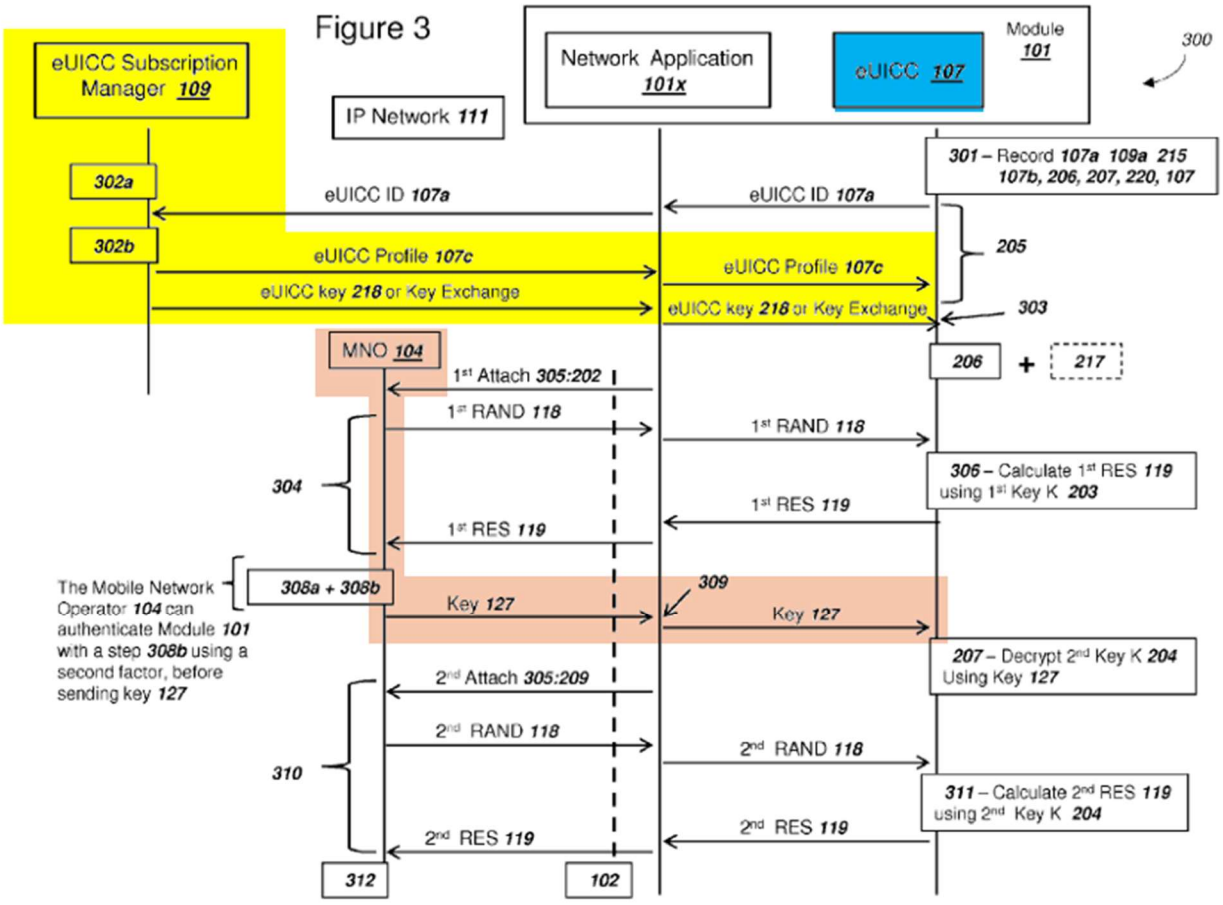
As explained for Grounds 1 and 4, 1[d][4], Park explains the first profile portion includes Network Access Application (NAA) parameters. Konstantinou teaches that such network parameters include numerical "MCC/MNC" values according to TIA standards. Ex-1014 ¶31; Ex-1002 ¶220.

F. Ground 6: Claims 1-17 are obvious over Nix175 in view of Park and GlobalPlatform

1. A POSITA would have been motivated to combine Nix175, Park, and GlobalPlatform and would have had a reasonable expectation of success.

Nix175 discloses the claims of the '893 Patent with the exception of claim element 1[c][2] "receiving, from the subscription manager … the symmetric key." As discussed above in Sections **Error! Reference source not found.** and **Error!**

Reference source not found., the '893 Patent (and Nix175) introduces the claimed "symmetric key" to address a security concern that arises if distribution and release of the profile (including decryption of the secret key K) were to be under the control of the SM and not the MNO. Ex-1016, 3:32-36, 34:27-45; Ex-1002 ¶¶221-22. Nix175's solution to the security problem allows the SM to handle delivery the encrypted profile but requires that the MNO handle delivery of the symmetric key, without which the eUICC cannot decrypt the portion of the profile containing key K. *Id*. 34:54-60. This architecture is depicted in Figure 3 of Nix175, annotated below:



Above, the subscription manager (yellow) provides the encrypted eUICC profile 107c to the eUICC (blue). But the eUICC cannot decode key K ("2nd Key K 204) until it receives symmetric key 127 (red) from the MNO 104. Ex-1016, Fig. 3.

While Nix175's introduction of a symmetric key controlled and delivered by the MNO addresses the security issue by preventing the SM from being able to access the secure key K, a POSITA would have recognized that it imposes an undue burden on the MNO, which now must handle key management and delivery for every eUICC. Ex-1002 ¶223. Thus a POSITA would have been motivated to look to

Park, which teaches a split architecture for the subscription manager that divides it into two parts: "SM-DP (Data Preparation)" for generating and encrypting the operator profile, and "SM-SR (Secure Routing)" for transporting and installing the encrypted profile onto the eUICC, as shown in Park's Figure 1 below. Ex-1005, 297; Ex-1002 ¶¶82-83.

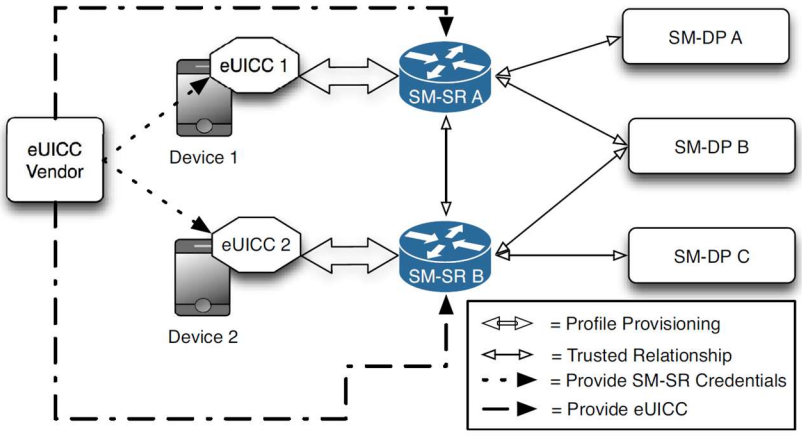


Fig. 1. eUICC Profile Ecosystem

By splitting the SM, Park allows for SM-SR, which securely routes the encrypted profile to the eUICC, to exist in a different trust zone[4] and potentially be operated by a different entity than SM-DP and the MNO, thereby allowing SM-DP to negotiate profile encryption keys with the eUICC without exposing them to the SM-SR or other intermediaries. Ex-1005, 299-301. Thus, a POSITA would have understood that Park's SM-DP would maintain control of the encryption of critical

[4] "Because the profile is security sensitive to the SM-DP itself and the customer, it is obvious that each SM-DP is hardly willing to reveal their generated profile to others even SM-SR." Ex-1005, 297.

data like key K, and SM-SR would deliver the encrypted profile to the eUICC but would not have access to the symmetric key, thereby solving the security problem while freeing the MNO from having to directly manage key delivery to each eUICC. Ex-1002 ¶¶82-83, 224.

In this combined system, a POSITA also would have recognized advantages to continuing to encrypt key K with a symmetric key that is separate from the key used to encrypt the overall profile. Ex-1002 ¶¶55-56, 225.

In particular, in embodiments of Nix175's system in which the profile key (the symmetric key used to encrypt the overall profile) is generated dynamically through a key-exchange protocol with the eUICC, the SM-DP would not be able to pre-encrypt the profile with the profile key. At the same time, a POSITA would have understood that sensitive data, such as key K, should not be stored at the SM-DP in plaintext. Ex-1002 ¶226 (citing Ex-1023, NIST SP 800-57, 73). Thus, encrypting key K under a separate symmetric key would help ensure that the SM-DP could store and handle key K securely, before establishing the profile key with the eUICC. Ex-1002 ¶226.

A POSITA would also have appreciated that retaining key K in its already-encrypted form, once the profile key has been established, and simply encrypting the entire profile (including already-encrypted key K) with that profile key, would provide additional security benefits, by providing greater protection against

compromise during transport. Ex-1002 ¶227 (citing Ex-1024, NIST SP 800-38F, 2). Indeed, Nix175 expressly contemplates this kind of layered encryption. Ex-1016, 33:60-63 ("ciphertext 208b could optionally be included within ciphertext 208a"), 37:57-67 ("a profile 107c can include multiple layers of ciphering").

This same principle is taught by GlobalPlatform, which teaches first encrypting sensitive data within a message "us[ing] the relevant data encryption session key (DEK)" and then further encrypting the message with the secure channel session key, providing layered protection for these highly sensitive materials. Ex-1006, 264, 258 (explaining that the session key, C-ENC, is used to encrypt "the command data field of the command message being transmitted to the card," which "includes any data within the data field that has ***already been protected*** for another purpose ***e.g. secret or private keys encrypted with the data encryption session key***"). This configuration is illustrated below in annotated Figure F-11. Ex-1002 ¶227.

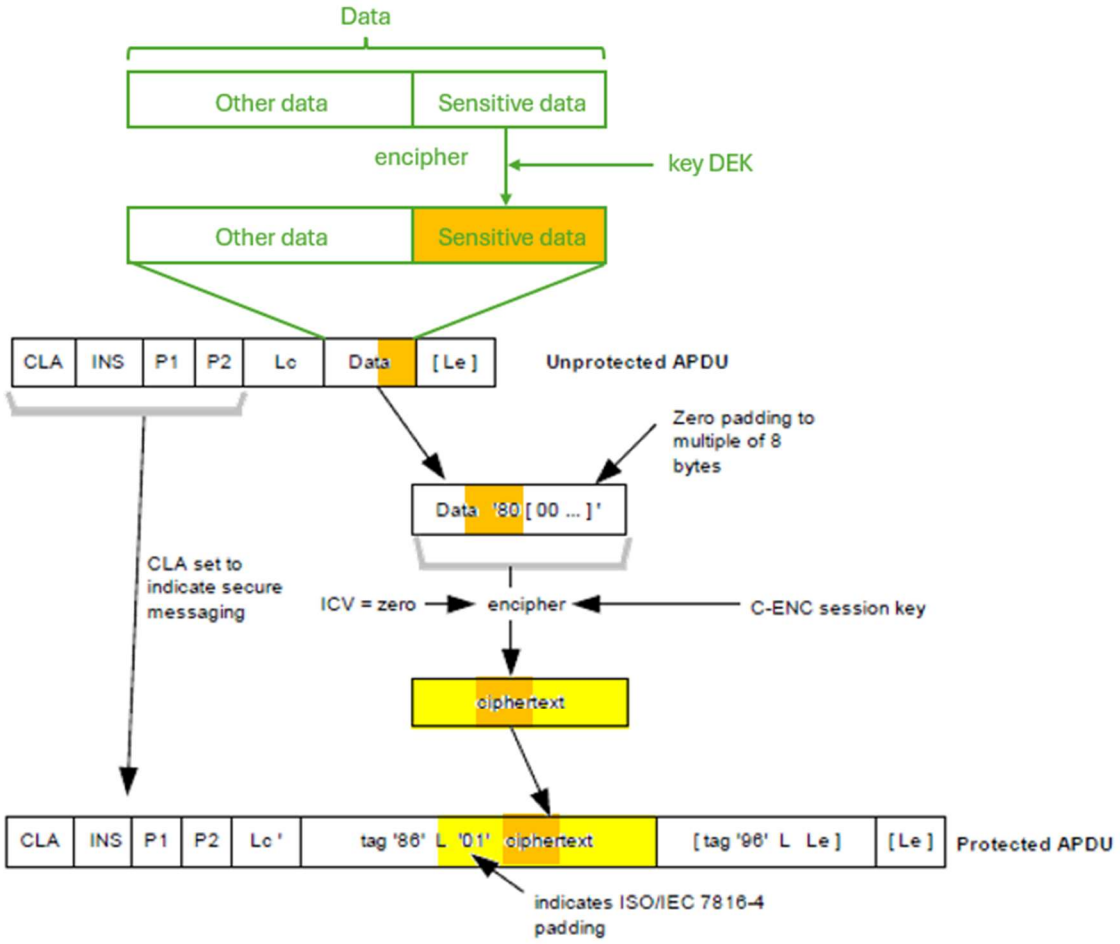


Figure F-11: Secure Messaging: Command message protected for confidentiality

Thus, in the combined system, profiles sent from the SM-DP to the eUICC would include an inner layer of encryption for sensitive materials like keys (using GlobalPlatform's DEK), as well as an outer layer of encryption using Nix175's profile key. Ex-1002 ¶229.

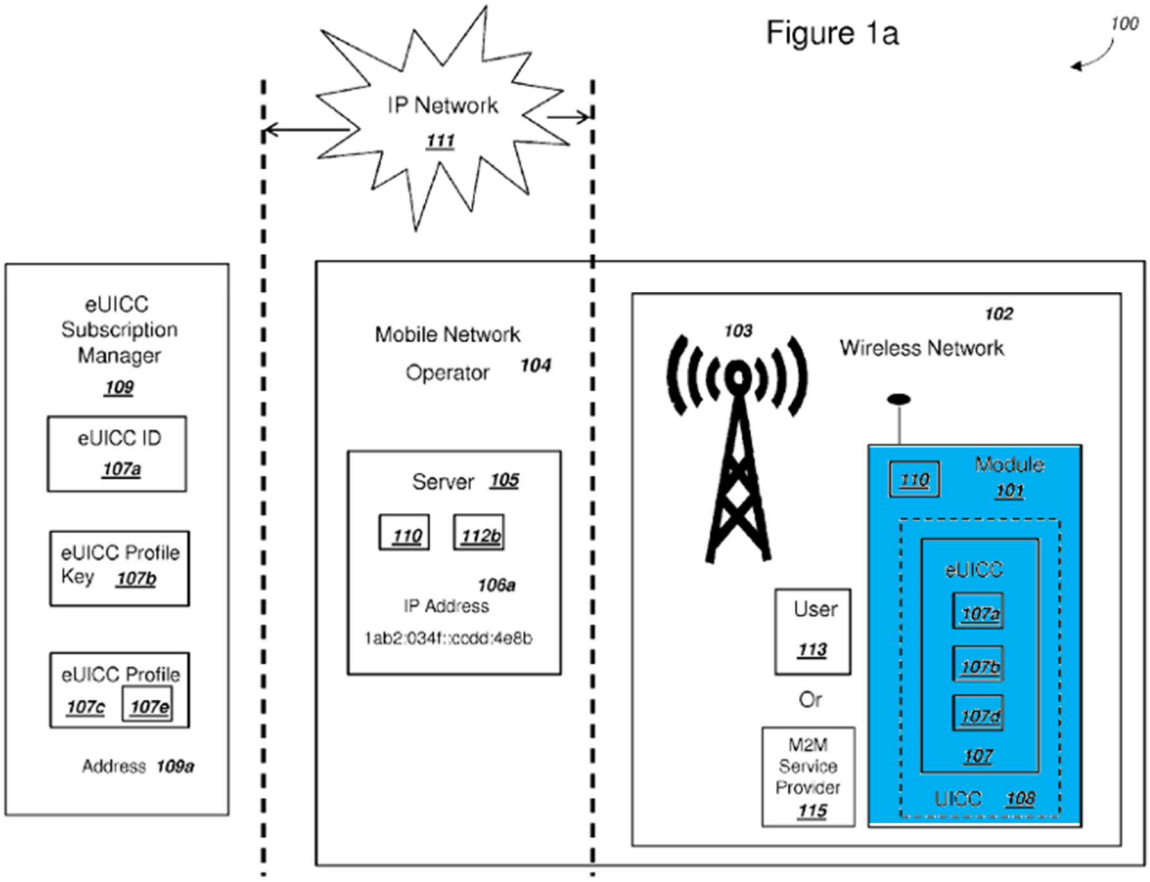
Alternatively, once the sensitive data portion (keys, IMSI) had been encrypted using DEK, it would not be necessary to further encrypt that portion of the profile with the profile key, and it would be a simple matter of design choice (computational

complexity vs. cryptographic security) to encrypt the sensitive portion only with DEK and the non-sensitive portion only with the profile key, since all of the profile would still be protected under at least one key and the sensitive portion would remain accessible only to an entity possessing the claimed "symmetric key" DEK. Ex-1002 ¶¶230-31.

2. Independent Claim 1

a. 1[pre]: A mobile device for communicating with a wireless network, the mobile device comprising:

Nix175 teaches "A module in the present invention can comprise a ***mobile phone*** such as a smartphone, and may also be referred to as a ***mobile device***, mobile station, or user equipment." Ex-1016, 4:24-27; Fig. 1a, module 101; Ex-1002 ¶232.



b. 1[a]: a first memory configured to store an embedded universal integrated circuit card (eUICC) identity;

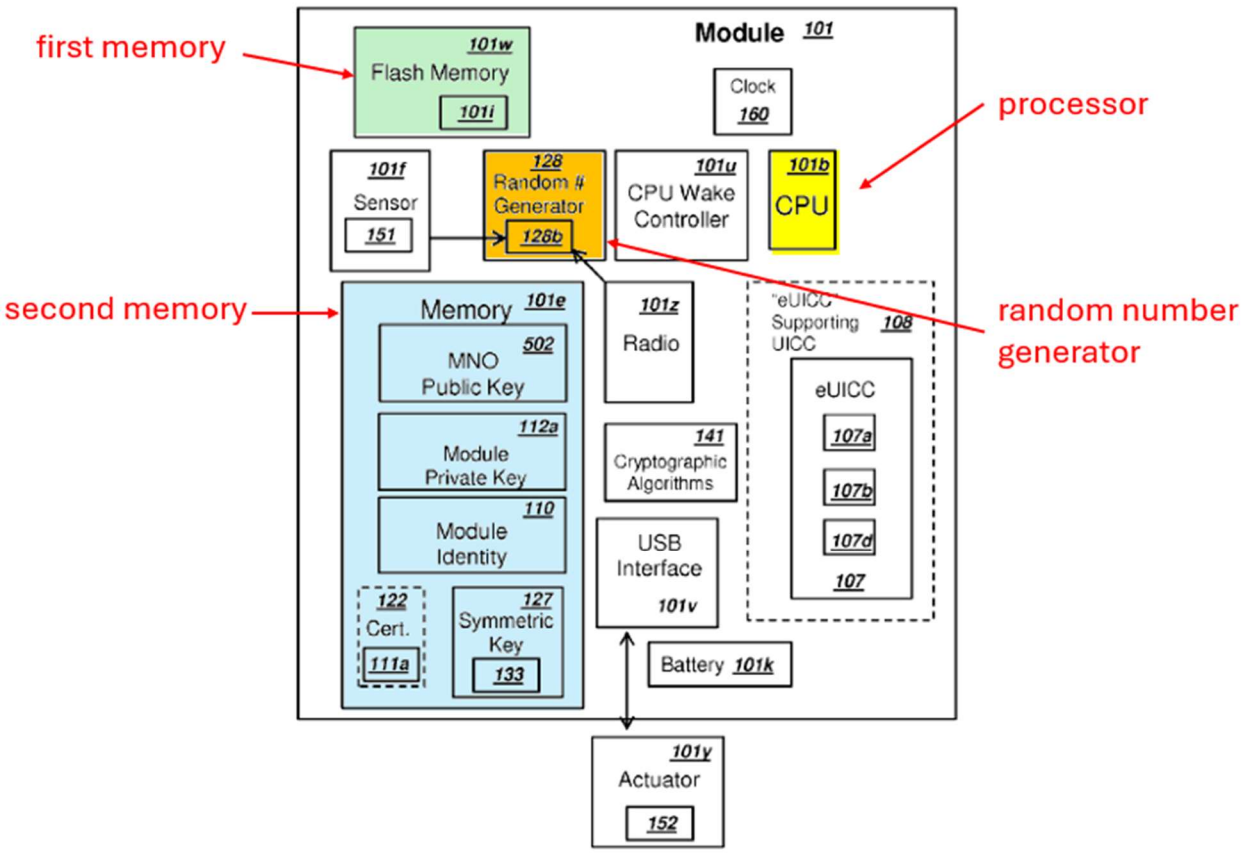
Nix175 teaches "A system for supporting authentication, the system comprising: a nonvolatile ***memory*** for recording an ***embedded Universal Integrated Circuit Card (eUICC) identity***. Ex-1016, Cl. 10. Ex-1002 ¶233.

c. 1[b]: a random number generator operably connected to a processor connected to a second memory configured to generate a random number for an eUICC private key corresponding to an eUICC public key;

Nix175 teaches "As illustrated in FIG. 1c, module 101 may also contain a random number generator 128 [orange]." Ex-1016, 22:32-33; Fig. 1c. Module 101

also includes flash memory 101w (green) (*id*. 19:24), RAM memory 101e (blue) (*id*. 19:39-41), and a CPU 101b. *Id*. 19:31-33.

Figure 1c



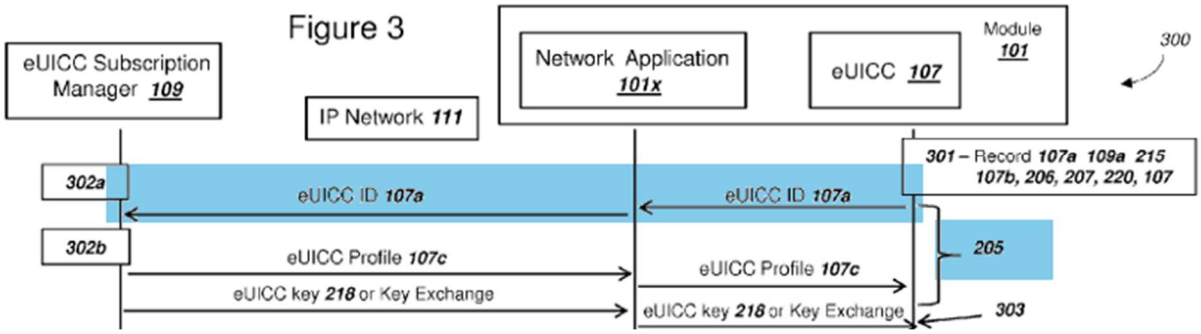
The random number generator may be used to generate the eUICC private/public key pair: "Several possibilities exist for the source of an eUICC private key 215 and eUICC public key 214 … The module 101 could derive the PKI key pair using a random number generator 128 and a set of cryptographic algorithms 141, where the random number generator 128 uses input from a sensor 101f and/or a clock 160 in order to obtain a random number with a high degree of information entropy." Ex-1016, 42:11-30. Ex-1002 ¶¶234-35.

d. 1[c]: a radio including one or more transmit antennas and one or more receiving antennas configured to:

Nix175 teaches, "module 101 can comprise a wireless module and include a radio 101z. … Although not illustrated, radio 101z could include antennas for reception and transmission of RF signals, and even multiple antennas could be used." 20:42-49. Ex-1002 ¶236.

e. 1[c][1]: a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and

As shown in Figure 3, excerpted below, Nix175's eUICC transmits the eUICC identity 107a to the subscription manager 109. Ex-1016, 48:65-66.



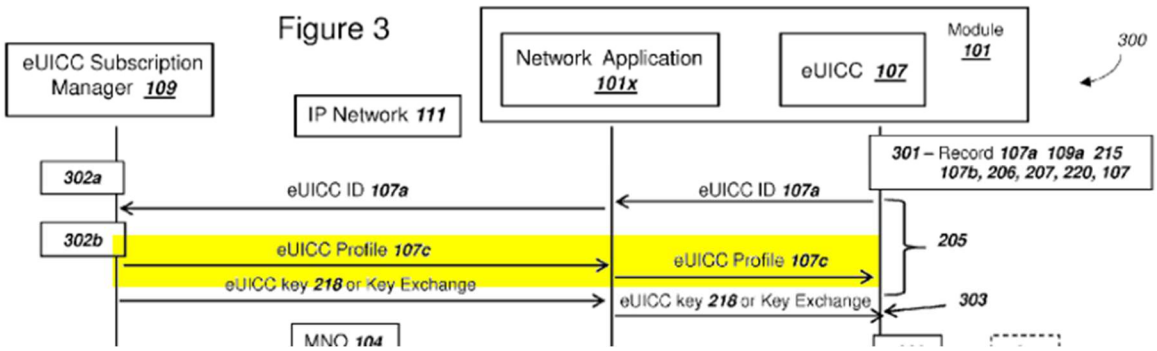
Ex-1016, Fig. 3. And "module 101 could send … send ***the eUICC public key 214*** along with the eUICC identity 107a (possibly with or in the form of a module identity 110) ***to an eUICC subscription manager 109*** before the module 101 receives the encrypted eUICC profile 170c." *Id*. 42:37-42. Ex-1002 ¶¶237-38.

f. 1[c][2]: b. receive, from the subscription manager, i) an eUICC profile comprising network parameters, a key K, and a subscriber identity and ii) a symmetric key; and

Nix175-Park-GlobalPlatorm teaches 1[c][2]. Ex-1002 ¶239.

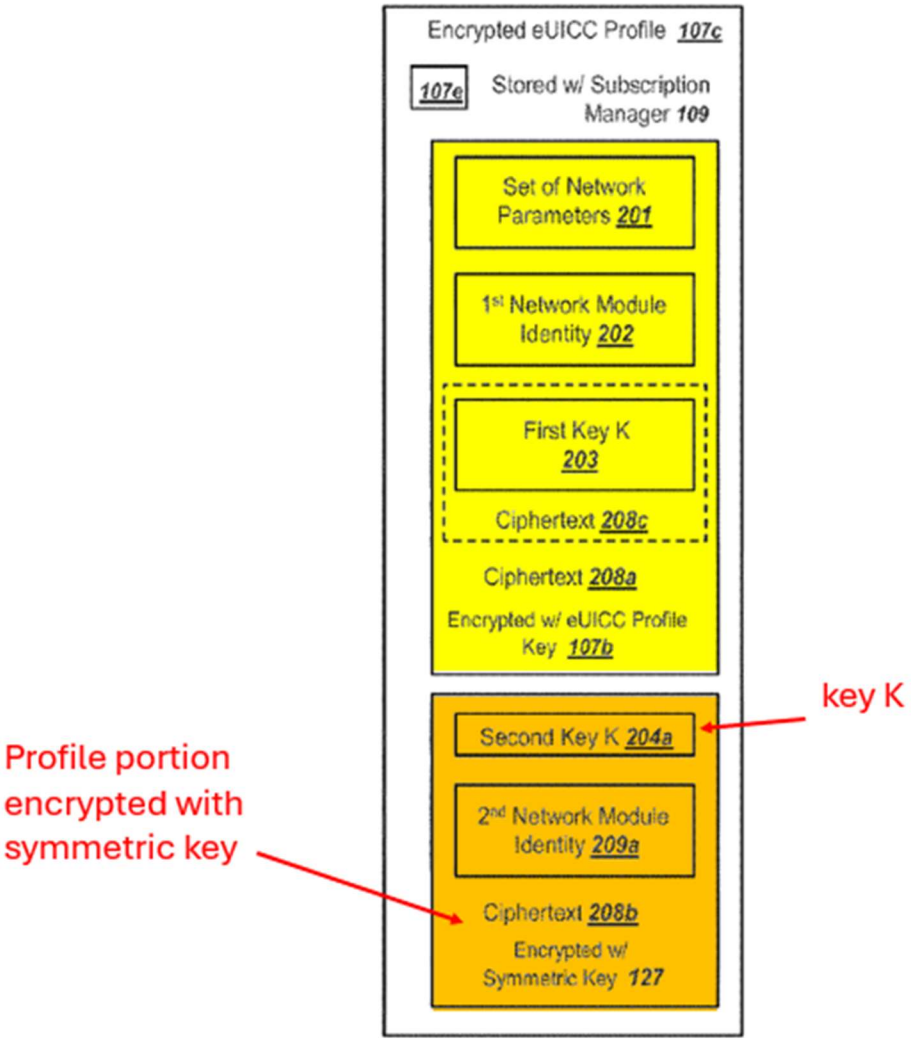
(1) eUICC profile comprising network parameters, a key K, and a subscriber identity

Nix175 shows the module receiving the eUICC profile 107c from the eUICC subscription manager 109 in Figure 3. Ex-1016, Fig. 3.



Nix175 further teaches "receiving, by the hardware module, a profile from the eUICC subscription manager, wherein the hardware module uses the profile key to decrypt a first portion of the profile, wherein the first portion includes a first key K1 … [and] wherein the hardware module uses the symmetric key to decrypt the second portion of the profile, and wherein the second portion includes a ***second key K2***." Ex-1016, Cl. 1. The portion of the profile encrypted with the symmetric key and comprising ciphertext 208b including "***second key K 204a***" (the claimed "key K") and the ***network identity 209a*** (claimed "subscriber identity"), is shown in orange in

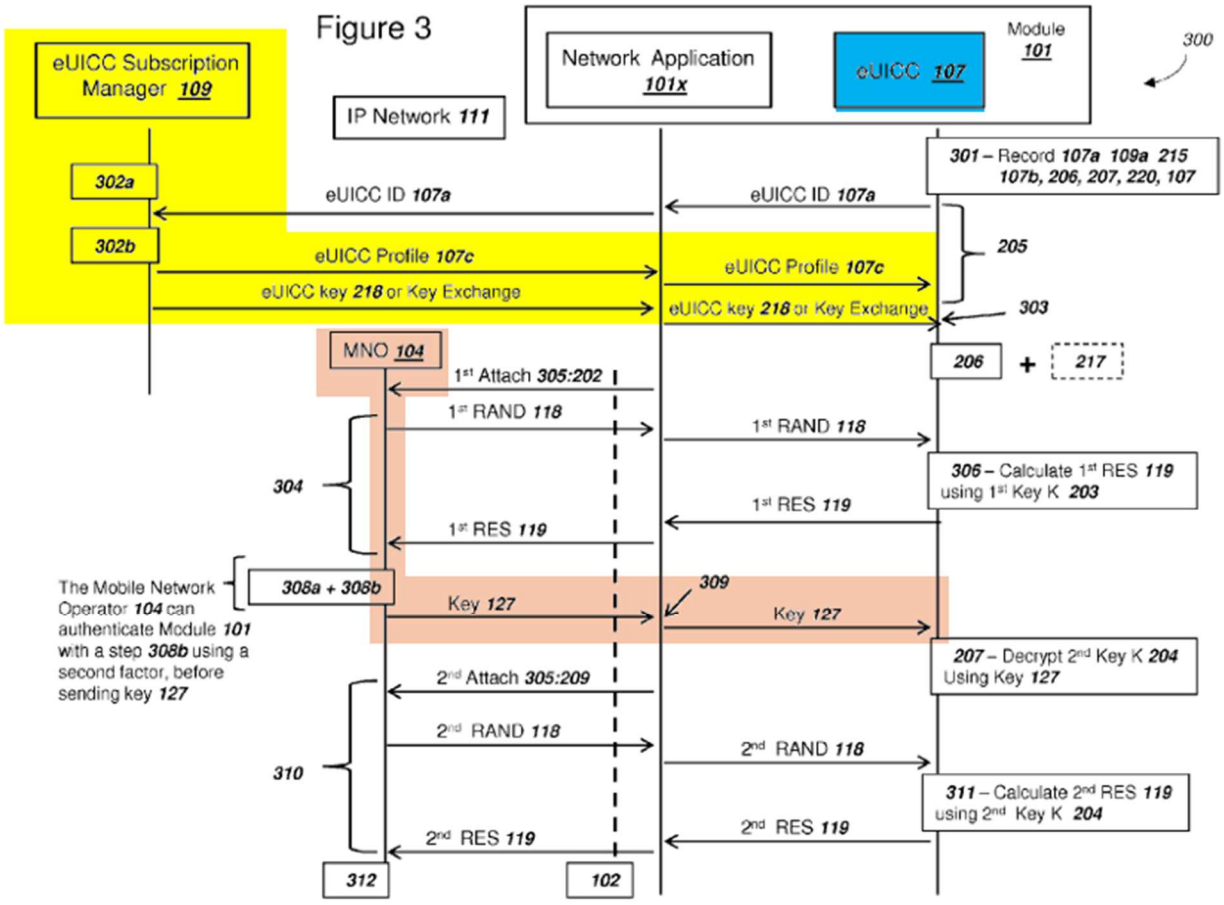
the annotated excerpt of Figure 2a, below. The portion of the profile encrypted with only the profile key and including the ***network parameters 201*** is shown in yellow. Ex-1002 ¶240.



Ex-1016, Fig. 2a. Ex-1002 ¶¶240-41.

(2) symmetric key

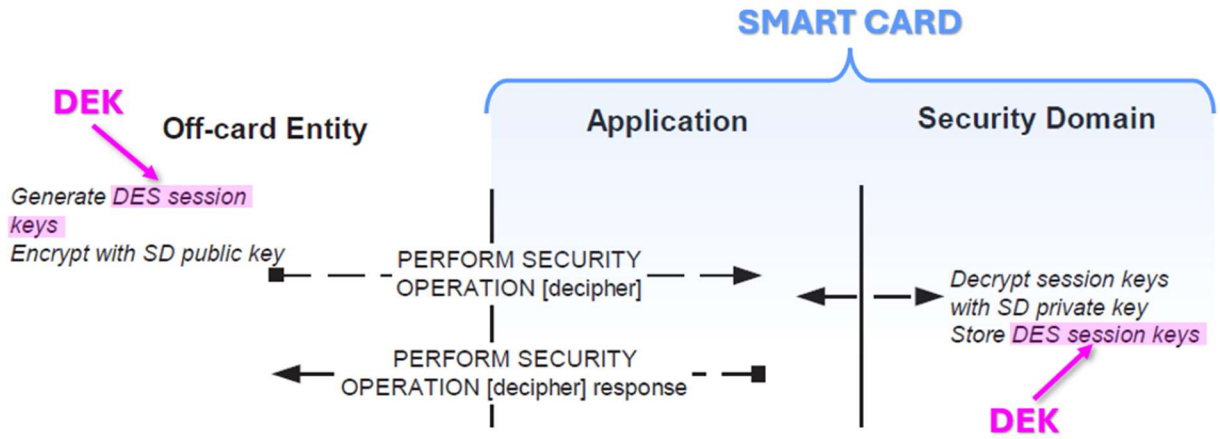
As discussed above, Nix175 teaches that the ***MNO*** sends the symmetric key 127 used to encrypt the key K in the profile, as shown below in red.



But it would have been obvious, in light of Park-GlobalPlatform, that the subscription manager could send the symmetric key 127 to the eUICC, provided that Park's split architecture of an SM-SR and SM-DP were used to address the security issue discussed above in Section XII.F.1.

Specifically Park-GlobalPlatform teaches a "key transport option" that may be used by an off-card entity to send DEK (equivalent to Nix175's "symmetric key") to a smart card. Ex-1006, 251-52. The DEK is sent to the card using the "PERFORM SECURITY OPERATION [decipher] command." Ex-1006, 255-56 (explaining that

the PERFORM SECURITY OPERATION [decipher] command includes "control reference templates" that "contain the actual key values," with "control reference template 'B8'" used to transmit the DEK). Ex-1006, 247, 275-76. This is illustrated in Figure F-9, excerpted below:

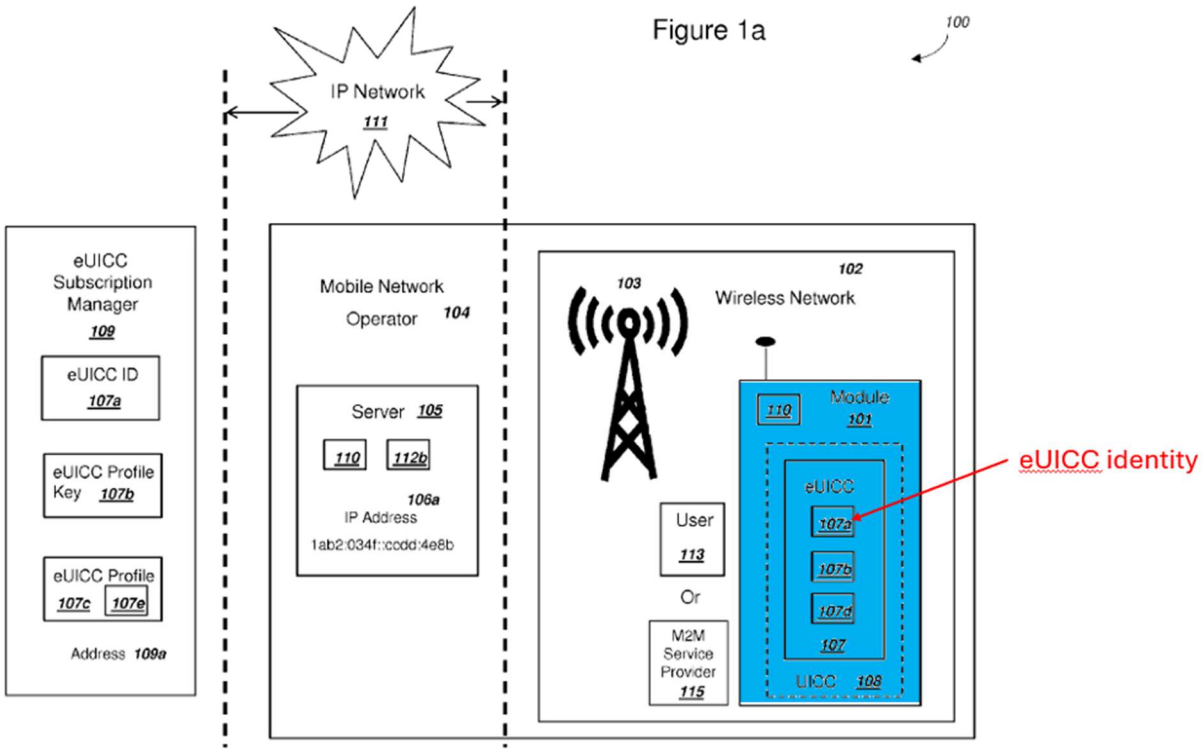


Ex-1006, Fig. F-9 (excerpted)

A POSITA would have recognized that in the combined Nix175-Park-GlobalPlatform system, Park's SM-DP would send the DEK (claimed "symmetric key") to the eUICC. Ex-1002 ¶¶40-41, 245. Further, the SM-DP is part of the network trust zone separate from the SM-SR. Ex-1002 ¶¶82-83. Thus, a POSITA would have recognized that in the Nix175-Park-GlobalPlatform system, the subscription manager (component SM-DP) would send the symmetric key to the eUICC without rendering void its security enhancements (as would be the case if the subscription manager of the unmodified Nix175 were to send it). Ex-1002 ¶¶243-45.

g. 1[d]: an eUICC associated with the eUICC identity and configured to

Nix175 teaches a module 101 having an eUICC 107, wherein the "eUICC 107 can include an eUICC identity 107a." Ex1016, 11:52-53; Fig. 1a. Ex-1002 ¶246.



h. 1[d][1]: a. derive a profile key using an elliptic curve Diffie-Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key;

Nix175 teaches "An eUICC 107 within a module 101 could use a ECDH key exchange in a step 303 when ECC algorithms are utilized for eUICC public key 214, ***eUICC private key*** 215, and eUICC subscription manager private key 222 and ***eUICC Subscription manager public key*** 220." Ex-1016, 51:65-52:2. Nix175 refers to a 2013 Wikipedia article for a description of the ECDH algorithm (*id*. 52:4-5),

and it was well known that an ECDH algorithm derives a shared key ("profile key") based on A's private key and B's public key. For example:

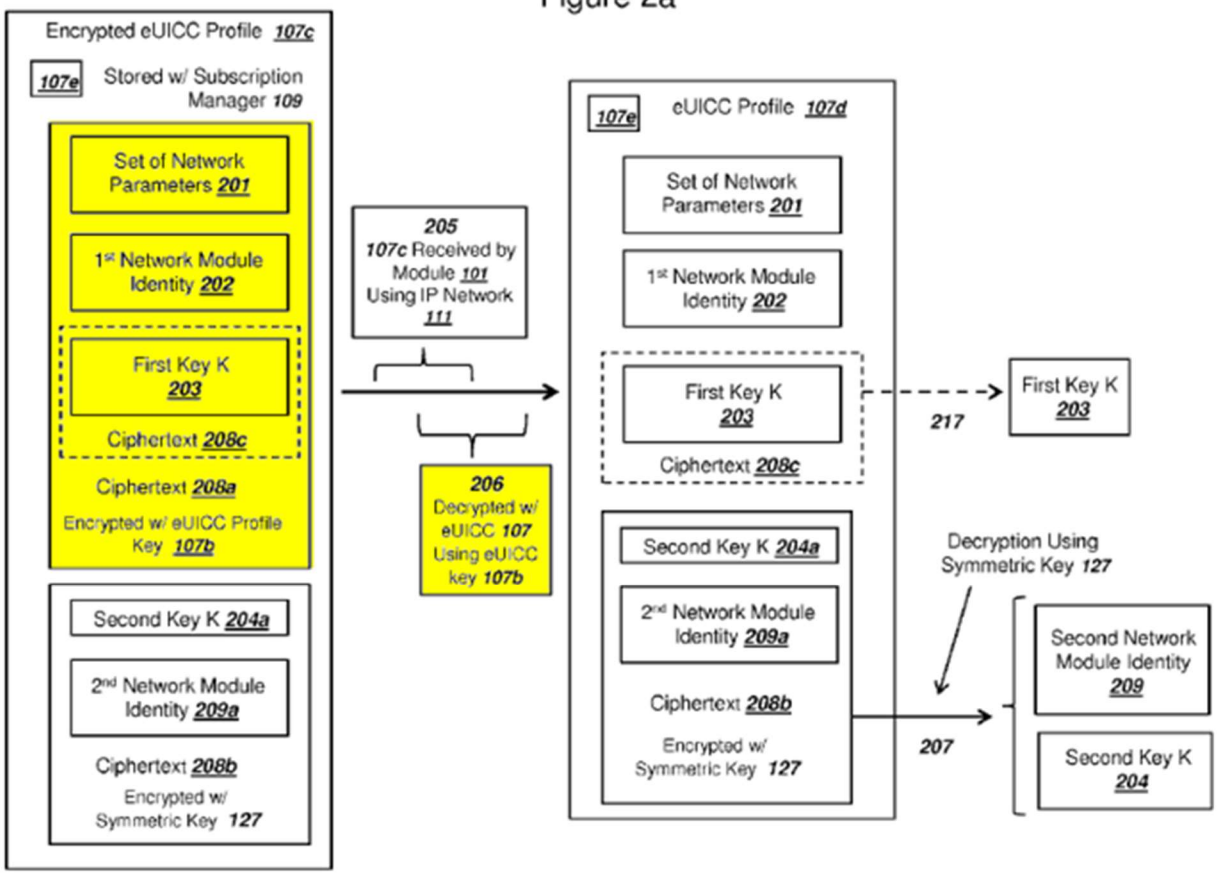
> Alice selects a random number n_a and computes $Y_a = n_aB$, she sends Y_a to Bob. Similarly Bob computes $Y_b = n_bB$ and sends Y_b to Alice. Alice and Bob generate the same key $K = n_aY_b = n_bY_a = n_an_bB$.

Ex-1007, 3. The derived key K in this example from Abi-Char corresponds to the claimed "profile key" calculated from A's (eUICC's) private key n_a (eUICC private key) and B's (subscription manager's) public key Y_b (subscription manager public key). Ex-1002 ¶45-48, 247.

i. 1[d][2]: b. decrypt a first portion of the eUICC profile using the profile key;

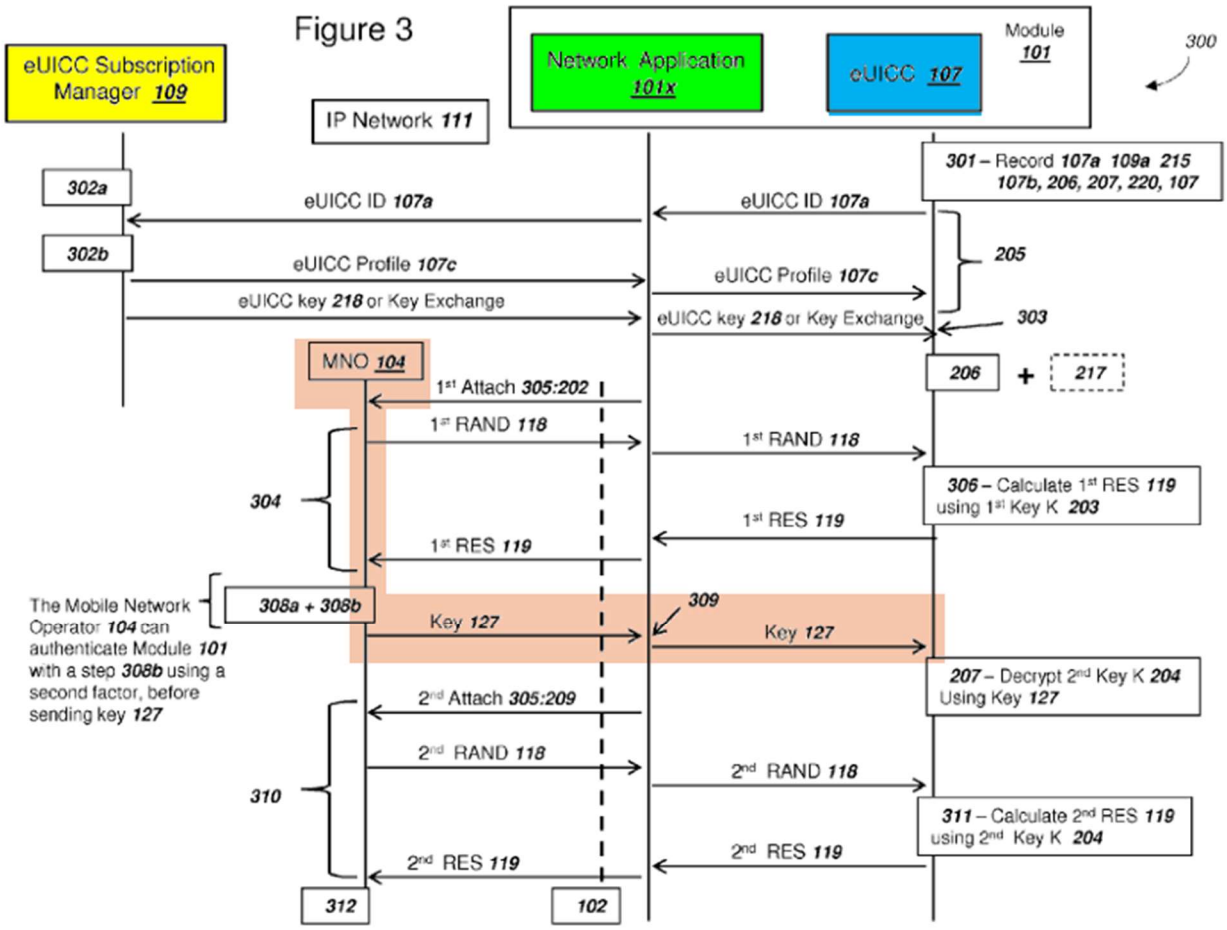
Nix175 teaches "receiving, by the hardware module, a profile from the eUICC subscription manager, wherein the hardware module uses the ***profile key to decrypt a first portion of the profile***." Ex-1016, Cl. 1. This is illustrated in the annotated Figure 2a, below, showing the portion of the profile encrypted by the profile key ("eUICC profile key 107b") in yellow and being decrypted with that key in step 206. Ex-1016, Fig. 2a; Ex-1002 ¶248.

Figure 2a



j. 1[d][3]: c. receive the symmetric key from a network application operating in the mobile device;

Although Nix175's symmetric key is sent by the MNO and not the subscription manager, it is nevertheless received by the module's network application which in turn sends it to the eUICC, as shown in Figure 3, below. MNO 104 (red) sends symmetric key 127 (red) to network application 101x (green), which forwards it on to eUICC 107 (blue). Ex-1016, Fig. 3; Ex-1002 ¶249.

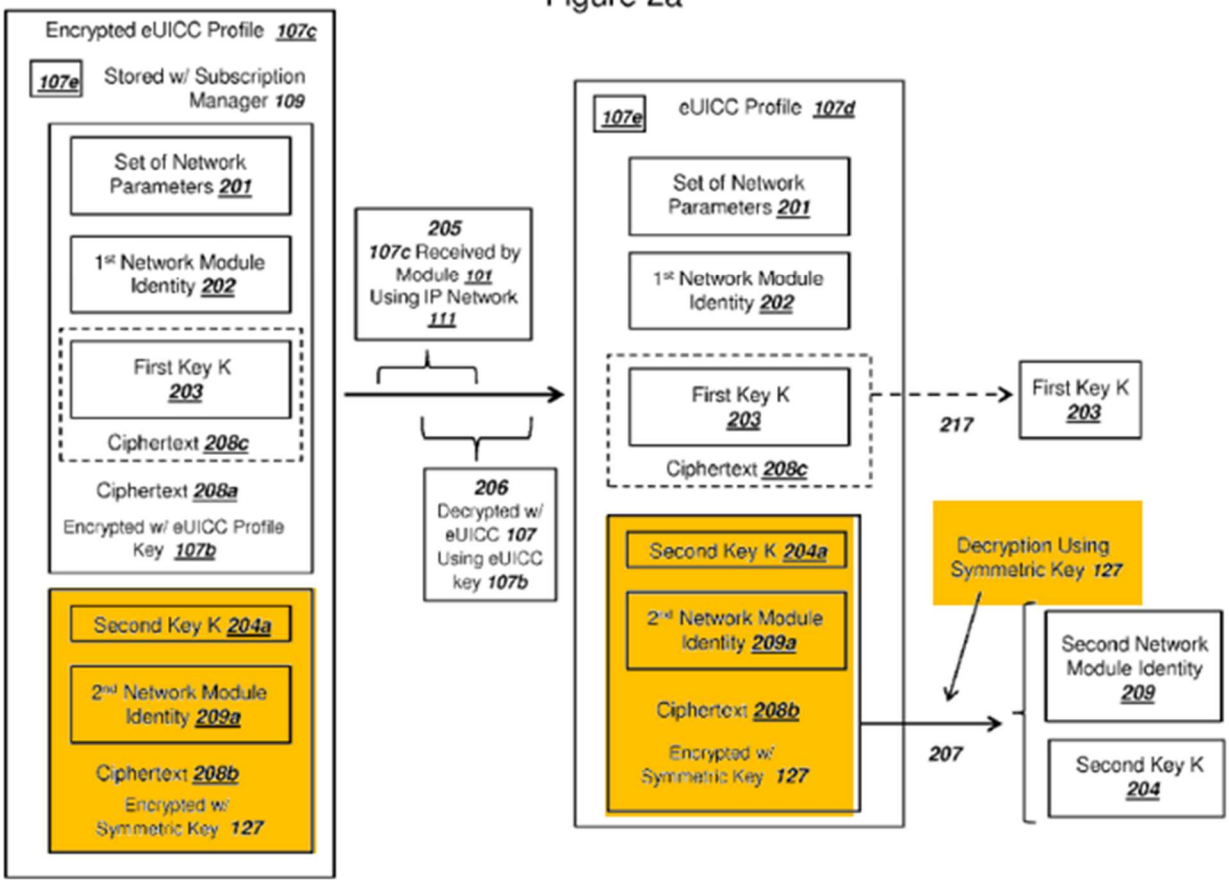


k. 1[d][4]: d. decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising the key K and the subscriber identity, wherein the first portion and the second portion are distinct; and

Nix175 teaches "wherein the hardware module ***uses the symmetric key*** to ***decrypt the second portion of the profile***, and wherein the second portion includes a second key K2." Ex-1016, Cl. 1. This is illustrated in Figure 2a below, where orange shading shows the second portion including key 204a and subscriber identity

209a encrypted by symmetric key 127 and then being decrypted by symmetric key 127 at step 207. Ex-1016, Fig. 2a; Ex-1002 ¶250.

Figure 2a

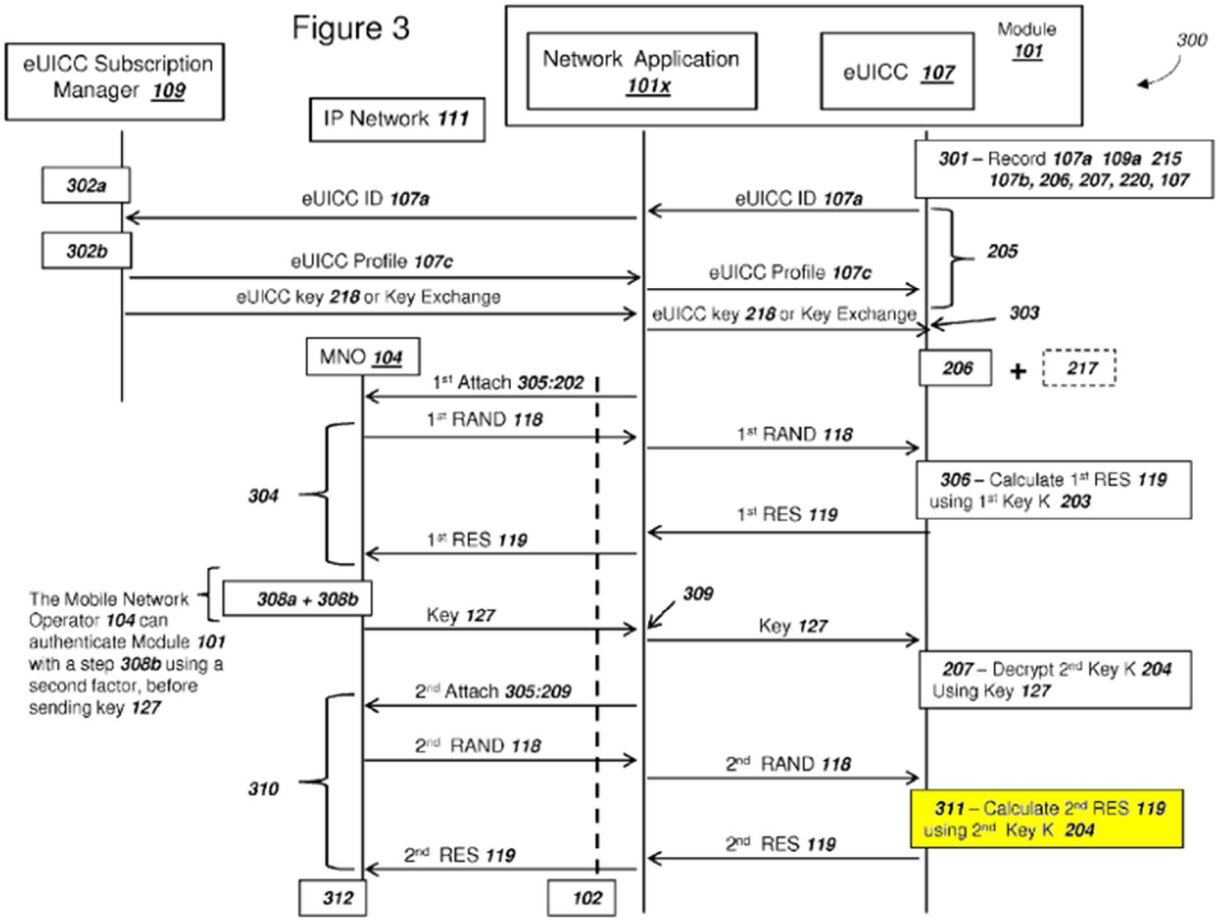


Nix175 teaches that ciphertext 208b may be separate from ciphertext 208a, or included within ciphertext 208a. Ex-1016, 33:60-63 ("ciphertext 208b could optionally be included within ciphertext 208a"). As explained in Section XII.F.1 (motivation to combine), it would have been a simple matter of design choice (computational complexity vs. cryptographic security) to encrypt the sensitive portion only with the symmetric key and the non-sensitive portion only with the profile key, since all of the profile would still be protected under at least one key and

the sensitive portion would remain accessible only to an entity possessing the symmetric key. Ex-1002 ¶251. In either case, ciphertext 208b (second portion of the profile) is distinct from ciphertext 208a (first portion of the profile). *Id*.

l. 1[d][5]: e. generate a response value for authentication of the mobile device with the wireless network using the key K.

Nix175 teaches "At a step 311, the eUICC 107 could calculate the second RES 119 using (i) the second RAND 118 received and (ii) the second key K 204. After receiving the exemplary second RAND 118 message, in order to conduct a second authentication 310, module 101 using an eUICC 107 could take steps to demonstrate to MNO 104 that module 101 has access to the same second key K 204 as recorded by the MNO 104 in an authentication vector 117." Ex-1016, 60:56-63; Fig. 3. Ex-1002 ¶252.



Thus, Nix175-Park-GlobalPlatform renders obvious Claim 1.

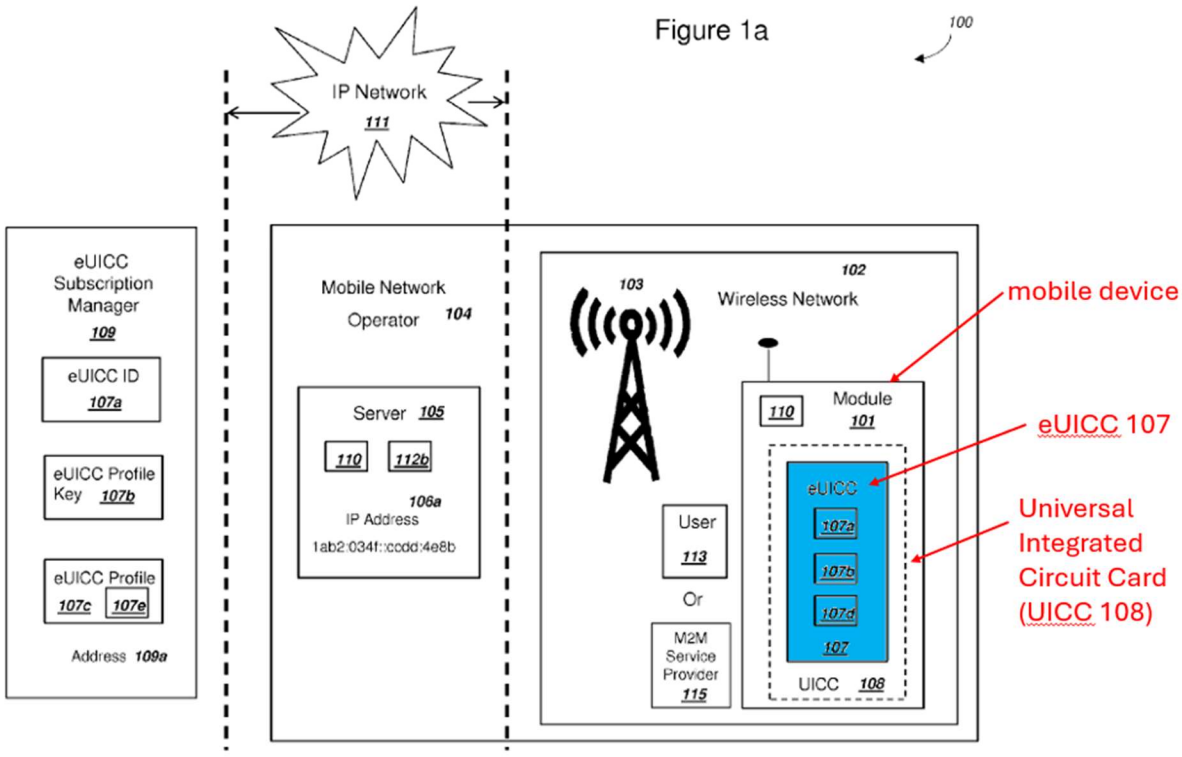
3. Dependent Claims 2-17

a. Claim 2: The mobile device of claim 1, wherein the eUICC is further configured to receive a profile identity for the eUICC profile as a plaintext.

Nix175 discloses that the subscription manage transmits the eUICC profile to the eUICC, as discussed above for element 1[c][2]. Nix175 further teaches "Some elements in a profile 107c could remain ***plaintext*** as well, such as the exemplary ***profile identity*** 107e." Ex-1016, 50:47-49; Ex-1002 ¶254.

b. Claim 3: The mobile device of claim 1, wherein the eUICC operates within a universal integrated circuit card within the mobile device.

Nix175 teaches an eUICC 107 operating within a UICC 108 within the mobile device 101. Ex-1016, Fig. 1a, below. Ex-1002 ¶255.



c. Claim 4: The mobile device of claim 1, wherein the random number generator is configured to generate the random number in response to input from at least one of a clock and a sensor.

Claim 5: The mobile device of claim 1, wherein the random number generator is configured to generate the random number from a seed value, wherein the seed value comprises data from at least one of a sensor, the radio, a bus, a clock, a physical interface, the memory, and an operating system.

Nix175 teaches Claims 4 and 5 as follows:

> As illustrated in FIG. 1 c, module 101 may also contain ***a random number generator 128***. … A plurality of the data as a source for a random number seed 128b could be appended together into a "module random seed file' with a combined series or list of states (i.e. a plurality of ***sensor*** 101 *f* measurements, ***radio*** 101z measurements, ***clock*** 160 times or values, memory 101e or memory 101w states, ***operating system 101h states***, actuator 101y states, and/or hardware 101a or 101d states).

Ex-1016, 22:32-43; Ex-1002 ¶256.

d. Claim 6: The mobile device of claim 1, wherein the network application is configured to communicate with i) the wireless network and ii) the eUICC in the mobile device using a system bus.

Nix175 teaches "The ***network application*** 101x and the eUICC 107 can send and receive data locally within the module 101 using an operating system 101h and/or a ***system bus*** 101d. … The module 101, using a ***network application*** 101x, can send and receive data with the eUICC subscription manager 109 using the ***IP network 111***." Ex-1016, 46:27-35. Ex-1002 ¶257.

e. Claim 7: The mobile device of claim 1, wherein the eUICC comprises computer executable instructions for a processor in the mobile device, and wherein the computer executable instructions are stored within the memory.

Nix175 teaches "Many of the logical steps for operation of module 101 or eUICC 107 can be performed in software and hardware," (Ex-1016, 14:65-66), wherein the eUICC includes "RAM memory, ROM memory, [and] EEPROM memory." *Id*. 11:62-12:1. A POSITA would understand one or more of these memories to store the "computer executable instructions," i.e., software, for performing the operations of eUICC 107. Ex-1002 ¶258.

f. Claim 8: The mobile device of claim 1, wherein the eUICC comprises a package soldered onto a circuit board of the mobile device.

Nix175 teaches "An eUICC 107 as illustrated in FIG. 1a and FIG. 1b can be implemented within module 101 in several different ways, including… (iv) a specialized circuit within a surface mount package that is soldered directly onto a circuitboard of the module 101." Ex-1016, 18:20-32; Ex-1002 ¶259.

g. Claim 9: The mobile device of claim 1, further comprising a user interface configured to receive user identification information before the mobile device receives the symmetric key.

Nix175 teaches "the module 101 receives the symmetric key 127 after the MNO 104 authenticates or verifies that a user 113 or M2M service provider 115 is associated with module 101, and until the receipt of the symmetric key 127 the cipher

text 208b cannot be feasibly decrypted." Ex-1016, 58:45-49. Further "wherein a user accesses a user interface of the hardware module to authenticate with the mobile network operator before the hardware module receives the symmetric key." *Id*. Cl. 2. Ex-1002 ¶260.

In the combined system, in which the subscription manager is split into Park's SM-SR (not necessarily trusted by the MNO) and SM-DP (trusted), the SM-DP would be tasked with authenticating the user, before sending either the symmetric key or the encrypted profile to the user. Ex-1002 ¶261.

h. Claim 10: The mobile device of claim 1, wherein the first portion of the eUICC profile includes the network parameters, the network parameters comprising a list of numbers associated with a mobile network operator.

Claim 11: The mobile device of claim 1, wherein the network parameters comprise a mobile country code (MCC) and a mobile network code (MNC) associated with the wireless network.

Nix175 teaches "The profile 107d could include values in the set of network parameters 201 that match or conform with values transmitted by the wireless network 102, such as using the same mobile country code (MCC) and mobile network code (MNC) as recorded in the profile 107d." Ex-1016, 64:1-5. Ex-1002 ¶262.

i. Claim 12: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, the eUICC profile using transport layer security.

Nix teaches "As transferred across a wireless network 102 and/or IP network 111, the encrypted eUICC profile 107c can be segmented into separate datagrams and transferred using a transport layer protocol Such as TCP." Ex-1016, 29:16-19. Ex-1002 ¶263.

j. Claim 13: The mobile device of claim 1, wherein the subscriber identity comprises an International Mobile Subscriber Identity (IMSI).

Nix175 teaches "In an exemplary embodiment, the first network module identity 202 can comprise an international mobile subscriber identity (IMSI)." Ex-1016, 30:11-13. Ex-1002 ¶264.

a. Claim 14: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, a ciphertext for the symmetric key, wherein the mobile device is configured to decrypt the ciphertext using at least the eUICC private key.

Nix175 teaches "In an exemplary embodiment of a step 309 in FIG. 3, the symmetric key 127 can first be encrypted with a key ciphering algorithm 216. An encrypted symmetric key 127 ciphered with the key ciphering algorithm 216 could be ***received by module 101*** in a step 309. … The module 101 could receive the encrypted symmetric key 127 and decrypt the symmetric key 127 in a step 309 by using a key deciphering algorithm 217 ***with the eUICC private key*** 215" Ex-1016,

58:23-35. However, Nix175 does not teach that it is the "subscription manager" that delivers the symmetric key as ciphertext. But for the same reasons discussed for claim element 1[c][2] above, it would have been obvious in light of Park and GlobalPlatform to receive the ciphertext from Park's SM-DP. Ex-1002 ¶265.

b. Claim 15: The mobile device of claim 1, wherein the mobile device further comprises at least one of a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a tracking device, and a circuit board with the radio.

Nix175 teaches "module 101 can be a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a computer with a radio, a tracking device, or a circuit board with a radio that accesses wireless network 102." Ex-1016, 10:25-29. Ex-1002 ¶266.

c. Claim 16: The mobile device of claim 1, wherein the second memory is the same memory as the first memory.

Nix175 discloses that that random key data may be stored in either nonvolatile memory (the first memory) or in volatile memory (the second memory), so whether the first and second memory are the same memory is a simple matter of design choice. For example, "The module 101 or eUICC 107 can record the plaintext second key K 204 in a ***nonvolatile memory*** such as, but not limited to, flash memory ***101w***" (*id*. 59:1-3) but "[i]n another embodiment, (A) the plaintext second key K204

is recorded only in a ***volatile memory*** within CPU 101b" *Id*., 59:29-30. Ex-1002 ¶267.

d. Claim 17: The mobile device of claim 1, wherein the one or more receiving antennas are the one or more transmit antennas.

Nix175 teaches that the antennas can be used for both receive and transmit: "Although not illustrated, radio 101z could include antennas for reception and transmission of RF signals, and even multiple antennas could be used." Ex-1016, 20:47-49; Ex-1002 ¶268.

XIII. CONCLUSION

Petitioner requests institution of IPR for Claims 1-17 of the '893 Patent based on each of the grounds in this Petition.

Respectfully Submitted,

/s/ *William M. Fink*
William M. Fink (Reg. No. 72,332)

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Petitioner certifies that this petition includes 13,500 words, as measured by Microsoft Word, exclusive of the table of contents, mandatory notices under §42.8, certificates of service, word count, and exhibits.

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

The undersigned hereby certifies that the above document was served on December 1, 2025, by filing this document through the Patent Trial and Appeal Board P-TACTS System, as well as delivering a copy via express mail upon the following attorneys of record for the Patent Owner:

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

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

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

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

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

Dated: December 1, 2025

Respectfully submitted,

/s/ William M. Fink

William M. Fink (Reg. No. 72,332)
O'Melveny & Myers LLP
1625 Eye Street, NW
Washington, DC 20006
Telephone: (202) 383-5300
Fax: (202) 383-5414
Email: tfink@omm.com
Attorney for Petitioner