United States of America

To Promote the Progress of Science and Useful Arts

The Director

of the United States Patent and Trademark Office has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this United States

Patent

grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America, and if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States of America, products made by that process, for the term set forth in 35 U.S.C. 154(a)(2) or (c)(1), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b). See the Maintenance Fee Notice on the inside of the cover.

Acting Director of the United States Patent and Trademark Office

Petitioner Samsung Ex-1004, 0001

Maintenance Fee Notice

If the application for this patent was filed on or after December 12, 1980, maintenance fees are due three years and six months, seven years and six months, and eleven years and six months after the date of this grant, or within a grace period of six months thereafter upon payment of a surcharge as provided by law. The amount, number and timing of the maintenance fees required may be changed by law or regulation. Unless payment of the applicable maintenance fee is received in the United States Patent and Trademark Office on or before the date the fee is due or within a grace period of six months thereafter, the patent will expire as of the end of such grace period.

Patent Term Notice

If the application for this patent was filed on or after June 8, 1995, the term of this patent begins on the date on which this patent issues and ends twenty years from the filing date of the application or, if the application contains a specific reference to an earlier filed application or applications under 35 U.S.C. 120, 121, 365(c), or 386(c), twenty years from the filing date of the earliest such application ("the twenty-year term"), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b), and any extension as provided by 35 U.S.C. 154(b) or 156 or any disclaimer under 35 U.S.C. 253.

If this application was filed prior to June 8, 1995, the term of this patent begins on the date on which this patent issues and ends on the later of seventeen years from the date of the grant of this patent or the twenty-year term set forth above for patents resulting from applications filed on or after June 8, 1995, subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b) and any extension as provided by 35 U.S.C. 156 or any disclaimer under 35 U.S.C. 253.

Form PTO-377C (Rev 09/17)

US012207094B2

(12) **United States Patent**
Nix

(10) **Patent No.: US 12,207,094 B2**
(45) **Date of Patent: *Jan. 21, 2025**

(54) **EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION**

(71) Applicant: **Network-1 Technologies, Inc.**, New York, NY (US)

(72) Inventor: **John A. Nix**, Evanston, IL (US)

(73) Assignee: **Network-1 Technologies, Inc.**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **18/416,534**

(22) Filed: **Jan. 18, 2024**

(65) **Prior Publication Data**

US 2024/0250938 A1 Jul. 25, 2024

Related U.S. Application Data

(63) Continuation of application No. 17/547,990, filed on Dec. 10, 2021, now Pat. No. 11,916,893, which is a (Continued)

(51) **Int. Cl.**
H04W 12/30 (2021.01)
H04B 1/3816 (2015.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04W 12/35*** (2021.01); ***H04B 1/3816*** (2013.01); ***H04L 9/0819*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC H04W 12/35; H04W 12/06; H04W 12/30; H04L 63/0853; H04L 63/08
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,216,715 A 6/1993 Markwitz
5,642,420 A 6/1997 Kuroda et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CA 2775853 A1 12/2012
CA 3110641 A1 10/2019
(Continued)

OTHER PUBLICATIONS

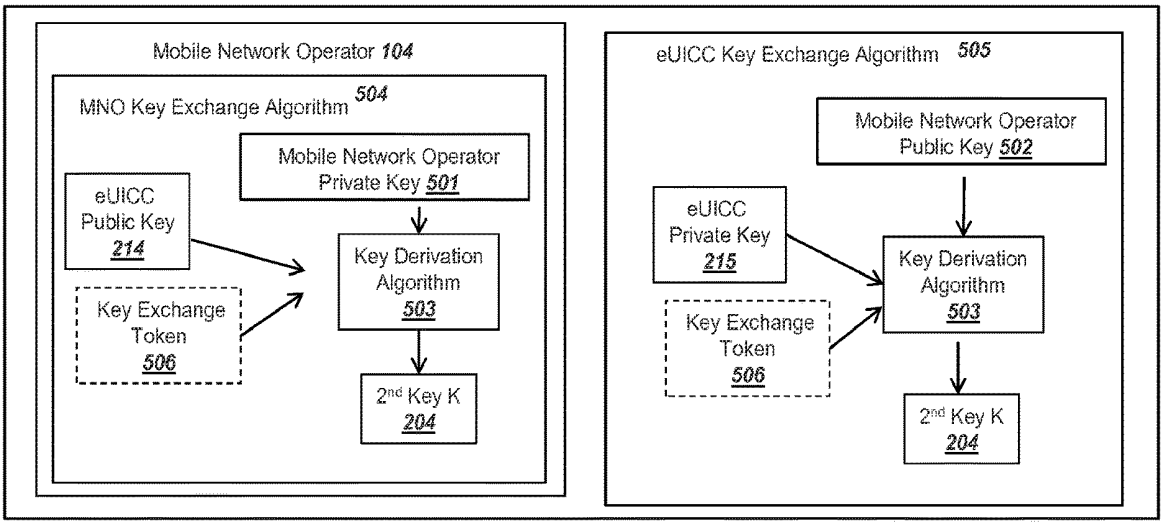
U.S. Appl. No. 18/435,042, filed Feb. 7, 2024, Pending—Ready for Examination.
(Continued)

Primary Examiner — Dao Q Ho
(74) *Attorney, Agent, or Firm* — Amster, Rothstein & Ebenstein LLP

(57) **ABSTRACT**

A module with an embedded universal integrated circuit card (eUICC) can include a profile for the eUICC. The profile can include a first and second shared secret key K for authenticating with a wireless network. The first shared secret key K can be encrypted with a first key, and the second shared secret key K can be encrypted with a second key. The module can (i) receive the first key, (ii) decrypt the first shared secret key K with the first key, and (iii) subsequently authenticate with the wireless network using the plaintext first shared secret key K. The wireless network can authenticate the user of the module using a second factor. The module can then (i) receive the second key, (ii) decrypt the second shared secret key K, and (iii) authenticate with the wireless network using the second shared secret key K. The module can comprise a mobile phone.

22 Claims, 12 Drawing Sheets



Petitioner Samsung Ex-1004, 0003

Related U.S. Application Data

continuation of application No. 16/453,682, filed on Jun. 26, 2019, now Pat. No. 11,233,780, which is a continuation-in-part of application No. 16/110,804, filed on Aug. 23, 2018, now Pat. No. 10,382,422, which is a continuation of application No. 15/928,848, filed on Mar. 22, 2018, now Pat. No. 10,084,768, which is a continuation of application No. 14/751,119, filed on Jun. 25, 2015, now Pat. No. 9,961,060, which is a continuation of application No. 14/099,329, filed on Dec. 6, 2013, now Pat. No. 9,100,175.

(51) **Int. Cl.**

H04L 9/08	(2006.01)
H04L 9/32	(2006.01)
H04L 9/40	(2022.01)
H04W 4/70	(2018.01)
H04W 12/06	(2021.01)

(52) **U.S. Cl.**

CPC ***H04L 9/0869*** (2013.01); ***H04L 9/3271*** (2013.01); ***H04L 63/0428*** (2013.01); ***H04L 63/0435*** (2013.01); ***H04L 63/06*** (2013.01); ***H04L 63/062*** (2013.01); ***H04L 63/08*** (2013.01); ***H04L 63/101*** (2013.01); ***H04W 4/70*** (2018.02); ***H04W 12/06*** (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,664,017	A	9/1997	Gressel et al.
5,852,665	A	12/1998	Gressel et al.
5,995,625	A	11/1999	Sudia et al.
6,038,322	A	3/2000	Harkins
6,256,733	B1	7/2001	Thakkar et al.
6,721,886	B1	4/2004	Uskela
6,804,357	B1	10/2004	Ikonen et al.
6,842,628	B1	1/2005	Arnold et al.
7,921,292	B1	4/2011	Pauker et al.
7,957,532	B2	6/2011	Chen et al.
8,127,142	B2	2/2012	Cuppett
8,352,739	B2	1/2013	Park et al.
8,434,139	B1	4/2013	Ortiz, Jr.
8,452,017	B2	5/2013	Sherkin
8,522,013	B2	8/2013	Zhang et al.
8,526,606	B2	9/2013	Muthaiah
8,555,067	B2	10/2013	Schell et al.
8,577,337	B2	11/2013	O'Leary
8,590,028	B2	11/2013	Saxena et al.
8,782,774	B1	7/2014	Pahl et al.
8,843,179	B2	9/2014	Li et al.
8,924,715	B2	12/2014	Schell et al.
8,948,386	B2	2/2015	Campagna et al.
8,965,366	B1	2/2015	Somayajula et al.
9,002,018	B2	4/2015	Wilkins et al.
9,020,479	B1	4/2015	Somayajula et al.
9,253,643	B2	2/2016	Pattar et al.
9,270,653	B2	2/2016	Maria
9,332,129	B2	5/2016	Li et al.
9,408,012	B2	8/2016	Li et al.
9,572,016	B2	2/2017	Cormier et al.
9,596,078	B2	3/2017	Nix
9,628,981	B2	4/2017	Park et al.
9,674,690	B2	6/2017	Lee et al.
9,698,981	B2	7/2017	Nix
9,794,775	B2	10/2017	Huber et al.
9,800,993	B2	10/2017	Lee et al.
9,807,605	B2	10/2017	Gao et al.
9,923,724	B2	3/2018	Lee et al.
10,169,587	B1	1/2019	Nix
10,621,352	B2	4/2020	NIx
2001/0029581	A1	10/2001	Knauft
2002/0018569	A1	2/2002	Panjwani et al.
2003/0003895	A1	1/2003	Wallentin et al.
2003/0211842	A1	11/2003	Kempf et al.
2004/0162472	A1	8/2004	Berson et al.
2004/0179684	A1	9/2004	Appenzeller et al.
2004/0221163	A1	11/2004	Jorgensen et al.
2005/0008159	A1	1/2005	Grilli et al.
2005/0021875	A1	1/2005	Bouthemy et al.
2005/0050323	A1	3/2005	Mizrah
2005/0058294	A1	3/2005	Chen et al.
2005/0120202	A1	6/2005	Cuellar et al.
2005/0138353	A1	6/2005	Spies et al.
2005/0193199	A1	9/2005	Asokan et al.
2005/0246282	A1	11/2005	Naslund et al.
2005/0278787	A1	12/2005	Naslund et al.
2006/0021063	A1	1/2006	Hori
2006/0056355	A1	3/2006	Love et al.
2006/0059344	A1	3/2006	Mononen
2006/0095771	A1	5/2006	Appenzeller et al.
2006/0129848	A1	6/2006	Paksoy et al.
2006/0206710	A1	9/2006	Gehrmann
2006/0281442	A1	12/2006	Lee et al.
2007/0101400	A1	5/2007	Freeman et al.
2007/0158439	A1	7/2007	Conner et al.
2007/0206799	A1	9/2007	Wingert et al.
2008/0016230	A1	1/2008	Hollmanns et al.
2008/0022089	A1	1/2008	Leedom
2008/0031204	A1	2/2008	Sood
2008/0044032	A1	2/2008	Lou et al.
2008/0107083	A1	5/2008	Shirota et al.
2008/0114978	A1	5/2008	Lehtoviorta et al.
2008/0130879	A1	6/2008	Heinonen et al.
2008/0165698	A1	7/2008	Dalsgard et al.
2008/0307218	A1	12/2008	Logvinov
2009/0028341	A1	1/2009	Hamachi
2009/0041110	A1	2/2009	Malladi
2009/0060197	A1	3/2009	Taylor et al.
2009/0077643	A1	3/2009	Schmidt et al.
2009/0113203	A1	4/2009	Tsuge et al.
2009/0116642	A1	5/2009	Yang et al.
2009/0125996	A1	5/2009	Guccione et al.
2009/0132806	A1	5/2009	Blommaert et al.
2009/0183541	A1	7/2009	Sadighi et al.
2009/0191857	A1	7/2009	Horn et al.
2009/0209232	A1	8/2009	Cha et al.
2009/0217348	A1	8/2009	Salmela et al.
2009/0268909	A1	10/2009	Girao et al.
2009/0274306	A1	11/2009	Nolte
2009/0282246	A1	11/2009	Gunther
2009/0313472	A1	12/2009	Guccione et al.
2010/0031042	A1	2/2010	Di Crescenzo et al.
2010/0062808	A1	3/2010	Cha et al.
2010/0093347	A1	4/2010	Hahn et al.
2010/0098253	A1	4/2010	Delerablee
2010/0166167	A1	7/2010	Karimi-Cherkandi et al.
2010/0195833	A1	8/2010	Priestley et al.
2010/0199334	A1	8/2010	Ehrensvard et al.
2010/0223461	A1	9/2010	Drader et al.
2010/0275028	A1	10/2010	Takashima
2011/0016321	A1	1/2011	Sundaram et al.
2011/0035584	A1	2/2011	Meyerstein et al.
2011/0035604	A1	2/2011	Habraken
2011/0055553	A1	3/2011	Lee et al.
2011/0158411	A1	6/2011	Medvinsky et al.
2011/0167272	A1	7/2011	Kolesnikov
2011/0213959	A1	9/2011	Bodi et al.
2011/0237281	A1	9/2011	Busropan et al.
2011/0268022	A1	11/2011	Xu
2011/0269422	A1	11/2011	Xu et al.
2011/0269461	A1	11/2011	Xu et al.
2011/0269472	A1	11/2011	Xu et al.
2011/0270747	A1	11/2011	Xu
2011/0291803	A1	12/2011	Bajic et al.
2011/0314287	A1	12/2011	Escott et al.
2012/0011360	A1	1/2012	Engels et al.
2012/0011362	A1	1/2012	Lambert
2012/0023336	A1	1/2012	Natarajan
2012/0030461	A1	2/2012	Willey et al.
2012/0033613	A1	2/2012	Lin et al.
2012/0072732	A1	3/2012	Canard et al.

Petitioner Samsung Ex-1004, 0004

(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0084568 A1 4/2012 Sarikaya et al.
2012/0087493 A1 4/2012 Chidambaram et al.
2012/0089568 A1 4/2012 Manley et al.
2012/0108205 A1 5/2012 Schell et al.
2012/0117635 A1 5/2012 Schell et al.
2012/0159153 A1 6/2012 Shim et al.
2012/0170451 A1 7/2012 Viswanathan et al.
2012/0190354 A1 7/2012 Merrien et al.
2012/0214444 A1 8/2012 McBride et al.
2012/0260086 A1 10/2012 Haggerty et al.
2012/0260090 A1 10/2012 Hauck et al.
2012/0260095 A1 10/2012 Von Hauck et al.
2012/0263298 A1 10/2012 Suh et al.
2012/0278490 A1 11/2012 Sennett et al.
2012/0300932 A1 11/2012 Cambridge et al.
2012/0331292 A1 12/2012 Haggerty et al.
2012/0331298 A1 12/2012 Xu et al.
2013/0007442 A1 1/2013 Mao et al.
2013/0012168 A1 1/2013 Rajadurai et al.
2013/0028184 A1 1/2013 Lee et al.
2013/0091556 A1 4/2013 Horn et al.
2013/0114810 A1 5/2013 Kobayashi et al.
2013/0117824 A1 5/2013 Naslund et al.
2013/0122864 A1 5/2013 Haggerty et al.
2013/0149996 A1 6/2013 King et al.
2013/0157673 A1 6/2013 Brusilovsky
2013/0165073 A1 6/2013 Madsen
2013/0165075 A1 6/2013 Rishy-Maharaj et al.
2013/0166915 A1 6/2013 Desai et al.
2013/0173747 A1 7/2013 Kim et al.
2013/0173926 A1 7/2013 Morese et al.
2013/0179962 A1 7/2013 Arial et al.
2013/0182586 A1 7/2013 Paladugu et al.
2013/0183932 A1 7/2013 Lemilainen et al.
2013/0212637 A1 8/2013 Guccione et al.
2013/0227646 A1 8/2013 Haggerty et al.
2013/0231087 A1 9/2013 O'Leary
2013/0283047 A1 10/2013 Merrien et al.
2013/0294602 A1 11/2013 Huxham et al.
2013/0305345 A1 11/2013 Bugenhagen
2013/0322621 A1 12/2013 Yoon et al.
2013/0331063 A1 12/2013 Cormier et al.
2013/0340040 A1 12/2013 Park et al.
2013/0344864 A1 12/2013 Park et al.
2014/0003604 A1 1/2014 Campagna et al.
2014/0040628 A1 2/2014 Fort et al.
2014/0049653 A1 2/2014 Leonard et al.
2014/0053241 A1 2/2014 Norman et al.
2014/0073375 A1 3/2014 Li et al.
2014/0082358 A1 3/2014 Nakhjiri et al.
2014/0082359 A1 3/2014 Nakhjiri et al.
2014/0082538 A1 3/2014 Nakhjiri et al.
2014/0082539 A1 3/2014 Nakhjiri et al.
2014/0087790 A1 3/2014 Babbage et al.
2014/0101444 A1 4/2014 Lee et al.
2014/0108801 A1 4/2014 McBride et al.
2014/0115335 A1 4/2014 Jorden et al.
2014/0120874 A1 5/2014 Kang et al.
2014/0122878 A1 5/2014 Cho et al.
2014/0140507 A1 5/2014 Park et al.
2014/0140509 A1 5/2014 Chastain et al.
2014/0143534 A1 5/2014 Chastain et al.
2014/0143826 A1 5/2014 Sharp et al.
2014/0161113 A1 6/2014 Cui et al.
2014/0165155 A1 6/2014 Zhang
2014/0192976 A1 7/2014 Yoon et al.
2014/0219447 A1 8/2014 Park et al.
2014/0219448 A1 8/2014 Froels et al.
2014/0235210 A1 8/2014 Park et al.
2014/0237101 A1 8/2014 Park
2014/0244994 A1 8/2014 Yu
2014/0273913 A1 9/2014 Michel et al.
2014/0281483 A1 9/2014 Vigliaturo et al.
2014/0287725 A1 9/2014 Lee
2014/0308991 A1 10/2014 Lee et al.
2014/0329502 A1 10/2014 Lee et al.
2014/0337937 A1 11/2014 Truskovsky et al.
2014/0351403 A1 11/2014 Lin et al.
2014/0357229 A1 12/2014 Lee et al.
2015/0012743 A1 1/2015 Holtmanns et al.
2015/0017910 A1 1/2015 Li et al.
2015/0071139 A1 3/2015 Nix
2015/0089214 A1 3/2015 Dupre
2015/0092590 A1 4/2015 Zhu et al.
2015/0095514 A1 4/2015 Yu
2015/0095648 A1 4/2015 Nix
2015/0106616 A1 4/2015 Nix
2015/0113275 A1 4/2015 Kim et al.
2015/0121066 A1 4/2015 Nix
2015/0121495 A1 4/2015 Gao et al.
2015/0143125 A1 5/2015 Nix
2015/0163056 A1 6/2015 Nix
2015/0215126 A1 7/2015 Ashdown
2015/0222604 A1 8/2015 Ylonen
2015/0222619 A1 8/2015 Hughes et al.
2015/0281964 A1 10/2015 Seo et al.
2015/0350881 A1 12/2015 Weiss et al.
2016/0014112 A1 1/2016 Gunning et al.
2016/0057725 A1 2/2016 Suh
2016/0088096 A1 3/2016 Quiriconi et al.
2016/0127132 A1 5/2016 Lee et al.
2016/0149903 A1 5/2016 Suh
2016/0294829 A1 10/2016 Angus
2017/0206532 A1 7/2017 Choi
2019/0313246 A1 10/2019 Nix
2019/0332774 A1 10/2019 Nix
2019/0356482 A1 11/2019 Nix
2020/0162247 A1 5/2020 Nix
2020/0162269 A1 5/2020 Nix
2020/0226258 A1 7/2020 Nix
2020/0280436 A1 9/2020 Nix
2021/0126801 A1 4/2021 Nix
2021/0184842 A1 6/2021 Nix
2021/0194681 A1 6/2021 Nix
2021/0211279 A1 7/2021 Nix
2021/0218560 A1 7/2021 Nix

FOREIGN PATENT DOCUMENTS

CA 3110468 A1 11/2019
DE 19803936 A1 8/1999
EP 1981 224 10/2008
EP 3766222 A1 1/2021
GB 2518976 A 4/2015
KR 10-2013-0026352 A 3/2013
KR 10-2013-0026958 A 3/2013
KR 20130026351 A 3/2013
WO 2011138238 A1 11/2011
WO 2013027085 A1 2/2013
WO 2013/048084 A2 4/2013
WO 2013066077 A1 5/2013
WO 2019178312 A1 9/2019
WO 2019209598 A1 10/2019
WO 2019222319 A1 11/2019
WO 2019246206 A1 12/2019
WO 2020006162 A1 1/2020
WO 2020061023 A1 3/2020
WO 2020123959 A1 6/2020
WO 2020223319 A1 11/2020
WO 2021007235 A1 1/2021
WO 2021087221 A1 5/2021

OTHER PUBLICATIONS

U.S. Appl. No. 18/587,462, filed Feb. 26, 2024, Pending—Ready for Examination.
U.S. Appl. No. 18/433,683, filed Feb. 6, 2024, Pending—Ready for Examination.
U.S. Appl. No. 18/438,147, filed Feb. 9, 2024, Pending—Undergoing Preexam Processing.
U.S. Appl. No. 18/416,534, filed 204-01-18, Present Application.
U.S. Appl. No. 18/433,664, filed Feb. 6, 2024, Pending—Ready for Examination.

Petitioner Samsung Ex-1004, 0005

(56) **References Cited**

OTHER PUBLICATIONS

U.S. Appl. No. 18/229,907, filed Aug. 3, 2023, Pending—Response to Final OA filed Mar. 28, 2024.
U.S. Appl. No. 18/111,669, filed Feb. 20, 2023, Non-Final OA mailed Oct. 2, 2023.
U.S. Appl. No. 17/647,812, filed Jan. 13, 2022, U.S. Pat. No. 11,606,204.
U.S. Appl. No. 17/547,990, filed Dec. 10, 2021, U.S. Pat. No. 11,736,283.
U.S. Appl. No. 17/304,922, filed Jun. 28, 2021, U.S. Pat. No. 11,736,283.
U.S. Appl. No. 17/249,242, filed Feb. 24, 2021, Response to Non-Final OA filed Nov. 13, 2023.
U.S. Appl. No. 16/879,325, filed May 20, 2020, U.S. Pat. No. 11,082,218.
U.S. Appl. No. 16/843,107, filed Apr. 8, 2020, U.S. Pat. No. 11,283,603.
U.S. Appl. No. 16/721,153, filed Dec. 19, 2019, U.S. Pat. No. 11,539,681.
U.S. Appl. No. 16/593,561, filed Oct. 4, 2019, U.S. Pat. No. 11,258,595.
U.S. Appl. No. 16/453,682, filed Jun. 26, 2019, U.S. Pat. No. 11/233,780.
U.S. Appl. No. 16/271,455, filed Feb. 8, 2019, U.S. Pat. No. 10,594,679.
U.S. Appl. No. 16/271,428, filed Feb. 8, 2019, U.S. Pat. No. 10,523,432.
U.S. Appl. No. 16/201,401, filed Nov. 27, 2018, U.S. Pat. No. 10,700,856.
U.S. Appl. No. 16/200,118, filed Nov. 26, 2018, U.S. Pat. No. 10,498,530.
U.S. Appl. No. 16/110,804, filed Aug. 23, 2018, U.S. Pat. No. 10,382,422.
U.S. Appl. No. 16/036,506, filed Jul. 16, 2018, U.S. Pat. No. 10,530,575.
U.S. Appl. No. 15/983,957, filed May 18, 2018, U.S. Pat. No. 10,177,911.
U.S. Appl. No. 15/973,012, filed May 7, 2018, U.S. Pat. No. 10,250,386.
U.S. Appl. No. 15/972,914, filed May 7, 2018, U.S. Pat. No. 10,652,017.
U.S. Appl. No. 15/928,848, filed Mar. 22, 2018, U.S. Pat. No. 10,084,768.
U.S. Appl. No. 15/010,905, filed Jan. 29, 2016, U.S. Pat. No. 9,641,327.
U.S. Appl. No. 15/680,758, filed Aug. 18, 2017, U.S. Pat. No. 10,187,206.
U.S. Appl. No. 15/162,292, filed May 23, 2016, U.S. Pat. No. 10,362,012.
U.S. Appl. No. 14/751,119, filed Jun. 25, 2015, U.S. Pat. No. 9,961,060.
U.S. Appl. No. 15/457,700, filed Mar. 13, 2017, U.S. Pat. No. 9,998,281.
U.S. Appl. No. 15/583,968, filed May 1, 2017, U.S. Pat. No. 10,057,059.
U.S. Appl. No. 15/043,293, filed Feb. 12, 2016, U.S. Pat. No. 9,998,280.
U.S. Appl. No. 15/642,088, filed Jul. 5, 2017, U.S. Pat. No. 10,003,461.
U.S. Appl. No. 15/130,146, filed Apr. 15, 2016, U.S. Pat. No. 9,742,562.
U.S. Appl. No. 15/162,302, filed May 23, 2016, U.S. Pat. No. 9,698,981.
U.S. Appl. No. 14/789,255, filed Jul. 1, 2015, U.S. Pat. No. 9,596,078.
U.S. Appl. No. 14/139,419, filed Dec. 23, 2013, U.S. Pat. No. 9,351,162.
U.S. Appl. No. 14/136,711, filed Dec. 20, 2013, U.S. Pat. No. 9,351,162.
U.S. Appl. No. 14/099,329, filed Dec. 6, 2013, U.S. Pat. No. 9,300,473.
U.S. Appl. No. 14/084,141, filed Nov. 19, 2013, U.S. Pat. No. 9,319,223.
U.S. Appl. No. 14/064,618, filed Oct. 28, 2013, U.S. Pat. No. 9,118,464.
U.S. Appl. No. 14/055,606, filed Oct. 16, 2013, U.S. Pat. No. 9,276,740.
U.S. Appl. No. 14/039,401, filed Sep. 27, 2013, U.S. Pat. No. 9,288,059.
U.S. Appl. No. 14/023,181, filed Sep. 10, 2013, U.S. Pat. No. 9,350,550.
AU 2019246774, Oct. 8, 2019, AU2019246774A1 Issued Sep. 23, 2021.
GB 1068573, Oct. 27, 2014, Published Aug. 3, 2016.
GB 2100530, Oct. 27, 2014, Published on May 12, 2021.
CA 2,965,119, Oct. 27, 2014, Published on May 7, 2015.
HK 17101082.8, Oct. 27, 2014, Published on Oct. 20, 2017.
EU 14868381.6, Dec. 4, 2014, Published on Jan. 4, 2017.
CA 2,969,829, Dec. 4, 2014, Published on Jun. 11, 2015.
HK 17106540.3, Dec. 4, 2014, Published on Jan. 19, 2018.
International Search Report for PCT/US2014/068544 dated Feb. 13, 2015.
T. Pornin, Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm ECDSA), Internet Engineering Task Force RFC 6979, Aug. 2013, pp. I-79.
GSMA, Fast Dormancy Best Practices Version 1.0,Jul. 27, 2011, TS.18, pp. 1-23.
N. Chu et al., Exalted: Expanding LTE for Devices, European Commission for Information Society and Media, Oct. 31, 2012, pp. 1-141.
J. Huang et al, A Close Examination of Performance and Power Characteristics of 4G LTE Networks, Mobisys' 12, Jun. 25-29, 2012, pp. 1-14.
F. Qian et al., TOP: Tail Optimization Protocol for Cellular Resource Allocation, 18th IEEE International Conference on Network Protocols (ICNP), 2010, Oct. 5-8, 2010, pp. 285-298.
ETSI, Machine-to-Machine communications (M2M), mia, dla, and mid interfaces, TS 102.921 v1.1.1, Feb. 2012, pp. 1-538.
C. Downey, Migrating Legacy M2M Systems to the Cloud, http://www.ecnmag.com/articles/2013/02/migrating-legacy-m2m-systems-cloud, Feb. 2013, pp. 1-2.
A. Wander et al., Energy Analysis of Public-Key Cryptography on Small Wireless Devices, Sun Microsystems Laboratories, pp. 1-16.
V. Martinez et al., A Survey of the Elliptic Curve Integrated Encryption Scheme, Journal of Computer Science and Engineering, vol. 2, Aug. 2010, pp. 7-13.
ETSI, UMTS;LTE; SIM/USIM Internal and External Interworking Aspects, TR 131900 v. 10.0.0, May 2011, pp. 1-41.
International Search Report and Written Opinion for PCT/US2014/062435 mailed Feb. 6, 2015.
Wikipedia, RSA (algorithm), http://en.wikipedia.org/wiki/RSA_(algorithm), Sep. 9, 2013, pp. 1-12.
Wikipedia, Elliptic Curve Cryptography, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography, Sep. 9, 2013, pp. 1-8.
L. Larzon, The Lightweight User Datagram Protocol (UDP-Lite), Internet Engineering Task Force RFC 3828, Jul. 2004, pp. 1-12.
Wikipedia, Digital Signature, http://en.wikipedia.orglwiki/Digital_signature, Sep. 9, 2013, pp. 1-10.
D. Cooper, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force RFC 5280, pp. 1-133.
J. Jonsson et al., Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Internet Engineering Task Force RFC 3447, Feb. 2003, pp. 1-72.
D. McGrew et al., Fundamental Elliptic Curve Cryptography Algorithms, Internet Engineering Task Force RFC 6090, Feb. 2011, pp. 1-34.
Wikipedia, Elliptic Curve Diffie-Hellman, http://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman, Sep. 24, 2013, pp. 1-2.
ETSI, Smart Cards; Embedded UICC; Requirements Specification, TS 103 383 v12.1.0, Jun. 2013, pp. 1-20.

Petitioner Samsung Ex-1004, 0006

(56) **References Cited**

OTHER PUBLICATIONS

3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture, 3GPP TS 33.401 V12.9.0 (Sep. 2013) pp. 1-75.
3GPP, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3, 3GPP TS 24.301 v12.2.0, Sep. 2013 pp. 1-6, 63-100.
ETSI, Smart Cards; UICC-Terminal Interfaces; Physical and Logical Characteristics, TS 102 221 v11.0.0, Jun. 2012, pp. 1-181.
Cakulev et al., "An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange," Aug. 2012, pp. 1-32.
Gollmann, "Authentication—Myths and Misconceptions," Progress in Computer Science and Applied Logic, vol. 20, 2001, pp. 203-225.
Tin et al., "Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach," Information Security Research Centre, Queensland University of Technology, Australia, 2003, pp. 166-179.
Hegland et al., "A Framework for Authentication in NBD Tactical Ad Hoc Networks," IEEE Communications Magazine, Oct. 2011, pp. 64-71.
Nicholson et al., "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, vol. 5, No. II, Nov. 2006, pp. 1489-1502.
Schwaiger et al., "Smart Card Security for Fieldbus Systems," 2003, pp. 398-406.
CSMG, Reprogrammable SIMs: Technology, Evolution and Implications, Sep. 25, 2012, pp. 1-95.
GlobalPlatform Inc., GlobalPlatform Card Specification, Version 2.2.1, Jan. 2011, pp. 1-303.
GlobalPlatform Inc., GlobalPlatform Card Security Upgrade for Card Content Management, Card Specification v 2.2.—Amendment E, Version 1.0, Nov. 2011, pp. 1-35.
GSM Association, Embedded SIM Task Force Requirements and Use Cases, Version 1.0, Feb. 21, 2011, pp. 1-38.
Kirk H.M. Wong et al., A Dynamic User Authentication Scheme for Wireless Sensor Networks, Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 1-8.
Pierre E. Abi-Char, et al., A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol for Low Power Mobile Communications, The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007), pp. 1-6.
Jun Shao, et al., An Improved Deniable Authentication Protocol, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, People's Republic of China, pp. 1-3.
Chris Foresman, Embedded SIM could cause carrier conflict for Apple, Nov. 19, 2010, pp. 1-2.
Embedded UICC Remote Provisioning Discussion, Source: Rogers Wireless, 3GPP/SA3-LI#46, Quebec City, Canada, Jul. 17-19, 2012, p. 1-39.
GSMA Launches Embedded SIM Initiative to Support the Connected Future, Nov. 18, 2010, p. 1-4.
Chang-Seop Park, On Certificate-Based Security Protocols for Wireless Mobile Communication Systems, Dankook University, IEEE Network Sep./Oct. 1997, pp. 50-55.
M. Prasad, et al., Secure Authentication Key Agreement Protocol for Long Term Evolution—Advanced, Research Scholar, Associate Professor, Department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry, India, Elsevier, 2012, pp. 158-162.
Eun-Jun Yoon, et al., Secure Deniable Authentication Protocol Based on ElGamal Cryptography, 2008 International Conference on Information Security and Assurance, pp. 36-39.
Pietre-Cambacedes et al., Cryptographic key management for SCADA systems—issues and perspectives, 2008 International Conference on Information Security and Assurance, IEEE, pp. 156-161.
Bender et al., Evolution of SIM provisioning towards a flexible MCIM provisioning in M2M vertical industries, 16th International Conference on Intelligence in Next Generation Networks, IEEE, 2012, pp. 57-64.
Park et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 International Conference on Availability, Reliability and Security, IEEE, 2013, pp. 297-303.
Appenzeller et al., Identity-Based Encryption Architecture and Supporting Data Structures RFC 5408, 2009, pp. 1-30.
Baugher et al., Group Key Management Architecture, RFC Draft, 2001, pp. 1-20.
Ben Saied, Yosra; Olivereau, Alexis; Laurent, Maryline; "A Distributed Approach for Secure M2M Communications", 5th International Conference on New Technologies, Mobility and Security (NTMS), May 7-10, 2012, pp. 1-7.
Boyen et al., Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles), 2006.
Boyen et al., Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BBI Cryptosystems, RFC 5091, 2007, pp. 1-63.
Harney et al., Group Key Management Protocol (GKMP) Architecture, 1994, pp. 1-19.
Kiltz et al., CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption, 2008.
Krylov, What is Kerberos Authentication?, 2003, pp. 1-4.
Martin, Introduction to Identity-Based Encryption, ISBN-13 978-1-59693-238-8, 2008.
Merrian-Webster, Network, 2014.
Park et al., A New Practical Identity-Based Encryption System, 2003, pp. 1-27.
Park et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 IEEE, pp. 297-303.
Shih, Jie-Ren; Hu, Yongbo; Hsiao, Ming-Chun; Chen, Ming-Shing; Shen, Wen-Chng; Yang, Bo-Yin; Wu, An-Yeu; Cheng, Chen-Mou; "Securing M2M with Post-Quantum Public-Key Cryptography", IEEE Journal on Emerging and Selected Topics in Circuits and Systems, Mar. 7, 2013, pp. 106-116.
Voltage Security, The Identity-Based Encryption Advantage, 2015.
Yang et al., Identity-Based Key Agreement and Encryption for Wireless Sensor Networks, IJCSNS International Journal of Computer Science and Network Security, vol. 6, No. 5B, May 2006, pp. 182-189.
Youngblood, An Introduction to Identity-based Cryptography, 2005.
Zhu et al., Public Key Cryptography for Initial Authentication in Kerberos (PPKINIT), RFC 4556, 2006, pp. 1-42.
Search Report issued in UK Application No. GB2108534.5 dated Jul. 7, 2021.
ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000).
TLS 1.3 Wish List Presentation, IETF 87 (Eric Rescorla), dated Aug. 1, 2013.
European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182424.8 dated Oct. 12, 2021.
European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182451.1 dated Oct. 12, 2021.
European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182432.1 dated Oct. 12, 2021.

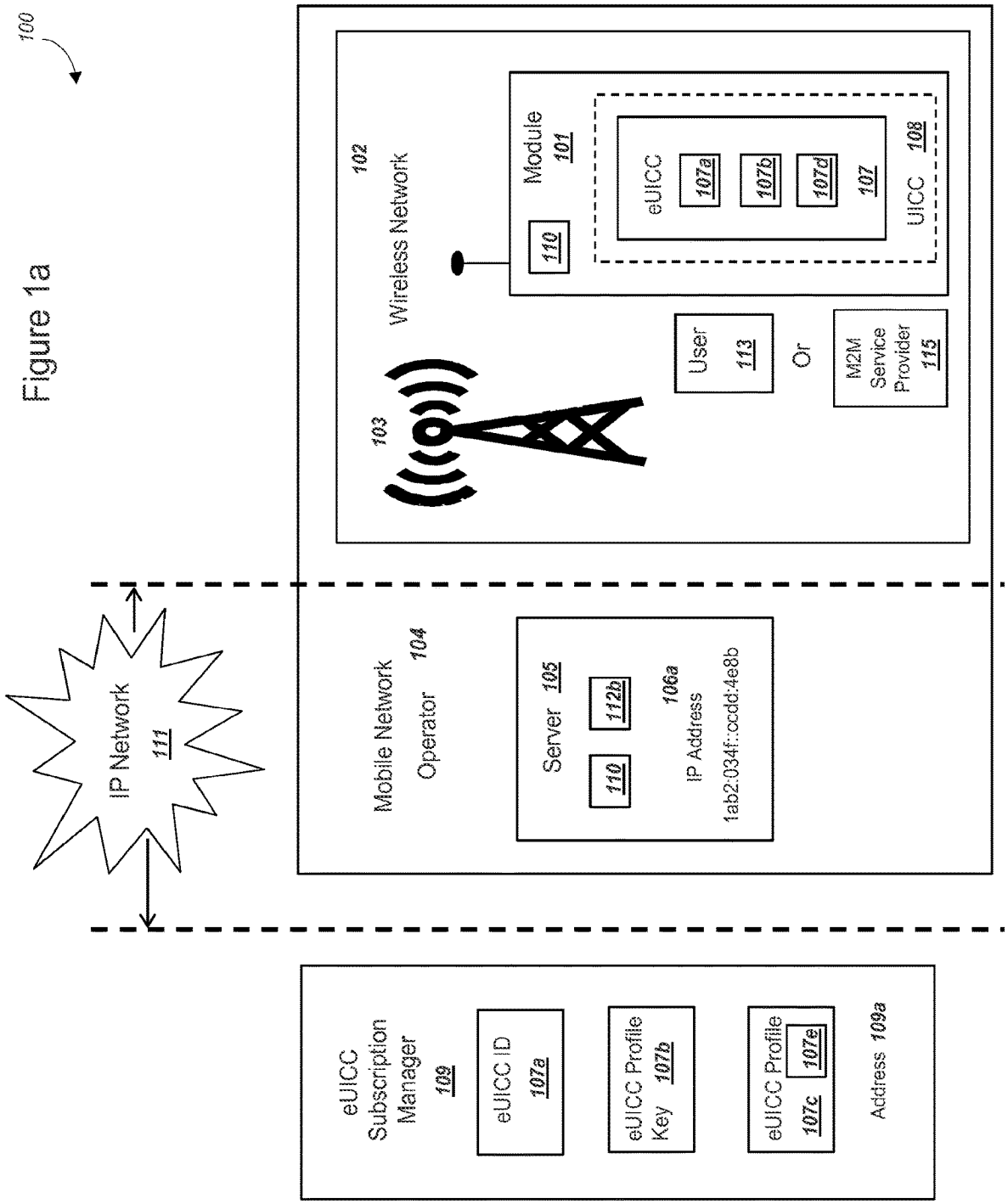

100
Figure 1a
102
Wireless Network
103
Module
101
110
eUICC
107a
107b
107d
107
UICC
108
User
113
Or
M2M
Service
Provider
115
Mobile Network
Operator
104
Server
105
110
112b
106a
IP Address
1ab2:034f::ccdd:4e8b
IP Network
111
eUICC
Subscription
Manager
109
eUICC ID
107a
eUICC Profile
Key
107b
eUICC Profile
107c
107e
Address
109a

Figure 1c

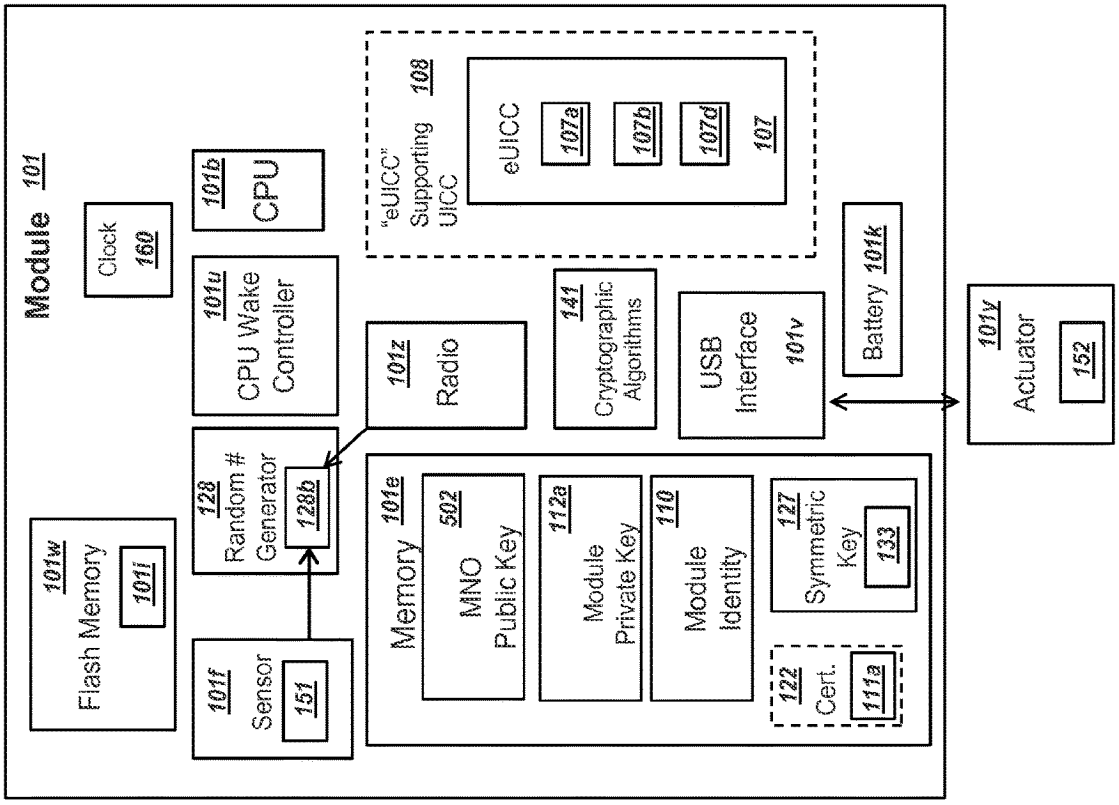


Figure 1b

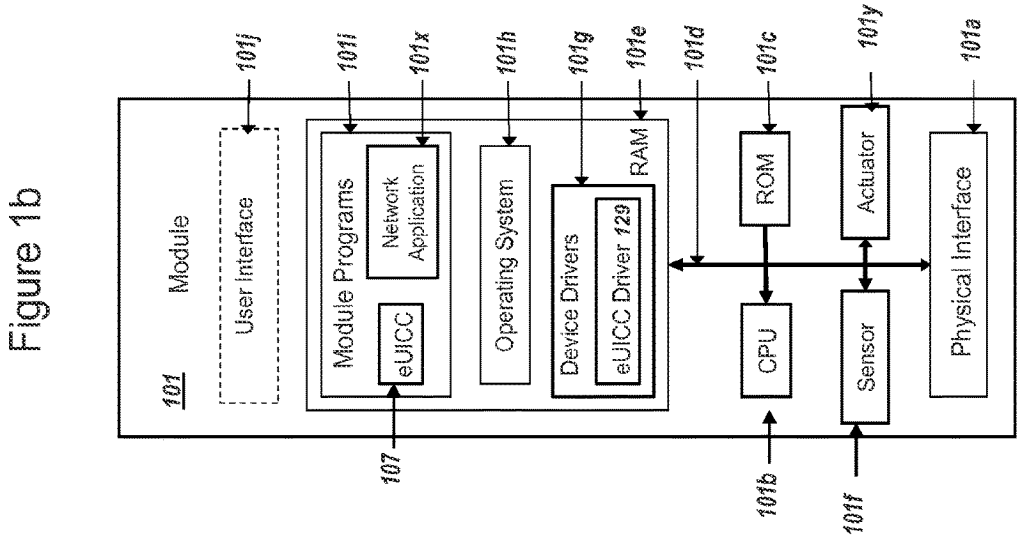


Figure 1d

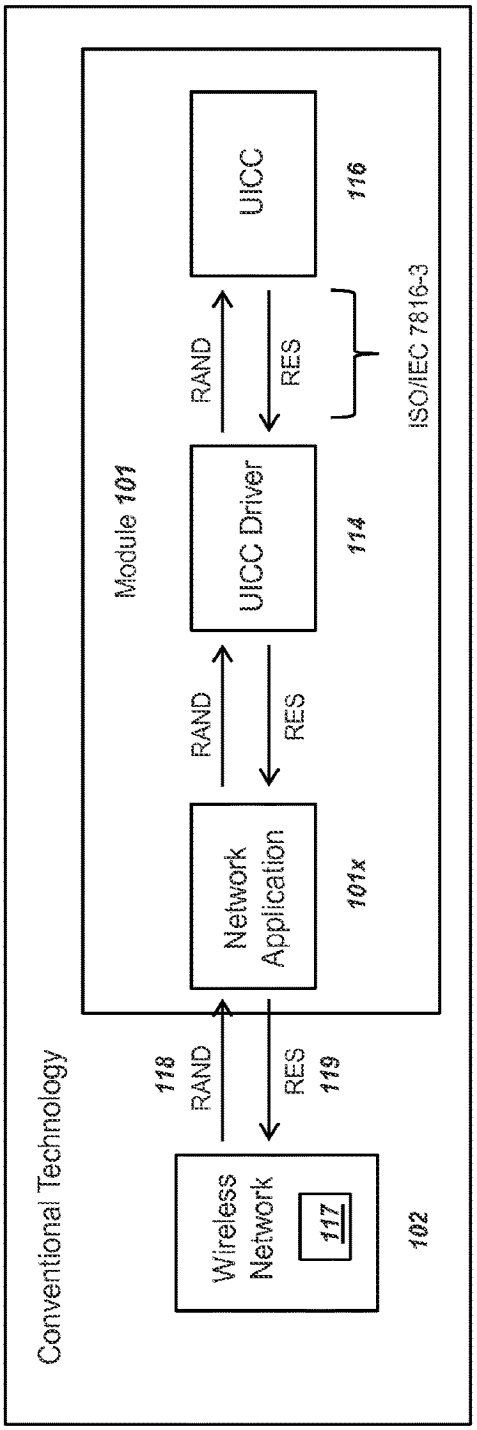
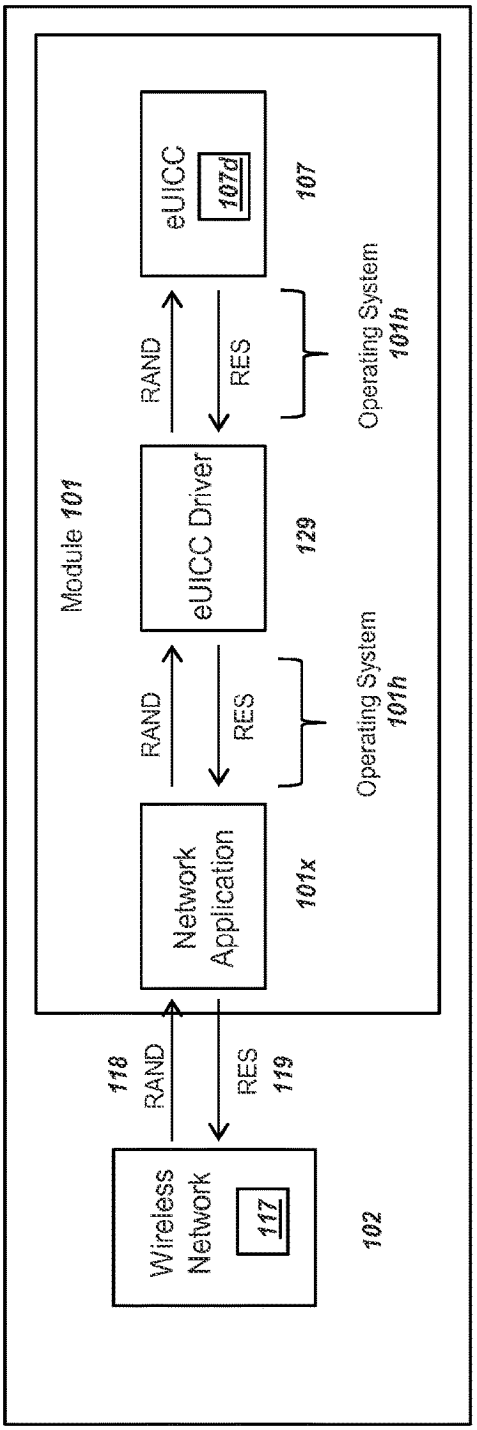


Figure 1e



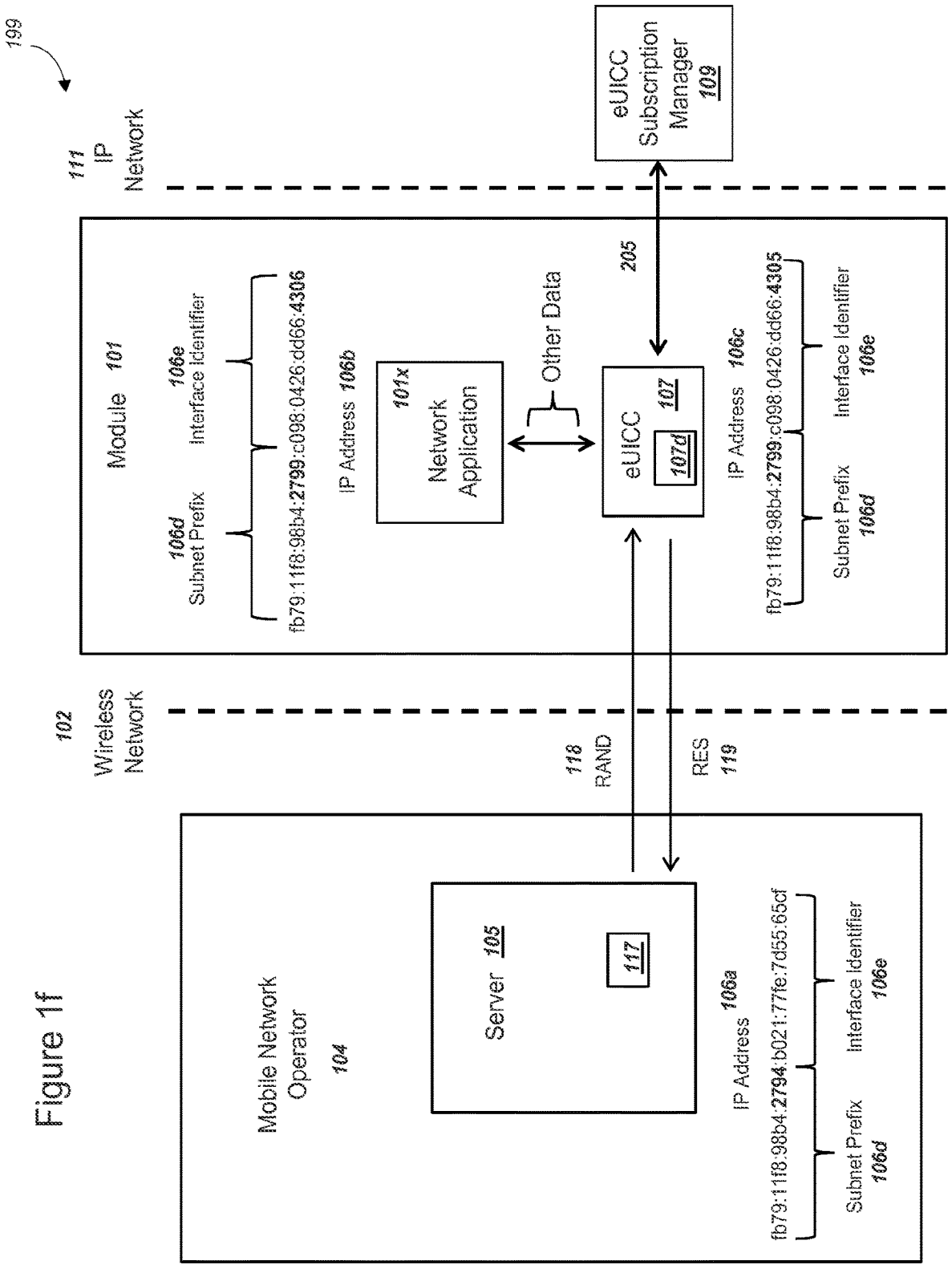
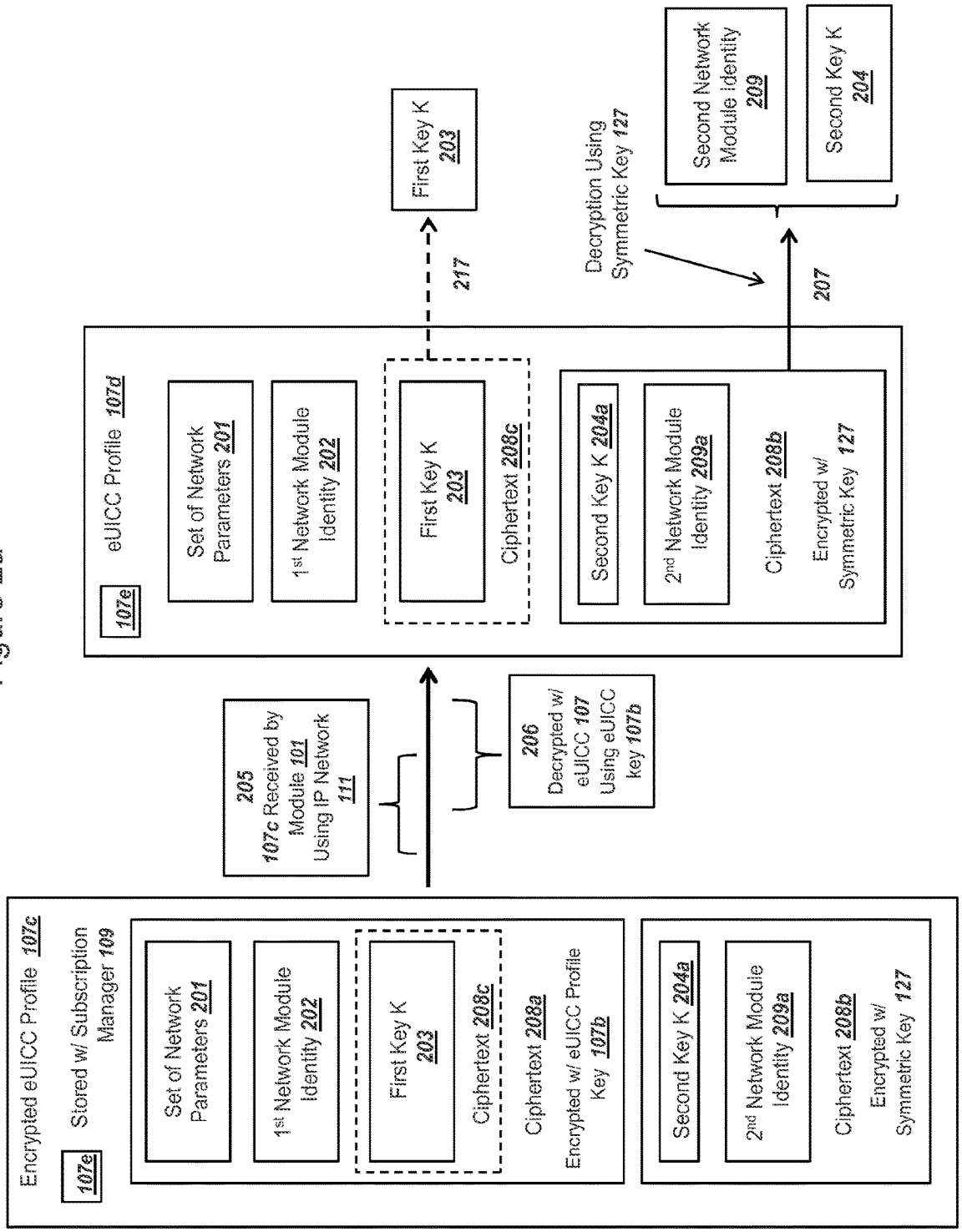

199
111
IP
Network
eUICC
Subscription
Manager
109
205
Module 101
106e
Interface Identifier
106d
Subnet Prefix
fb79:11f8:98b4:2799:c098:0426:dd66:4306
IP Address 106b
101x
Network
Application
Other Data
eUICC 107
107d
IP Address 106c
fb79:11f8:98b4:2799:c098:0426:dd66:4305
Subnet Prefix 106d
Interface Identifier 106e
102
Wireless
Network
118
RAND
RES
119
Mobile Network
Operator
104
Server 105
117
IP Address 106a
fb79:11f8:98b4:2794:b021:77fe:7d55:65cf
Subnet Prefix 106d
Interface Identifier 106e

Figure 1f

Figure 2a


Encrypted eUICC Profile 107c
Stored w/ Subscription Manager 109
107e
Set of Network Parameters 201
1st Network Module Identity 202
First Key K 203
Ciphertext 208c
Ciphertext 208a
Encrypted w/ eUICC Profile Key 107b
Second Key K 204a
2nd Network Module Identity 209a
Ciphertext 208b
Encrypted w/ Symmetric Key 127
205
107c Received by Module 101 Using IP Network 111
206
Decrypted w/ eUICC 107 Using eUICC key 107b
eUICC Profile 107d
107e
Set of Network Parameters 201
1st Network Module Identity 202
First Key K 203
Ciphertext 208c
Second Key K 204a
2nd Network Module Identity 209a
Ciphertext 208b
Encrypted w/ Symmetric Key 127
217
First Key K 203
Decryption Using Symmetric Key 127
207
Second Network Module identity 209
Second Key K 204

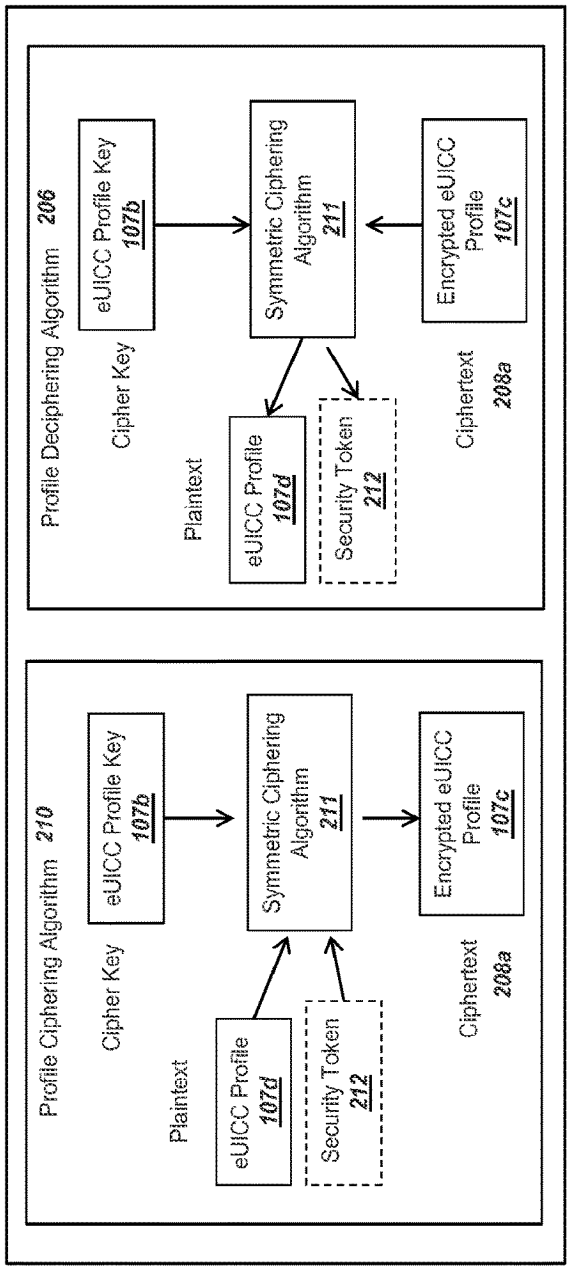


Figure 2b

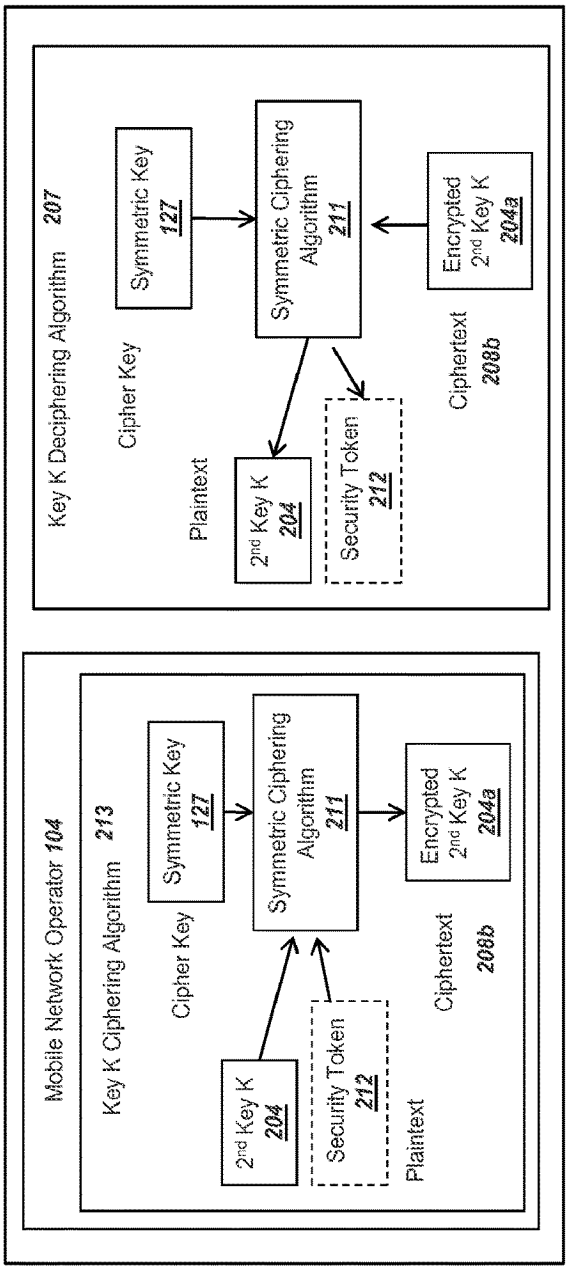


Figure 2c

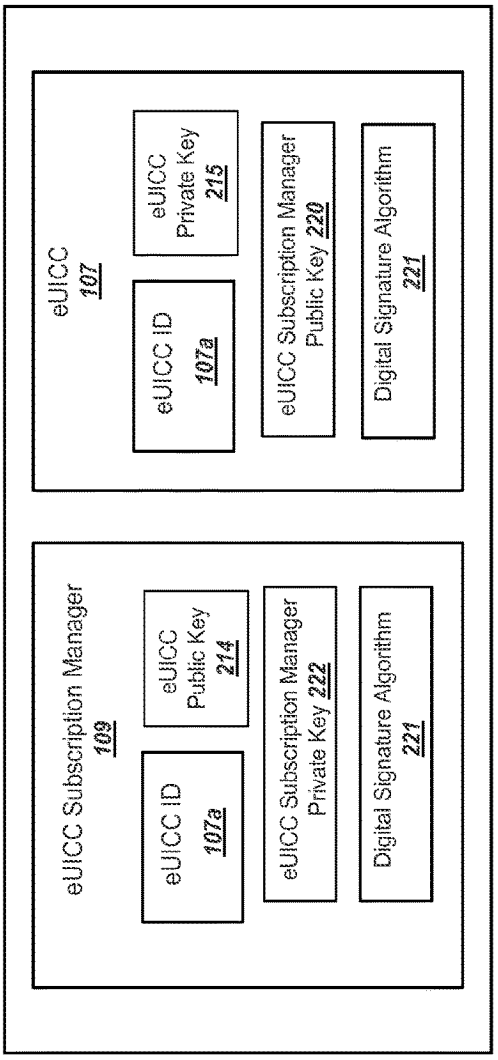


Figure 2d

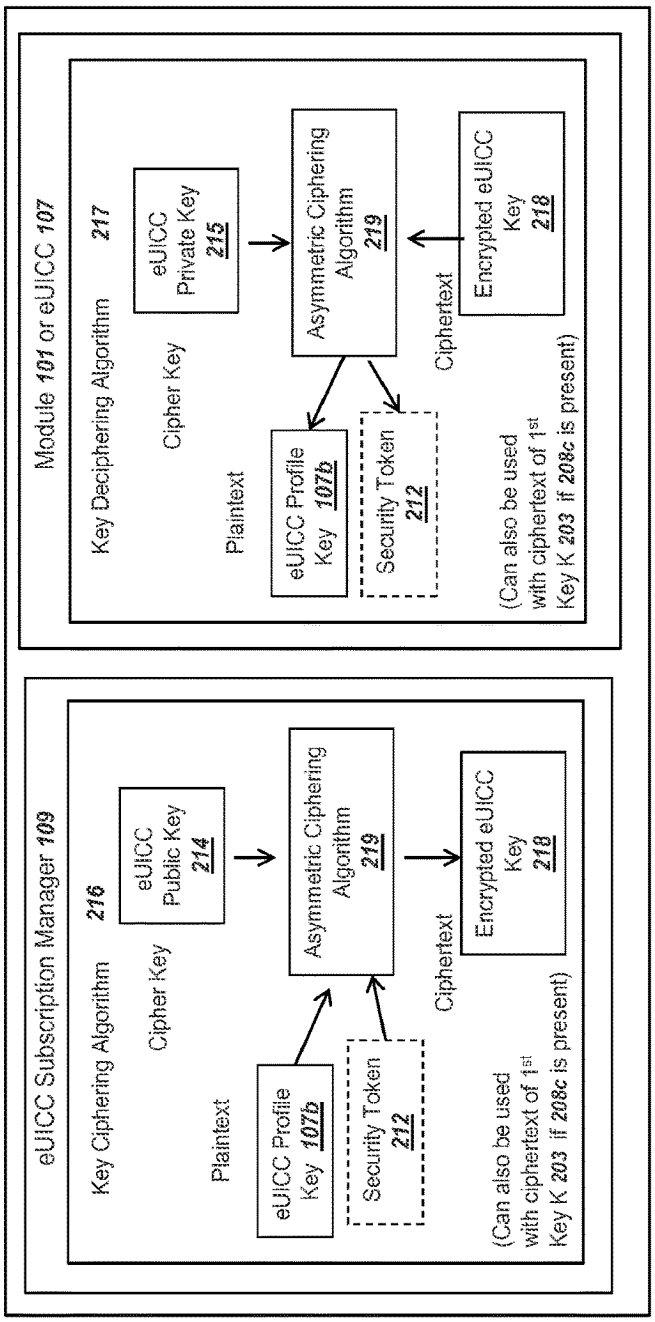


Figure 2e

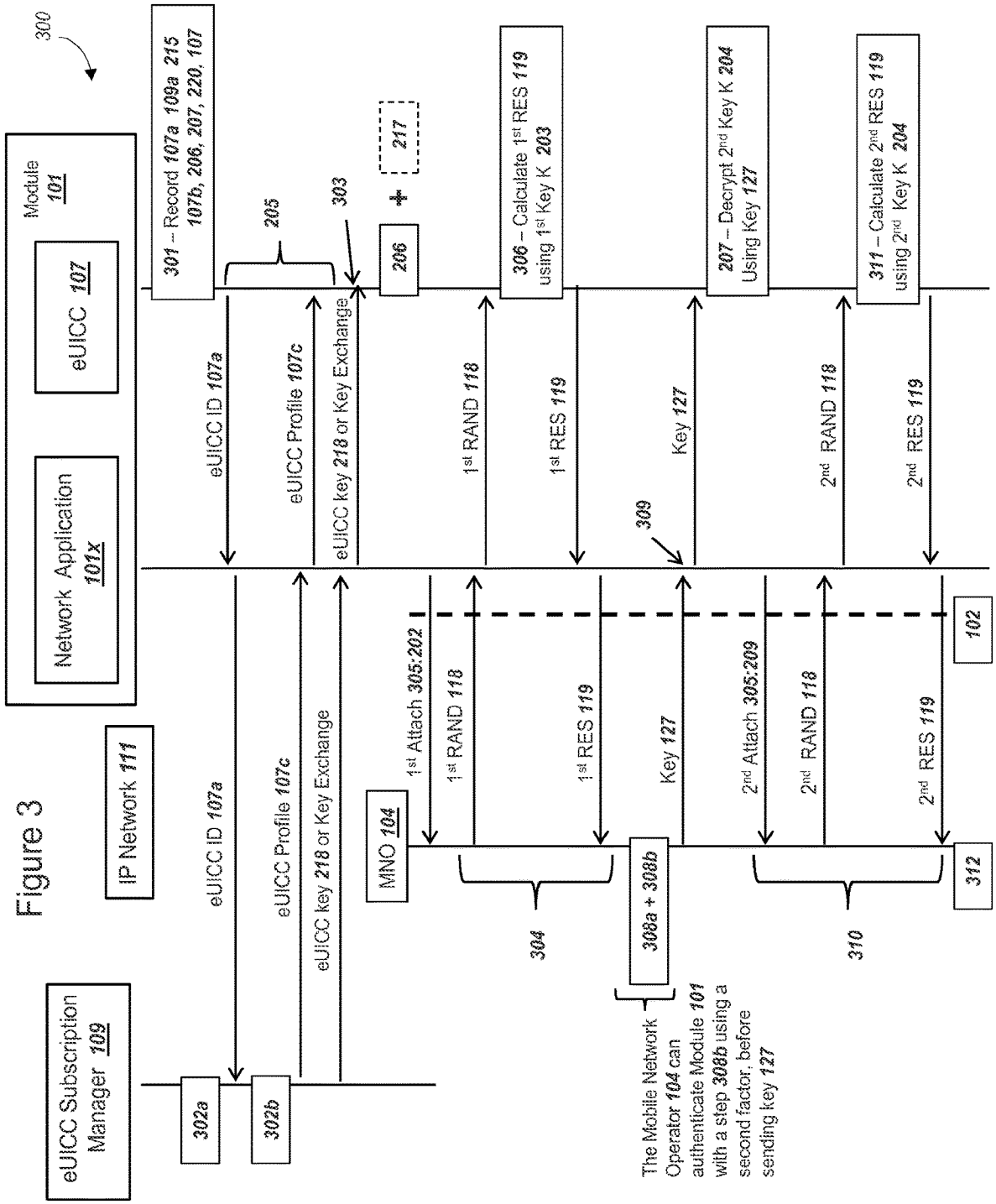
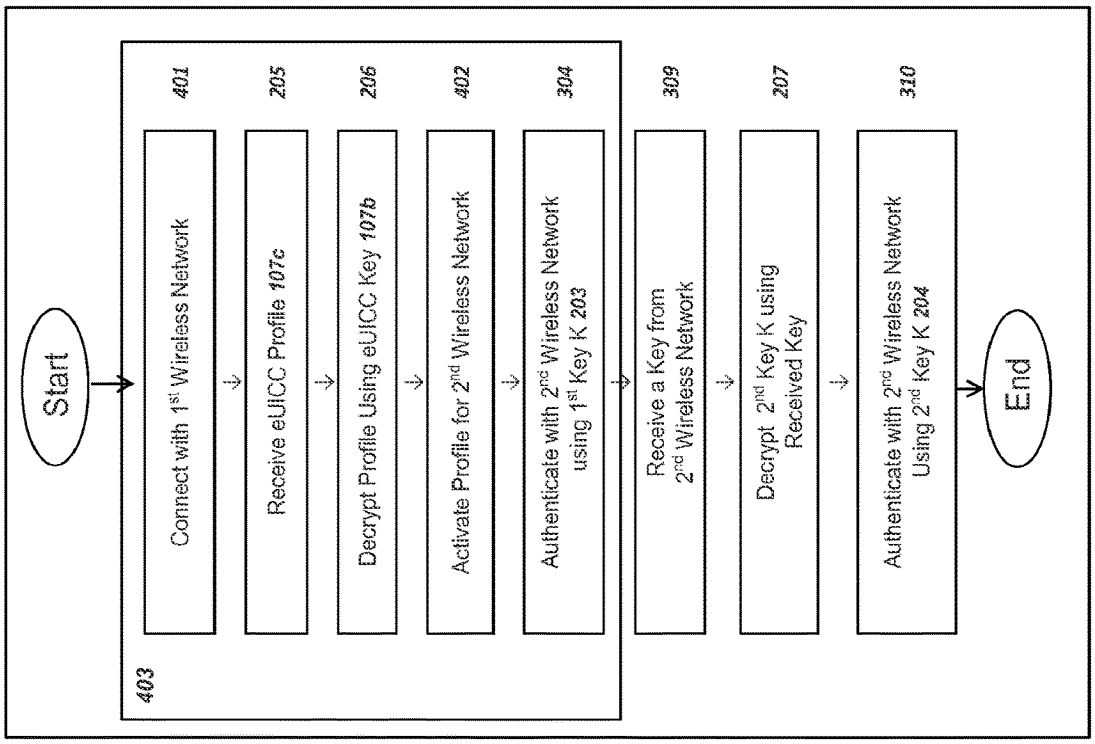

300
Module 101
eUICC 107
Network Application 101x
301 – Record 107a 109a 215 107b, 206, 207, 220, 107
205
303
206
217
306 – Calculate 1st RES 119 using 1st Key K 203
207 – Decrypt 2nd Key K 204 Using Key 127
311 – Calculate 2nd RES 119 using 2nd Key K 204
eUICC ID 107a
eUICC Profile 107c
eUICC key 218 or Key Exchange
1st RAND 118
1st RES 119
Key 127
309
2nd RAND 118
2nd RES 119
eUICC Subscription Manager 109
IP Network 111
MNO 104
1st Attach 305:202
2nd Attach 305:209
102
302a
302b
304
308a + 308b
310
312
The Mobile Network Operator 104 can authenticate Module 101 with a step 308b using a second factor, before sending key 127

Figure 3

Figure 4


Start
401
Connect with 1st Wireless Network
205
Receive eUICC Profile 107c
206
Decrypt Profile Using eUICC Key 107b
402
Activate Profile for 2nd Wireless Network
304
Authenticate with 2nd Wireless Network using 1st Key K 203
403
309
Receive a Key from 2nd Wireless Network
207
Decrypt 2nd Key K using Received Key
310
Authenticate with 2nd Wireless Network Using 2nd Key K 204
End

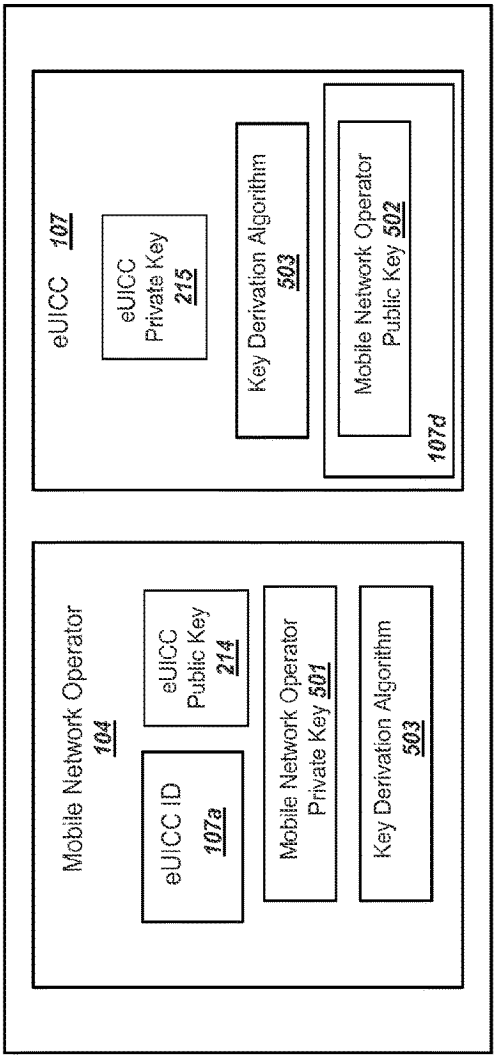


Figure 5a

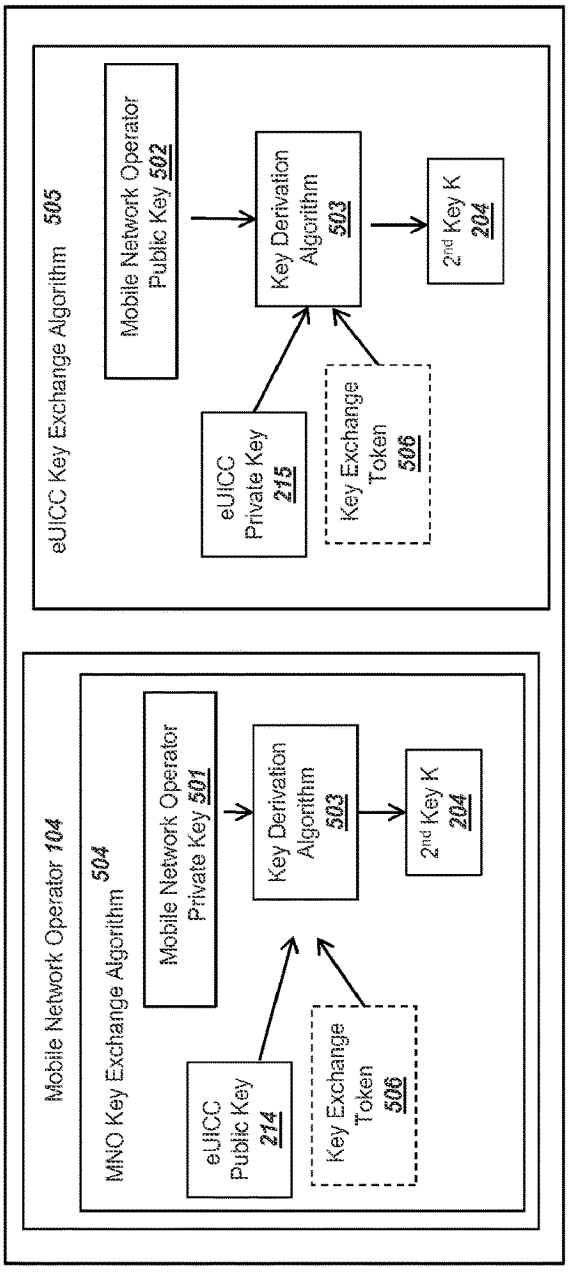


Figure 5b

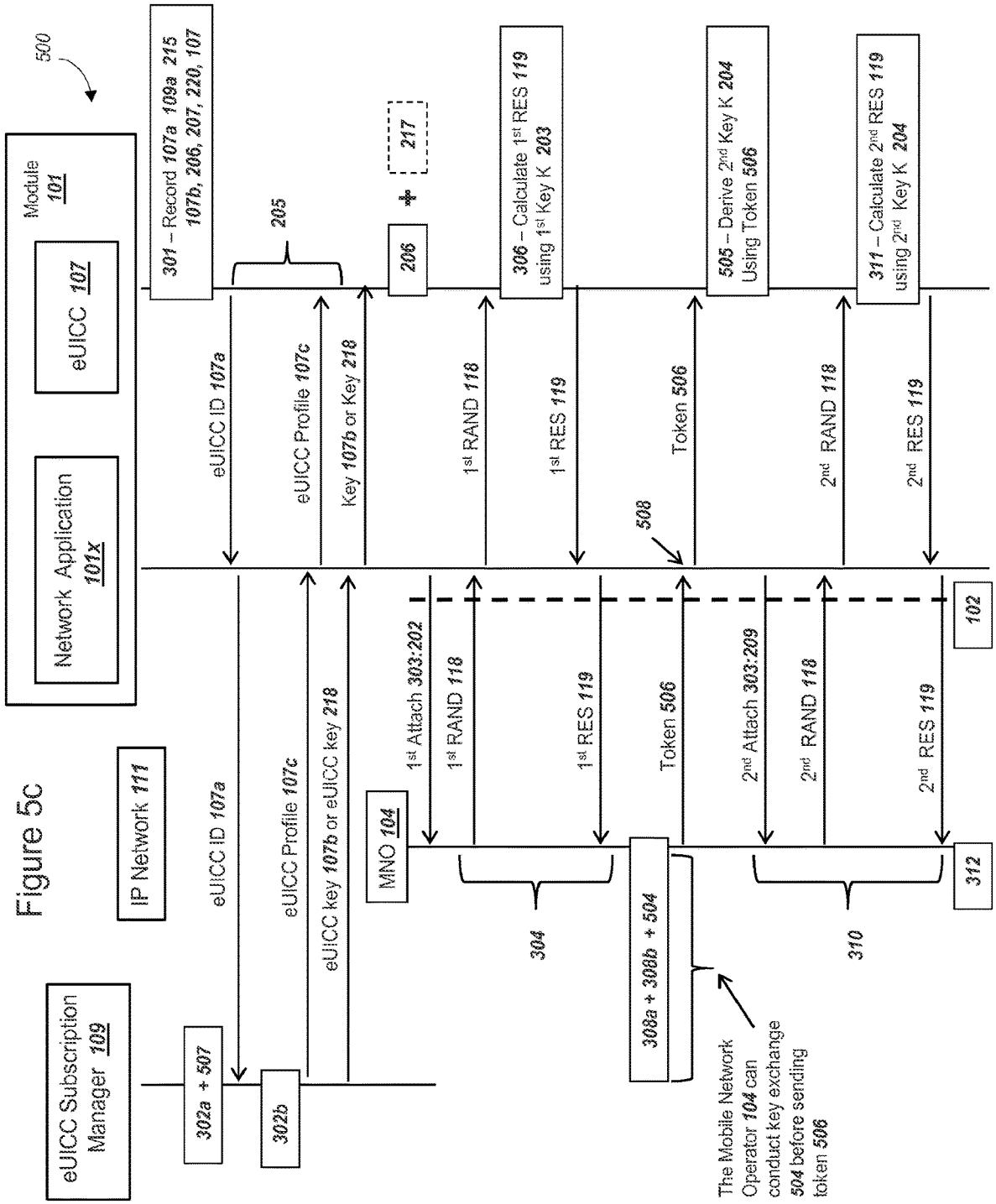
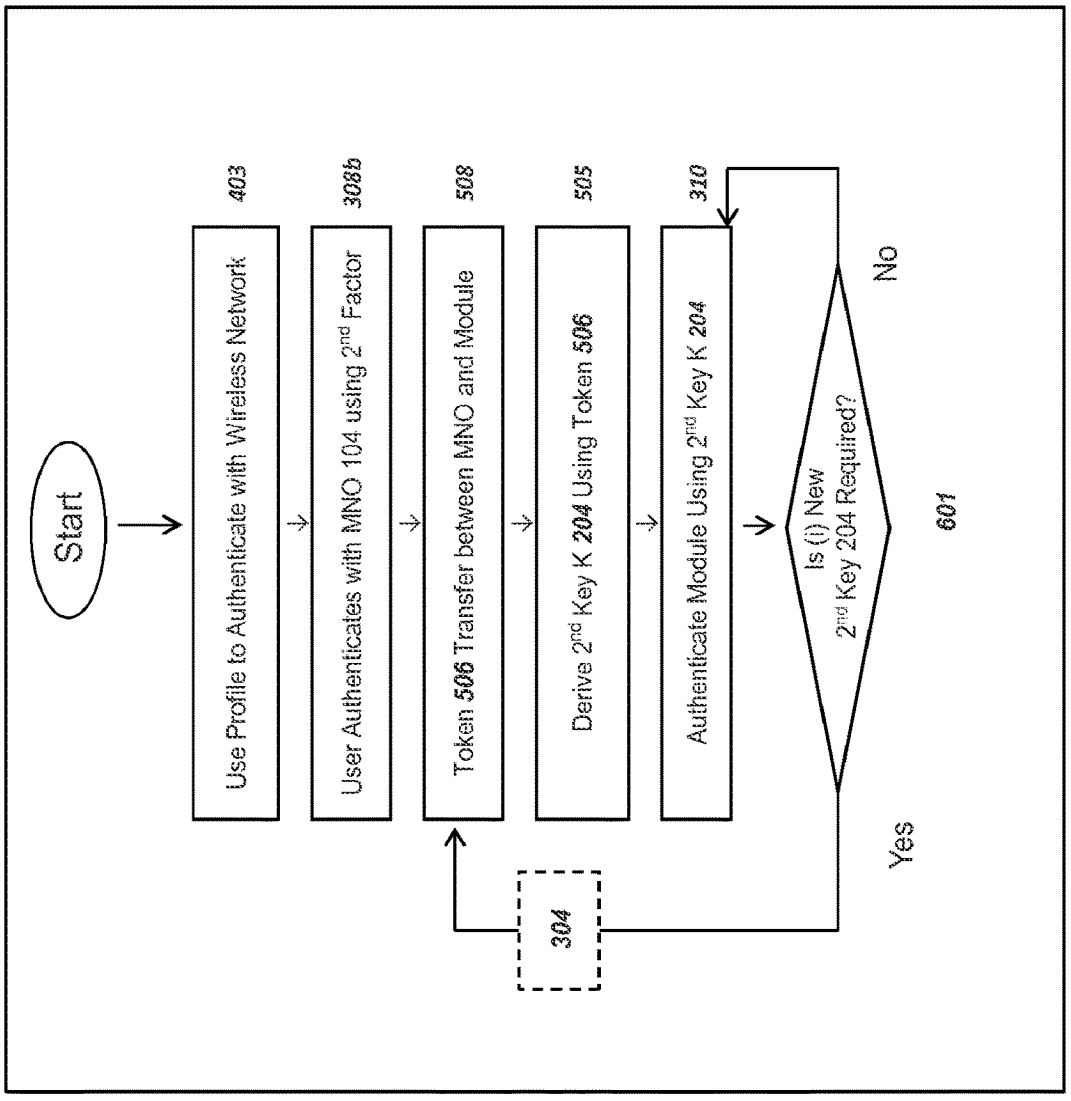

500
Module 101
eUICC 107
Network Application 101x
eUICC Subscription Manager 109
IP Network 111
MNO 104
102
312
301 – Record 107a 109a 215 107b, 206, 207, 220, 107
205
206
217
302a + 507
302b
eUICC ID 107a
eUICC Profile 107c
eUICC key 107b or eUICC key 218
Key 107b or Key 218
1st Attach 303:202
1st RAND 118
1st RES 119
306 – Calculate 1st RES 119 using 1st Key K 203
Token 506
508
505 – Derive 2nd Key K 204 Using Token 506
2nd Attach 303:209
2nd RAND 118
2nd RES 119
311 – Calculate 2nd RES 119 using 2nd Key K 204
304
308a + 308b + 504
310
The Mobile Network Operator 104 can conduct key exchange 504 before sending token 506

Figure 5c

Figure 6


Start
Use Profile to Authenticate with Wireless Network
403
User Authenticates with MNO 104 using 2nd Factor
308b
Token 506 Transfer between MNO and Module
508
Derive 2nd Key K 204 Using Token 506
505
Authenticate Module Using 2nd Key K 204
310
Is (i) New 2nd Key 204 Required?
No
Yes
304
601

EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

This is a continuation of U.S. patent application Ser. No. 17/547,990, filed Dec. 10, 2021, and entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication", which is a continuation of U.S. patent application Ser. No. 16/453,682, filed Jun. 26, 2019, entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," which is a continuation of U.S. patent application Ser. No. 16/110,804, filed Aug. 23, 2018, entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," which is a continuation of U.S. patent application Ser. No. 15/928,848, filed Mar. 22, 2018, entitled "EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION," which is a continuation of U.S. patent application Ser. No. 14/751,119, filed Jun. 25, 2015, entitled "An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication", now U.S. Pat. No. 9,961,060, which is a continuation of U.S. patent application Ser. No. 14/099,329, filed Dec. 6, 2013, entitled "An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," now U.S. Pat. No. 9,100,175, the contents of all of which are incorporated herein by reference in their entirety.

The subject matter of this application is related to the subject matter of U.S. patent application Ser. No. 14/084,141, filed Nov. 19, 2013 in the name of John Nix, entitled "Key Derivation for a Module using an Embedded Universal Integrated Circuit Card," now U.S. Pat. No. 9,319,223, which is hereby incorporated by reference in its entirety.

BACKGROUND

Technical Field

The present methods and systems relate to communications for a module, and more particularly, to methods and systems for using an embedded universal integrated circuit card (eUICC), where the methods and systems also support the authentication of a user associated with the eUICC.

Description of Related Art

The combination of "machine-to-machine" (M2M) communications and using low-cost sensors, Internet connections, and processors is a promising and growing field. Among many potential benefits, M2M technologies allow the remote monitoring and/or control of people, assets, or a location where manual monitoring is not economic, or costs can be significantly reduced by using automated monitoring as opposed to manual techniques. Prominent examples today include vending machines, automobiles, alarm systems, and remote sensors. Fast growing markets for M2M applications today include tracking devices for shipping containers or pallets, health applications such as, but not limited to, the remote monitoring of a person's glucose levels or heartbeat, monitoring of industrial equipment deployed in the field, and security systems. Many M2M applications leverage either wired Internet connections or wireless connections, and both types of connections continue to grow rapidly. M2M applications may also be referred to as "the Internet of things".

M2M communications can provide remote control over actuators that may be connected to a M2M device, such as, but not limited to, turning on or off a power switch, locking or unlocking a door, adjusting a speed of a motor, or similar remote control. A decision to change or adjust an actuator associated with an M2M device can utilize one or a series of sensor measurements. An M2M device may also be referred to as a "wireless module" or also simply a module. As one example, if a building or room is too cold, then temperature can be reported to a central server by an M2M device and the server can instruct the M2M device to turn on a switch that activates heat or adjusts a thermostat. As the costs for computer and networking hardware continue to decline, together with the growing ease of obtaining either wired or wireless Internet access for small form-factor devices, the number of economically favorable applications for M2M communications grows.

Many M2M applications can leverage wireless networking technologies. Wireless technologies such as, but not limited to, wireless local area networks and wireless wide area networks have proliferated around the world over the past 15 years, and usage of these wireless networks is also expected to continue to grow. Wireless local area network (LAN) technologies include WiFi and wireless wide area network (WAN) technologies include 3rd Generation Partnership Project's (3GPP) 3rd Generation (3G) Universal Mobile Telecommunications System (UMTS) and 4th Generation (4G) Long-term Evolution (LTE), LTE Advanced, and the Institute of Electrical and Electronics Engineers' (IEEE) 802.16 standard, also known as WiMax. The use of wireless technologies with M2M communications creates new opportunities for the deployment of M2M modules in locations less suitable for fixed-wire Internet access, but also creates a significant new class of problems that need to be solved.

One class of problems for using M2M modules with traditional wireless networks results from basic design considerations for the wireless networks, where many wireless wide-area networking standards were designed and optimized for mobile phones, including smart phones. A core element of traditional wireless WAN technologies such as 3GPP and ETSI standards over the past 20 years has included the use of a subscriber identity module (SIM) card within 2G networks and a related universal integrated circuit card (UICC) for 3G and 4G networks, including LTE networks. ETSI standards for a physical UICC as of 2013 include ETSI TR 102 216. Traditionally, these cards have been supplied by a mobile network operator (MNO) and contain 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. The parameters could include (i) an identity such as an IMSI, (ii) a set of frequencies for a mobile phone to scan in order to locate a beacon signal from the MNO, (iii) a preferred access list of other MNOs in order to support roaming in locations where the MNI associated with the IMSI is not available, and (iv) many other related parameters as well. The physical media and cards in the form of a UICC can be appropriate or suitable for a mobile phone or mobile handset, where an end user can readily replace or "swap out" the physical card as the mobile phone changes geographical locations or due to other preferences for the subscriber or end-user. Distribu-

Petitioner Samsung Ex-1004, 0020

tors of either mobile handsets or mobile phone service can physically insert or change an appropriate UICC for the mobile phones as well.

However, the rapid growth for "machine-to-machine" applications has created significant challenges to the traditional model of utilizing physical media such as a UICC in order to provide data and parameters for a module's connectivity to a MNO. Exemplary reasons for potential difficulties with physical media such as a UICC in M2M applications include (i) the modules may be installed in remote locations that are difficult or expensive to reach after installation, such as, but not limited to, tracking devices on shipping containers that can move globally, (ii) a manufacturer or service provider may prefer for the module to be hermetically sealed for business or technical reasons, including the physical UICC may not be easily tampered with, and (iii) a module (such as a tracking device on a 40 foot shipping container) may move between several different countries, and the lowest costs for Internet or data connectivity through the wireless WAN may be through utilizing different UICC cards from different operators, but the cost of swapping the UICC card could be prohibitive.

Other needs for changing a preferred network or network credentials without physically changing a UICC exist as well. These needs have been one motivation for the industry, including ETSI and 3GPP standards bodies, to consider an embedded UICC, also known as an "eUICC". With an eUICC, the operation of an UICC can be essentially "virtualized", such that the data and algorithms within a UICC can be processed in software and distributed through electronic media (such as, but not limited to, a file transfer or file download). Exemplary benefits and technical considerations for using an eUICC in M2M applications as of November 2013 is outlined in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. Note that this published standard from June 2013, and the standard is primarily in the requirements definition phase, and many of the technical specifications for implementation and operation of an eUICC will be defined in the future.

Although the use of an embedded eUICC can solve many of the issues for distributing and managing physical media such as a UICC, many additional challenges remain. Many open and remaining challenges for a eUICC pertain to securely and electronically transferring a new set of MNO network access credentials (such as an IMSI and network key K) to a module in a secure and efficient manner. A need exists in the art for a module to securely obtain network access credentials. Another need exists in the art for the obtained credentials in a eUICC to be fully compatible with the significant installed and legacy base of networks that use a pre-shared secret key K, where the key K serves as the foundation for authentication and ciphering of data for a mobile phone or user equipment, including modules using conventional technology. A successful solution to these needs for M2M applications in the form of an eUICC can also provide a working solution of the needs for regular mobile phones as well, such that a consumer mobile phone or smartphone could implement and utilize an eUICC in order to eliminate the costs and complexity of dealing with a physical UICC.

A need exists in the art for module and a mobile network operator to securely share a pre-shared secret key K without depending on physical distribution of the key K or electronic distribution of the key K through 3rd parties, even in an encrypted form. A need exists in the art for the decryption of data within an eUICC profile to be under the control of the mobile network operator, because the mobile network operator may not control the distribution or release of profiles from an eUICC subscription manager to a module with an eUICC. As currently contemplated in November of 2013 by eUICC standards discussed above, a pre-shared secret key K and related network access credentials are transmitted to a module from an eUICC subscription manager. The pre-shared secret key K is also known as key K in 4G LTE and related networks and key Ki in 3G networks. The resulting security for the electronically transferred, pre-shared secret key K is no stronger than (i) the encryption on the channel used to transfer key K, and (ii) the security and chain of control for keys used to encrypt the communications channel transferring key K to a module or a mobile phone. A module and mobile network operator (MNO) using an electronically transferred key K for network access credentials is dependent on the communications channel for transferring key K, even though that communications channel may be outside the control of the MNO (such as at a time when key K is transferred using another MNO or a different network). Therefore, a need exists in the art for the MNO to securely and efficiently control the use of an electronically transferred key K within a profile for an eUICC, even though copying and distributing the profile may be outside the control of the MNO.

In addition, over an extended period of time such as several years, a mobile network operator could prefer for the key K to periodically rotate or change for an individual module or mobile phone in order to increase security. The continued and extended use of a single key K for all communications with a module or mobile phone can be a security risk, especially with a large volume of data transferred that could be subject to analysis for cryptographic weaknesses by potential attackers. Additionally, in the future a standard key length for key K may increase from today's current 128 bits to a longer key length such as an exemplary 256 bits. With conventional technology where key K is recorded in physical media such as a UICC, the only feasible way to change key K for a module or mobile phone is to physically distribute a new UICC card, with resulting costs and business complexities. A need exists in the art for a module, including a mobile phone, and a MNO to securely and efficiently support a change in network access credentials, including a key K for the module connecting to the MNO, without requiring a physical replacement of a UICC or equivalent physical media recording a key K.

And other needs exist in the art as well, as the list recited above is not meant to be exhaustive but rather illustrative.

SUMMARY

Methods and systems are provided for secure and efficient communication using a module to communicate with a server and a mobile operator network. The module can support "Machine to Machine" (M2M) communications, also known as "the Internet of things". The methods and systems contemplated herein can also support other applications as well, including mobile phone handsets connecting to a wireless network, where the wireless network can be associated with or the radio access portion of a mobile network operator. 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. An objective of the invention is to address the challenges noted above for securing the deployment of modules that can utilize an embedded universal integrated circuit card (eUICC) and/or also PKI algorithms and keys.

Petitioner Samsung Ex-1004, 0021

The methods and systems contemplated herein can reduce the need for manual intervention with a module in order to automatically and remotely change network access credentials in order for the module to utilize new or different keys in order to connect and authenticate with a wireless network. By using an eUICC, where the eUICC can support both (i) the authentication of a user by the MNO, and (ii) the secure decryption or derivation of the key K under control of the MNO, the value and usefulness of modules can be increased for a user and a mobile operator network. An eUICC can also comprise software and/or firmware components to "virtualize" the operation of a physical UICC, such that (i) the data normally recorded in a physical UICC can be recorded in a file with encryption, and (ii) the steps for using the data in the file can be processed by an eUICC.

In a first embodiment, a mobile network operator can process a set of data for inclusion in a profile for an eUICC. Data within the profile can be equivalent or similar to the data recorded in a physical UICC, including a set of network parameters, a module network identity, and a first key K. The mobile network operator can send the data for a profile to an eUICC subscription manager. A module can include an embedded universal integrated circuit card (eUICC). The eUICC can be processed by an operating system on the module and can be recorded in a nonvolatile memory, such that the eUICC is available after a powered off state. The eUICC can include data such as an eUICC identity, an eUICC profile key, and a symmetric ciphering algorithm. A manufacturer or distributor could record the data for the eUICC before the module is received by a user. The eUICC can communicate in the module with a network application. The network application can communicate with the mobile network operator using a wireless network and a radio within the module. The module can connect with a first network, send the eUICC identity and receive an encrypted profile, and the module can record the encrypted profile in a nonvolatile memory associated with the eUICC. The first network can be a network different than the wireless network for the profile, and the first network could comprise a WiFi network, a LAN connection using a USB interface to the module, or a public land mobile network.

Continuing with this first embodiment, the encrypted profile as received by the module can include a first portion of ciphertext and a second portion of ciphertext. The module using the eUICC can decrypt the first portion of ciphertext using the eUICC profile key and the symmetric ciphering algorithm. The resulting plaintext from the decrypted first portion of ciphertext can include the set of network parameters, the first network module identity, and the first key K. The module using the eUICC can select and activate the profile in order to connect with the wireless network associated with the mobile network operator. The module can conduct a first authentication with the mobile network operator using the first network module identity and the first key K. The module can send an attach request message, including an exemplary radio resource request message with the first network module identity, and the module can receive a random number in the form of a first RAND value.

Continuing with this first embodiment, the module can forward the RAND to the eUICC with the activated profile. The eUICC can input the first RAND and the first key K into a cryptographic algorithm in order to output a response RES value. The eUICC can return the RES value to the module, and the module could forward the RES to the wireless network. The wireless network can compare the received RES with a stored, expected RES (previously calculated using the same first RAND and first key K), and if the two RES values match then the module with the eUICC and profile can be authenticated by the network. The network and the module can take additional steps for the module to have at least limited access to an IP network. With access to the IP network for the module, a user associated with the module can conduct an authentication with the mobile network operator (whereas the mobile network operator may not have control over distribution of the profile with the network access credentials including the first key K up to this point).

Continuing with this first embodiment, the mobile network operator can authenticate or verify a user or M2M service provider associated with the module. The authentication or verification could comprise steps to verify a user, including the user entering information in a web page through the IP connection established with the network in the paragraph above using the first key K. Or the user could place a telephone call to a call center, and the user could verbally confirm identification information or enter DTMF digits. Or, the MNO could authenticate or verify the identity of a user associated with the module by a representative of the MNO visually viewing physical identification of the user such as a drivers license or a passport. If the module is associated with or operated by an M2M service provider, then the MNO could exchange data with the M2M service provider in order to confirm the module with the first key K is authenticated. In either case, where the module is associated with a user or an M2M service provider, the MNO could take steps to authenticate with a second factor, where authentication with the first factor comprised receiving the RES. After successful authentication with the second factor, the MNO can confirm the identity of an entity associated with the module, whereas that identity may not be known before the authentication with the second factor since the distribution of the eUICC profile may be outside the control of the mobile network operator.

Continuing with this first embodiment, after successful authentication with the second factor, the mobile network operator can send a symmetric key to the module. The symmetric key can be encrypted with a key ciphering algorithm. Or, the symmetric key can be (i) plaintext at the application layer, and (ii) encrypted at the data-link layer using the encryption between the module and wireless network after the first authentication above with the first key K. The module can receive the symmetric key (and decrypt the symmetric key if encrypted), and subsequently decrypt the second portion of ciphertext in the eUICC profile. The second portion of ciphertext can include a second network module identity and a second key K. The module can convert the second portion of ciphertext into plaintext using the symmetric ciphering algorithm and the received symmetric key. Note that the decryption of the second portion of ciphertext in the profile without the symmetric key is not feasible, and thus the mobile network operator can retain control over the use of the second key K in the profile for the eUICC, such as not releasing the symmetric key until after a user has successfully completed authentication with the mobile network operator as contemplated in the paragraph above.

After decrypting the second portion of ciphertext, the module with the eUICC can read a plaintext second network module identity and second key K. The second key K can be recorded in a protected, nonvolatile memory. The module can disconnect from the wireless network (where the first session used the first key K), and reconnect with the wireless network using the second network module identity and the second key K. The module with the eUICC can conduct a

Petitioner Samsung Ex-1004, 0022

second authentication using the second key K, including sending the second network module identity, receiving a second RAND value, calculating a second RES value using the second RAND and the second key K, and sending the second RES value. After a successful second authentication, the module can access the IP network and the public Internet through the wireless network, and subsequent authentications with the wireless network can continue to use the second network module identity and the second key K. For embodiments where the module comprises a mobile phone and the user is an individual subscribing to mobile phone services from the mobile network operator, the user can be associated with a telephone number and place/receive phone calls after a successful second authentication.

In another embodiment, the eUICC profile key, associated with decrypting the profile from the eUICC subscription manager, may not be recorded in the eUICC before the eUICC sends an eUICC identity to the module, where the module sends the eUICC identity to the eUICC subscription manager through a first network. The eUICC can record an eUICC private key and the eUICC subscription manager could record an eUICC public key. The eUICC subscription manager can (i) encrypt the profile with the eUICC profile key, and then (ii) encrypt the eUICC profile key with an asymmetric ciphering algorithm and the eUICC public key, where the output is an encrypted eUICC profile key. The eUICC can receive the encrypted eUICC profile key from the eUICC subscription manager and decrypt the encrypted eUICC key using the asymmetric ciphering algorithm and the eUICC private key. After reading the plaintext eUICC profile key, the eUICC can decrypt the encrypted profile using the plaintext eUICC profile key, in order to read a plaintext first key K and first network module identity.

In an exemplary embodiment, the first key K is a null value for a profile recorded in the eUICC in a module. The use of a null value or the number zero for a shared secret key K is contemplated in wireless WAN standards and supported by commercial wireless networks in order to support emergency services for a module without a valid UICC. With a null value for the first key K, the MNO and wireless network can provide limited access to the IP network, such that a user of the module with a null or zero value for the first key K could perform steps to authenticate or verify the user with the MNO through the IP network accesses with the first key K as a null value. The data-link layer may not be effectively ciphered due to the use of a null value for the first key K, but the application or transport layer could secure communication from a web browser on the module to a web server for the user to authenticate with the MNO. The secure communication between the web browser and web server can utilize transport layer security (TLS) or similar standards for security at the transport or application layer, even though the data-link or network layer may not be encrypted. After successful authentication via the web browser, the MNO can take steps (discussed in other embodiments) allowing the module with the eUICC to access and use a second key K and a second network module identity for subsequent secured communication between the module and the MNO.

In another embodiment, the second key K can be derived using by both the mobile network operator and the module with the eUICC using a key derivation algorithm. The eUICC could include an eUICC key exchange algorithm and the mobile network operator could include a MNO key exchange algorithm, and the key exchange algorithms can include a key derivation algorithm that accepts input of a token value, a private key, and a public key for the other node. The mobile network operator and the module with the eUICC could communicate the token value used for the key derivation algorithm (including using the connectivity through the wireless network after using the first key K in the profile). The module can record an eUICC private key, and the MNO can have access to the eUICC public key. The key derivation algorithm in the eUICC key exchange algorithm can output a second key K using the token. The MNO can obtain the same value for the second key K. In this manner, both node can derive the same second key K without electronically transferring the second key K, even in encrypted form and thereby increasing the security of a systems with an eUICC.

In an exemplary embodiment can support a module changing a key K used to (i) authenticate with a wireless network and (i) cipher/decipher data with a wireless network. The module can change key K without requiring the manual exchange of a UICC or other physical intervention. The module can use an eUICC profile and change key K while using the same eUICC profile. The module, could also comprise a mobile phone such as, but not limited to, a smart phone. After connecting with a first network, which could comprise a first wireless WAN, wireless LAN, or wired connection, the module can receive a eUICC profile for an eUICC in the module, where the eUICC profile includes a first network module identity and a first key K. The first key K can be a standards-based key K used with wireless networks, and be equivalent to a pre-shared secret key K recorded in physical UICCs for LTE networks.

After authenticating with the wireless network using the first key K, the module and MNO can share a token. The module and MNO can mutually derive a second key K using the token and a key derivation algorithm. The module can disconnect from the wireless network after attaching using the first key K, and then reconnect using the second key K which has now been mutually derived by both the module and the mobile network operator. The module or MNO could determine or evaluate if the use of a new key K is required or preferred, and share a new token for input into the key derivation algorithms to derive a mutually shared new key K. In this manner, a module can change the key K used to authenticate and cipher/decipher data with a wireless network from a first key K to a second key K. This can increase flexibility of the system and reduce costs of physically distributing a new UICC to the module (or electronically sending new eUICC profiles) in order to change a key K.

These as well as other aspects and advantages will become apparent to those of ordinary skill in the art by reading the following detailed description, with reference where appropriate to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Various exemplary embodiments are described herein with reference to the following drawings, wherein like numerals denote like entities.

FIG. **1***a* is a graphical illustration of an exemplary system that includes a module and a mobile network operator, in accordance with exemplary embodiments;

FIG. **1***b* is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments;

FIG. **1***c* is a graphical illustration of components within a module, in accordance with exemplary embodiments;

FIG. **1***d* is a graphical illustration for authenticating with a wireless network using a physical UICC, in accordance with conventional technology;

Petitioner Samsung Ex-1004, 0023

FIG. **1***e* is a graphical illustration for authenticating with a wireless network using an eUICC, in accordance with exemplary embodiments;

FIG. **1***f* is a graphical illustration of an exemplary system that includes a module, a mobile network operator, and an eUICC in accordance with exemplary embodiments;

FIG. **2***a* is a graphical illustration of an exemplary profile for an eUICC, including encrypted data, decryption steps, and decrypted data for the profile, in accordance with exemplary embodiments;

FIG. **2***b* is a graphical illustration for ciphering and deciphering a profile using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments;

FIG. **2***c* is a graphical illustration for ciphering and deciphering a key K using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments;

FIG. **2***d* is a graphical illustration of a public key and a private key for an eUICC, in accordance with exemplary embodiments;

FIG. **2***e* is a graphical illustration for ciphering and deciphering a key for an eUICC using an asymmetric ciphering algorithm using a PKI key pair, in accordance with exemplary embodiments;

FIG. **3** is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments;

FIG. **4** is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments;

FIG. **5***a* is a graphical illustration of a public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments;

FIG. **5***b* is a graphical illustration of deriving a second key K using public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments;

FIG. **5***c* is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments; and,

FIG. **6** is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS OF THE INVENTION

FIG. **1***a*

FIG. **1***a* is a graphical illustration of an exemplary system that includes a module and a mobile network operator, in accordance with exemplary embodiments. The system **100** includes a module **101** operating within a wireless network **102**. System **100** can also include a mobile network operator **104**, an IP Network **111**, and an eUICC subscription manager **109**. Mobile network operator (MNO) **104** can include a server **105**. For embodiments where the MNO **104** uses 4G LTE and LTE Advanced networks, server **105** could comprise a home subscriber server (HSS) and/or a mobility management entity (MME). Server **105** could be a server with related functionality as a HSS or MME for a MNO **104** that uses different wireless network standards than those based on 4G LTE. Although not illustrated in FIG. **1***a*, an eUICC subscription manager **109** may also include one or more servers **105**, such that a first server **105** could function as an HSS in 4G LTE and LTE Advanced networks and a second server **105** could function as a MME in 4G LTE and LTE Advanced networks.

System **100** is illustrated without specific packet transmissions between module **101** and mobile network operator **104** and eUICC subscription manager **109**. Examples of the communications and messages pertaining to the present invention will be illustrated in later Figures. As contemplated herein, machine-to-machine communications may comprise communication between a module **101** and a server **105**, such that data can be transferred between the two with minimal manual intervention, although manual intervention can be required to set up system **100** and any occasional manual maintenance required. As contemplated herein, machine-to-machine communications may also be referred to as "the Internet of things" (IoT). Also note that module **101** may comprise a wireless module, such that module **101** can communicate with wireless network **102** using a radio and an antenna. A wireless or a wired configuration for module **101** can be utilized in the present invention.

If module **101** operates as a wireless module, module **101** and wireless network **102** can communicate using a base station **103**. Module **101** and wireless network **102** can utilize a variety of wireless technologies to communicate, including WiFi, WiMax, a 2nd generation wireless wide area network (WAN) technology such as, but not limited to, General Packet Radio Services (GPRS) or Enhanced Data rates for GSM Evolution (EDGE), 3rd Generation Partnership Project (3GPP) technology such as, but not limited to, 3G, 4G LTE, or 4G LTE Advanced, and other examples exist as well including wireless networks based on WiMAX standards. A wired module **101** can connect to the IP Network **111** via a wired connection such as, but not limited to, an Ethernet, a fiber optic, or a Universal Serial Bus (USB) connection (not shown).

Generally, the communication techniques described herein can be independent of the network technologies utilized at the physical and data-link layers, so long as the underlying network provides access to the IP Network **111** and supports Internet Protocols (IP). The IP Network **111** can be an IPV4 or an IPV6 packet-switched based network that utilizes standards derived from the Internet Engineering Task Force, such as, but not limited to, RFC 786 (User Datagram Protocol), RFC 793 (Transmission Control Protocol), and related protocols. The IP Network **111** can be the public Internet comprising globally routable IP addresses, or a private network that utilizes private IP addresses. IP Network **111** as illustrated in FIG. **1***a* could comprise the globally routable public Internet, or IP Network **111** could also be a private Internet that is (i) not globally routable and (ii) only accessible to authorized modules and servers. As one example of a private IP Network **111**, IP Network **111** could use private IP addresses for nodes on the network, and in this case IP Network **107** could be referred to as an intranet or private network. Alternatively, IP Network **111** could be a private network layered on top of the publicly routable Internet via secured and encrypted connections. The specific numbers for IP addresses and port numbers shown in FIG. **1***a* and other figures are illustrative and any valid IP address or port number can be used, including an IPV4 and an IPV6 address. Server **105** within mobile network operator **104** can communicate with the module **101** using IP network **111**, where IP network **111** can comprise a private network that utilizes Internet Protocol standards. Module **101** can access the public Internet after authenticating with the server **105** associated with the MNO **104**.

Petitioner Samsung Ex-1004, 0024

When operating in a wireless network configuration, module **101** can access the IP Network **111** via the wireless network **102**. In the wireless network configuration, 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**. Examples of wireless modules that utilize a wireless WAN such as, but not limited to, 2G and 3G networking technologies include the Motorola® G24-1 and Huawei® MC323. Example manufacturers of wireless modules in 2012 include Sierra Wireless® and Telit®. Example leading manufacturers of mobile phones in 2013 include Apple® and Samsung®. In a wired configuration (not shown), module **101** can be a computer, security camera, security monitoring device, networked controller, etc. Module **101** can include a module identity **110**, which can comprise a serial number or identity code in order to identify an individual, specific module **101** among a plurality of modules **101**. A more detailed depiction of exemplary components of a module **101** is included in FIG. **1***b* and FIG. **1***c* below. Module **101** could also operate as a "smartcard" such that an end user presents module **101** to merchants for payments.

Wireless network **102** may comprise either a wireless local area network (LAN) or a wireless WAN such as a public land mobile network (PLMN). Examples for technologies used in wireless LANs include an 802.11 WLAN, Bluetooth, or Zigbee among other possibilities. Module **101** operating in wireless mode could communicate with a base station **103** of a wireless network **102** using a radio and an antenna. Wireless network **102** could operate as a Mode II device according to FCC Memorandum Opinion and Order (FC-12-36) and related white space regulation documents. If module **101** supports IEEE 802.15.4, then wireless network **102** could be a Zigbee network, an ISA100.11a standards-based network, or a 6LoWPAN network as described by IETF RFC 4944. Other possibilities exist as well for the wireless technology utilized by a wireless network **102** and module **101**, operating in a wireless mode, without departing from the scope of the present invention.

System **100** can include an eUICC subscription manager **109**, where an eUICC subscription manager **109** can manage the recording and secure distribution of eUICC profiles **107***c* to a module **101**. Example entities that could operate or control an eUICC subscription manager **109** include a manufacturer of module **101**, an M2M service provider that manages the operation of module **101**, or possibly a mobile network operator **104** could operate the eUICC subscription manager **109**. Other entities could operate as an eUICC subscription manager **109** as well. An exemplary eUICC subscription manager **109** is described in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. An eUICC subscription manager **109** can also use a server **105** and record private keys and public keys for the server/subscription manager operation (including exemplary keys depicted and described in connection with FIG. **2***d* below).

In exemplary embodiments, eUICC subscription manager **109** can use an eUICC profile key **107***b* to cipher portions of an eUICC profile **107***c*, such that only module **101** with the same eUICC profile key **107***b* could reasonably decipher the portions of the eUICC profile **107***c*. In this manner, the eUICC profile **107***c* can remain reasonably secured. The eUICC subscription manager **109** can share the eUICC profile key **107***b* in several different ways, including (i) pre-sharing the eUICC profile key **107***b*, or (ii) the eUICC subscription manager **109** sending the eUICC profile key **107***b* to the eUICC **107** using an asymmetric ciphering algorithm **219** as depicted and described in connection with FIG. **2***e* below. An eUICC profile **107***c* can include an eUICC profile identity **107***e* in order to identify a profile among a plurality of eUICC profiles **107***c*. An eUICC subscription manager **109** can include an address **109***a*. The address **109***a* could comprise a domain name, such that a domain name system (DNS) or secure DNS (DNSSEC) query could resolve the name into an IP address in order for module **101** to communicate with the eUICC subscription manager **109**. Or the address **109***a* could comprise an Internet Protocol (IP) address, and the address **109***a* could include or be associated with a port number, such as port number **443** for data that utilizes transport layer security.

An eUICC **107** within module **101** can comprise an embedded universal integrated circuit card (eUICC) **107**. An eUICC **107** can provide the equivalent functionality as a physical UICC, where definitions for a physical UICC are included in ETSI TR 102 216 and ETSI TS 102 221 V11.0.0, and other examples for the use of a physical UICC in mobile phones and M2M modules exist as well. An eUICC **107** in FIG. **1***a* can support exemplary requirements for an eUICC outlined in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. In other words, an eUICC **107** can operate as a "virtualized" UICC, such that data operations and input/output to a physical UICC can be provided by an eUICC **107**. Exemplary details of a conventional, physical UICC for authenticating a module **101** (which can be "virtualized in an eUICC **107**) are depicted and described in connection with FIG. **1***d* below. An eUICC **107** can include an eUICC identity **107***a*, such that an eUICC subscription manager **109** can select and identify the eUICC **107** among a plurality of eUICCs **107**. The eUICC **107** can also record an eUICC profile key **107***b* and an eUICC profile **107***d*. Profile **107***d* can represent a profile that is partially decrypted using the eUICC profile key **107***b*, as depicted and described in connection with FIG. **2***a* below. Additional exemplary details for the operation of an eUICC **107** within module **101** are also provided in FIG. **1***b*, FIG. **1***c*, FIG. **1***e*, and FIG. **1***f* below.

According to an exemplary embodiment, an eUICC **107** can be recorded and operate within a "eUICC supporting" physical universal integrated circuit card (UICC) **108** within module **101**. This "eUICC supporting", physical UICC **108** can include a processing unit, RAM memory, ROM memory, EEPROM memory, a bus, and a physical interface (not shown in FIG. **1***a*, but described in FIG. **1***b*). An exemplary processing unit, RAM memory, ROM memory, EEPROM memory, and bus are depicted and described in connection with FIG. **1***b* below. The physical interface for an UICC **108** is depicted and described in connection with FIG. **1***d* below. The "eUICC supporting" physically UICC **108** can perform all of the functions of an eUICC **107**, including (i) receiving and recording profiles **107***d*, (ii) receiving and recording eUICC profile keys **107***b*, (iii) recording an eUICC identity **107***e*, (iv) decrypting an eUICC profile **107***c* into an eUICC profile **107***d* as depicted and described in connection with FIG. **2***a* below, (v) recording a set of network parameters **201** (in FIG. **2***a* below) for module **101** to connect with wireless network **102**, and (vi) recording keys such as a key K for conducting a message digest authentication with wireless network as depicted and described in FIG. **1***d*, FIG. **1***e*, and FIG. **3** below. An "eUICC supporting" physical UICC **108** can include a physical electrical interface of ISO/IEC 7816-3 in order to support

Petitioner Samsung Ex-1004, 0025

existing physical slots for UICCs. The use of an "eUICC supporting" physical UICC **108** is optional, and can be omitted. In this case (where "eUICC supporting" physical UICC **108** is omitted), the eUICC **107** can operate as a program within module **101** as depicted and described in connection with FIG. **1***b* below, and the eUICC **107** would not reside within the "eUICC supporting" physical UICC **108**.

The physical form-factor for an "eUICC supporting" UICC **108** could be identical to a UICC, and a difference between the two may not even be apparent upon visual inspection without special markings on the card. The physical form-factor for an "eUICC supporting" UICC **108** could comprise a "micro-SIM" or a "nano-SIM" as defined in ETSI TS 102 221 V11.0.0, which is herein incorporated by reference. When the module **101** detects a "eUICC supporting" UICC **107**, the module **101** could send received eUICC profiles **107***c* to the "eUICC supporting" UICC **107**, and also select, deselect, activate, and deactivate the different received eUICC profiles **107***d* recorded in the "eUICC supporting" UICC **108**. When a module **101** detects that a regular UICC (i.e. not an "eUICC supporting" UICC **108**) has been loaded into a slot for UICCs within the module, the module **101** could access the UICC in a regular manner implemented by mobile phones and modules for connecting to existing wireless networks in 2013, such as LTE or 3G networks. This use of conventional technology for a physical UICC is depicted and described in connection with FIG. **1***d* below.

A module **101** can be associated with a user **113** or an M2M service provider **115**. A user **113** could be a subscriber to mobile phone services provided by the mobile network operator **104**. In this case, the user could be an individual and the module **101** could comprise a mobile phone with a telephone number, an email client, and a web browser (in addition to other, standard functionality for a mobile phone). The user **113** could periodically charge the module **101** (which can comprise a mobile phone), such as typically at night and carry the module **101** during the day in order to place calls and send/receive data. Thus, the user **113** may typically be physically close to a mobile phone as module **101**, but an M2M service provider **115** can be associated with module **101** but may not be physically close to module **101**. For embodiments where module **101** is associated with M2M communications, such as including a sensor to collect data regarding a monitored unit, the module **101** can be associated with an M2M service provider **115**. In this case, the M2M service provider **115** can be a company or a division or department within a larger company that is associated with a plurality of modules **101** for collecting data using sensors and sending the data to a server similar to server **105**. The M2M service provider **115** may operate the server similar to server **105** in order to automatically collect data from the plurality of modules **101**. The server for the M2M service provider **115** could communicate with module **101** using the IP network **111** and the wireless network **102** when module **101** is connected to the wireless network **102**.

Other configurations besides the one illustrated in FIG. **1***a* are possible as well. In many common commercial relationships for the operation of mobile phone service in the United States in 2013, wireless network **102** could represent a portion of the radio access network used by a mobile network operator **104**. MNO **104** could outsource portions of the operation and maintenance of a radio access network, such as a wireless network **102**, to 3rd parties. In this configuration, wireless network **102** could represent a network operated by a first company specializing in the operation of radio towers and BTS equipment. This first company could be contracted with the mobile network operator **104** in order to support mobile phone service or data services to modules **101**.

In addition, server **105** could reside within wireless network **102** in a data center managed by wireless network **102**. Wireless network **102** could also operate as an eUICC subscription manager **109**. Although a single module **101**, server **105**, wireless network **102**, and mobile network operator **104** are illustrated in FIG. **1***a*, system **100** could comprise a plurality of each of these elements. Module **101** could also record sensor data pertaining to a monitored unit (not shown). Module **101** could be mobile, such as physically attached to a truck or a pallet, and module **101** could connect to a series of different wireless networks **102** or base stations **103** as module **101** moves geographically. Other configurations are possible as well for the elements illustrated in FIG. **1***a* without departing from the scope of the present invention.

FIG. **1***b*

FIG. **1***b* is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments. FIG. **1***b* is illustrated to include many components that can be common within a module **101**, and module **101** may also operate in a wireless configuration in order to connect with a wireless network **102**. In a wireless configuration, the physical interface **101***a* of module **101** may support radio-frequency (RF) communications with networks including a wireless network **102** via standards such as, but not limited to, GSM, UMTS, mobile WiMax, CDMA, LTE, LTE Advanced, and/or other mobile-network technologies. In a wireless configuration, the physical interface **101***a* may also provide connectivity to local networks such as, but not limited to, 802.11 WLAN, Bluetooth, or Zigbee among other possibilities. In a wireless configuration, module **101** could use a physical interface **101***a* be connected with both a wireless WAN and wireless LAN simultaneously. In a wired configuration, the physical interface **101***a* can provide connectivity to a wired network such as, but not limited to, through an Ethernet connection or USB connection. As contemplated herein, a physical interface **101***a* can include a network interface (such as a radio or an Ethernet port), such that module **101** can use the network interface in order to connect with a network and communicate with the network. A network interface can also comprise a physical interface **101***a* as contemplated herein.

The physical interface **101***a* can include associated hardware to provide the connections such as, but not limited to, radio-frequency (RF) chipsets, a power amplifier, an antenna, cable connectors, etc., and additional exemplary details regarding these components are described below in FIG. **1***c*. Device driver **101***g* can communicate with the physical interfaces **101***a*, providing hardware access to higher-level functions on module **101**. Device drivers **101***g* may also be embedded into hardware or combined with the physical interfaces **101***a*. Module **101** may preferably include an operating system **101***h* to manage device drivers **101***g* and hardware resources within module **101**. The operating systems described herein can also manage other resources such as, but not limited to, memory and may support multiple software programs operating on module **101** at the same time.

The operating system **101***h* can include Internet protocol stacks such as, but not limited to, a User Datagram Protocol (UDP) stack, Transmission Control Protocol (TCP) stack, a domain name system (DNS) stack, etc., and the operating system **101***h* may include timers and schedulers for manag-

Petitioner Samsung Ex-1004, 0026

ing the access of software to hardware resources. The operating system shown of **101***h* can be appropriate for a low-power device with limited memory and CPU resources (compared to a server **105**). An example operating system **101***h* for module **101** includes Linux, Android® from Google®, Windows® Mobile, or Open AT® from Sierra Wireless®. Additional example operating systems **101***h* for module **101** include eCos, uC/OS, LiteOs, and Contiki, and other possibilities exist as well without departing from the scope of the present invention.

A module program **101***i* may be an application programmed in a language such as, but not limited to, C, C++, Java, and/or Python, and could provide functionality to support regular mobile phone functionality. The module program **101***i* could include a network application **101***x*, where network application **101***x* comprises the user equipment protocol for accessing and communicating with the wireless network **102**. For embodiments where module **101** connects with a wireless network **102** comprising an LTE network, the network application **101***x* can receive, process, and send signals with the wireless network **102** for user equipment messages in ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification", which is herein incorporated by reference. In other words, network application **101***x* can comprise software for accessing and communicating with the wireless network **102**. Although network application **101***x* is depicted in FIG. **1***b* as operating as software within RAM memory **101***e*, the network application **101***x* could be included in firmware or a processor or application associated with a radio **101***z* (described in FIG. **1***c*). Exemplary messages sent and received by a network application **101***x* are also depicted and described in connection with FIG. **3** below.

A module program **101***i* could also include software for M2M applications such as, but not limited to, remote monitoring of sensors and remote activation of actuators. Module program **101***i* could also include a software routine, subroutine, linked library, or software module, according to one preferred embodiment. As contemplated herein, a module program **101***i* can include an application operating within a smartphone, such as, but not limited to, an iPhone® or Android®-based smartphone, and in this case module **101** could comprise a smartphone. The application functioning as a module program **101***i* could be downloaded from an "app store" associated with the smartphone. A set of device drivers **101***g* could include an eUICC driver **129**, such that a network application **101***x* or other software or firmware within module **101** communicating with the eUICC **107** could send and receive data with the eUICC driver **129**. Additional details regarding an exemplary eUICC driver **129** are depicted and described in connection with FIG. **1***e* below.

Many of the logical steps for operation of module **101** or eUICC **107** can be performed in software and hardware by various combinations of physical interface **101***a*, device driver **101***g*, operating system **101***h*, and a module program **101***i*. As depicted in FIG. **1***b*, module program **101***i* can include an eUICC **107** and a network application **101***x*. When module **101** or eUICC **107** is described herein as performing various actions such as acquiring an IP address, connecting to the wireless network, monitoring a port, transmitting a packet, sending a message, receiving a response, or encrypting or signing data, specifying herein that module **101** or eUICC **107** performs an action can refer to software, hardware, and/or firmware operating within module **101** illustrated in FIG. **1***b* or FIG. **1***c* performing the action.

Note that module **101** may also optionally include user interface **101***j* which may include one or more devices for receiving inputs and/or one or more devices for conveying outputs. User interfaces are known in the art and thus user interfaces are not described in detail here. User interface **101***j* could comprise a touch screen if module **101** operates as a smartphone or mobile phone. For embodiments where module **101** comprises a module for M2M applications and is associated with an M2M service provider **115**, then module **101** can optionally omit a user interface **101***j*, since no local user **113** input may be required for many M2M applications, although a user interface **101***j* could be included with module **101**. For embodiments where module **101** comprises a mobile phone and is associated with a user **113**, the user interface **101***j* could comprise a touch screen on the front of a mobile phone.

Module **101** may be a computing device that includes computer components for the purposes of collecting data from a sensor **101***f* or triggering an action by an actuator **101***y*. Module **101** may include a central processing unit (CPU) **101***b*, a random access memory (RAM) **101***e*, and a system bus **101***d* that couples various system components including the random access memory **101***e* to the processing unit **101***b*. The system bus **101***d* may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures including a data bus. Note that the computer components illustrated for the module **101** in FIG. **1***b* may be selected in order to minimize power consumption and thereby maximize battery life, if module **101** includes a battery and is not attached to external power. In addition, the computer components illustrated for the module **101** in FIG. **1***b* may also be selected in order to optimize the system for both long periods of sleep or idle states relative to active communications and also may be optimized for predominantly uplink (i.e. device to network) communications with small packets or messages. The computer components illustrated for the module **101** in FIG. **1***b* may also be general-purpose computing components, and specialized components may not be required in order to utilize many of the embodiments contemplated herein.

Module **101** may include a read-only memory (ROM) **101***c* which can contain a boot loader program. Although ROM **101***c* is illustrated as "read-only memory", ROM **101***c* could comprise long-term memory storage chipsets or physical units that are designed for writing once and reading many times. As contemplated within the present invention, a read-only address could comprise a ROM **101***c* memory address or another hardware address for read-only operations accessible via bus **101***d*. Changing data recorded in a ROM **101***c* can require a technician have physical access to module **101**, such as, but not limited to, removing a cover or part of an enclosure, where the technician can subsequently connect equipment to a circuit board in module **101**, including replacing ROM **101***c*. ROM **101***c* could also comprise a nonvolatile memory, such that data is stored within ROM **101***c* even if no electrical power is provided to ROM **101***c*. Although not illustrated in FIG. **1***b*, but illustrated in FIG. **1***c* below, module **101** could also include a flash memory **101***w*. Module program **101***i*, network application **101***x*, operating system **101***h*, eUICC **107**, or device drivers **101***g* could be stored in flash memory **101***w* within module **101** when the module is powered off. These components and/or instructions could be moved from a flash memory **101***w* (not shown

Petitioner Samsung Ex-1004, 0027

in FIG. **1***b* but shown in FIG. **1***c*) into RAM **101***e* when the module is powered on by a bootloader program recorded in the ROM **101***c*. Note that ROM **101***c* could be optionally omitted or included in a memory unit within CPU **101***b* (not shown).

Although the exemplary environment described herein employs ROM **101***c* and RAM **101***e*, it should be appreciated by those skilled in the art that other types of computer readable media which can store data that is accessible by a module **101**, such as, but not limited to, memory cards, subscriber identity module (SIM) cards, local miniaturized hard disks, and the like, may also be used in the exemplary operating environment without departing from the scope of the invention. The memory and associated hardware illustrated in FIG. **1***b* provide nonvolatile storage of computer-executable instructions, data structures, program modules, module program **101***i*, and other data for computer or module **101**. Note the module **101** may include a physical data connection at the physical interface **101***a* such as, but not limited to, a miniaturized universal serial bus adapter **101***v* (illustrated in FIG. **1***c*), firewire, optical, or other another port.

The computer executable instructions such as, but not limited to, module program **101***i*, network application **101***x*, eUICC **107**, operating system **101***h*, or device driver **101***g* can be initially loaded into memory such as, but not limited to, ROM **101***c* or RAM **101***e* through the physical interface **101***a* before module **101** is given to an end user, shipped by a manufacturer to a distribution channel, or installed by a technician. In addition, the computer executable instructions such as, but not limited to, module program **101***i*, network application **101***x*, operating system **101***h* or device driver **101***g* could be transferred wirelessly to module **101**. In either case (wired or wireless transfer of computer executable instructions), the computer executable instructions such as module program **101***i*, network application **101***x*, operating system **101***h*, or device driver **101***g* could be stored remotely on a disk drive, solid state drive, or optical disk (external drives not shown).

A number of program modules may be stored in RAM **101***e*, ROM **101***c*, or possibly within CPU **101***b*, including an operating system **101***h*, device driver **101***g*, an http client (not shown), a DNS client, and related software. Further, the module program **101***i* and/or network application **101***x* can perform the various actions described in the present invention for the module **101** through instructions the module program **101***i* and/or network application **101***x* provide to the CPU **101***b*. A user may enter commands and information into module **101** through an optional user interface **101***j*, such as a keypad, keyboard (possibly miniaturized for a mobile phone form-factor), and a pointing device. Pointing devices may include a trackball, an electronic pen, or a touch screen.

The module **101**, comprising a computer, may operate in a networked environment using logical connections to one or more remote computers, such as the server **105** illustrated in FIG. **1***a*. Server **105** can also function as a general purpose server to provide files, programs, disk storage, remote memory, and other resources to module **101** usually through a networked connection. Additional remote computers with which module **101** communicates may include another module **101** or mobile device, an M2M node within a capillary network, a personal computer, other servers, a client, a router, a network PC, a peer device, a base station **103**, or other common network node. It will be appreciated that the network connections shown throughout the present invention are exemplary and other means of establishing a wireless or wired communications link may be used between mobile devices, computers, servers, corresponding nodes, and similar computers. Although a single module program **101***i* is depicted in FIG. **1***b*, module **101** could include a plurality of module programs **101***i*.

The module program **101***i*, eUICC **107**, and network application **101***x* operating within module **101** illustrated in FIG. **1***b* can provide computer executable instructions to hardware such as CPU **101***b* through a system bus **101***d* in order for a module **101** to (i) connect with a wireless network **102**, (ii) authenticate with a mobile network operator **104** associated with the wireless network **102**, and (iii) send or receive packets with a server **105** or a server associated with an eUICC subscription manager **109**. The module program **101***i* and/or network application **101***x* can enable the module **101** or eUICC **107** to transmit or send data from the eUICC **107** or module **101**. The eUICC **107** or module **101** can send data by recording data in memory such as RAM **101***e*, where the data can include cryptographic data such as a RAND and RES values, a destination IP:port number, a packet or packet header value, an encryption or ciphering algorithm and key, a digital signature algorithm and key, etc. The data recorded in RAM **101***e* can be subsequently read by the operating system **101***h* or the device driver **101***g*. The operating system **101***h* or the device driver **101***g* can write the data to a physical interface **101***a* using a system bus **101***d* in order to use a physical interface **101***a* to send data to the wireless network **102** and IP network **111** using a radio **101***z* (shown in FIG. **1***c*). Alternatively, the module program **101***i* and/or network application **101***x* can write the data directly to the physical interface **101***a* using the system bus **101***d*.

The module program **101***i*, eUICC **107**, network application **101***x*, and/or operating system **101***h* can include steps to process the data recorded in memory such as, but not limited to, encrypting data, selecting a destination address, or decrypting ciphertext data. The data recorded in memory could also include an eUICC profile **107***c* or eUICC profile **107***d*, as described in FIG. **1***a* above and FIG. **2***a* below. The eUICC profiles **107***d* can include instructions and data for connecting with wireless network **102**, including network parameters and network access credentials. The module **101** can use the physical interface **101***a* such as, but not limited to, a radio to transmit or send the data associated with a profile **107***d* to a base station **103**. For those skilled in the art, other steps are possible as well for a module program **101***i* or operating system **101***h* to communicate with a wireless network **102** using data associated with an UICC (where an eUICC **107** records data normally associated with a physical UICC) without departing from the scope of the present invention.

Conversely, in order for module **101**, network application **101***x*, or eUICC **107** to receive a packet or message from MNO **104** or wireless network **102**, the physical interface **101***a* can use a radio to receive data from a base station **103**. The received data can include information from MNO **104** and may comprise a datagram, a source IP:port number, a packet or header value, an instruction for module **101**, an acknowledgement to a packet that module **101** sent, a digital signature, and/or encrypted data. The received data can also include radio resource control (RRC) messages, and related layer 1 and layer 2 access and control messages for module **101** to access the wireless network **102**. The operating system **101***h* or device driver **101***g* can use a system bus **101***d* and CPU **101***b* to record the received data in memory such as RAM **101***e*, and the module program **101***i* or operating system **101***h* may access the memory in order to

Petitioner Samsung Ex-1004, 0028

process the received data and determine the next step for the module **101** after receiving the data. The steps within this paragraph may also describe the steps a module program **101***i*, eUICC **107**, or network application **101***x* can perform in order to receive a message from wireless network **102** that includes a RAND value. For those skilled in the art, other steps are possible as well for a module program **101***i*, network application **101***x*, module **101**, and/or eUICC **107** to receive a message from a mobile network operator **104** or wireless network **102** within the scope of the present invention.

Module program **101***i* can include an eUICC **107**, which can provide the functionality or CPU **101***b* instructions for module **101** to access data normally within a physical UICC, such as network parameters and network access credentials. An eUICC **107** as illustrated in FIG. **1***a* and FIG. **1***b* can be implemented within module **101** in several different ways, including (i) as depicted in FIG. **1***b* a module program **101***i* stored in RAM **101***e* during operation, but also recorded in a nonvolatile memory, such as, but not limited to, either flash memory **101***w* (described in FIG. **1***c*) or ROM **101***c* at other times than normal operation (such as during periods of power off), (ii) firmware within CPU **101***b* or another specialized processing unit within module **101**, (iii) an "eUICC supporting" physical UICC **108** within module **101** that contains the eUICC **107**, or (iv) a specialized circuit within a surface mount package that is soldered directly onto a circuit board of the module **101**, including an 8-lead small outline non-leaded (SON-8) package. For the embodiment where an eUICC **107** comprises a module program **101***i*, the eUICC **107** could be loaded and installed within nonvolatile memory **101***w* in module **101** using the steps and procedures described for a module program **101***i* in FIG. **1***b*. Other possibilities exist as well for the physical implementation of an eUICC **107** within a module **101** without departing from the scope of the present invention. An eUICC **107** may also be referred to as an "electronic UICC", an "electronic SIM" (eSIM), or an "embedded SIM" (also eSIM).

For embodiments where an eUICC **107** can be loaded into a RAM **101***e* or flash **101***w* memory, a CPU **101***b* could designate the RAM **101***e* or flash **101***w* memory containing the instructions or data for an eUICC **107** to be a protected memory. When (i) loaded with appropriate data (such as, but not limited to a eUICC profile **107***d* described in FIG. **2***a* below), and (ii) a profile for a MNO **104** is selected and activated, then an eUICC **107** can provide the equivalent functionality of a physical UICC. The eUICC **107**, using an activated eUICC profile **107***d*, can provide the module **101** with (i) network access credentials **202** and **203**, and (ii) network parameters **201** in order to connect with wireless network **102**. The eUICC **107**, using an activated eUICC profile **107***d*, can record a first key K **203** (described in FIGS. **2***a* and **3** below) and also a first network module identity **202**. The eUICC **107** can support standard steps by module **101** for network authentication contemplated in 3GPP TS 33.401 V12.9.0 and related standards, including inputting a RAND value into the eUICC **107** and outputting a RES value.

Moreover, those skilled in the art will appreciate that the present invention may be implemented in other computer system configurations, including hand-held devices, netbooks, portable computers, multiprocessor systems, microprocessor based or programmable consumer electronics, network personal computers, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments, where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices. In addition, the terms "mobile node", "mobile station", "mobile device", "M2M module", "M2M device", "networked sensor", "industrial controller", or "user equipment" can also refer to module **101** or its functional capabilities. Other possibilities exist as well for the configuration or combination of components illustrated in FIG. **1***b* without departing from the scope of the present invention.

FIG. **1***c*

FIG. **1***c* is a graphical illustration of components within a module, in accordance with exemplary embodiments. FIG. **1***c* is illustrated to show a combination of components useful for leveraging the efficient and secure communication techniques described in the present invention. In addition to the components illustrated in FIG. **1***b* above, module **101** can include a an eUICC **107**, a battery **101***k*, a MNO public key **502**, a wireless module private key **112***a*, a connection to an actuator **101***y*, a USB interface **101***v*, a CPU wake controller **101***u*, a flash memory **101***w*, a symmetric key **127**, a random number generator **128**, cryptographic algorithms **141**, a radio **101***z*, and other components illustrated in FIG. **1***c*. Not all of the components illustrated in FIG. **1***c* are required for many exemplary embodiments, and some of the components illustrated in FIG. **1***c* may also be optionally omitted in some exemplary embodiments.

The CPU **101***b* can comprise a general purpose processor appropriate for the low power consumption requirements of a module **101**, and may also function as a microcontroller. CPU **101***b* could be a processor with an ARM® core, or possibly an ATOM® core or processors, and other possibilities exist as well. The CPU **101***b* can include registers, a cache memory, and arithmetic logic units. Clock **160** can comprise a crystal oscillator generating sine or square wave outputs at a frequency to drive a system bus **101***d*, CPU **101***b*, and RAM **101***e*, in addition to other functionality. In exemplary embodiments, clock **160** can comprise a temperature-compensated crystal oscillator (TCXO), a voltage-controlled crystal oscillator (VCXO), or a voltage-controlled temperature-compensated crystal oscillator (VCTCXO), and other possibilities exist as well. Clock **160** could include circuits and logic to keep time while module **101** is both in an active state and a dormant state.

Sensor **101***f* could be a device to collect environmental data or data regarding (i) a monitored unit for M2M applications or (ii) user **113** for applications where module **101** comprises a mobile phone and user **113** is an individual person such as a mobile phone subscriber. Sensor **101***f* could collect data such as, but not limited to, temperature, humidity, pressure, visible light levels, radiation, shock and/or vibration, voltage, current, weight, pH levels, orientation/motion, or the presence of specific chemicals. Sensor **101***f* could also be a microphone. Sensor **101***f* could be a magnetic strip reader for credit cards and similar cards, or an antenna for either near-field RF communications, such as, but not limited to, reading an RF identity tag. An antenna for a sensor **101***f* could also collect longer-range RF signals, such as, but not limited to, reading long-range radio frequency identity tags. Sensor **101***f* could also collect biometric data such as, but not limited to, heart rate, glucose levels, body temperature, or other health measurements for a user **113**. The sensor **101***f* can provide data to the CPU **101***b* in the form of analog or digital data, which can be communicated via a system bus **101***d* or physical interface **101***a* and other electrical interfaces are possible as well. A sensor

Petitioner Samsung Ex-1004, 0029

measurement can comprise the analog or digital data collected by CPU **101***b* from sensor **101***f*.

A sensor measurement from sensor **101***f* can include processing of the analog or digital data input CPU **101***b* by sensor **101***f*, such as, but not limited to, averaging over time, using mathematic formulas to convert the raw data from sensor **101***f* into a usable form. Module **101** may also collect sensor data or sensor values using a sensor **101***f* and CPU **101***b*, where the data or values are derived from electrical signals output by a sensor **101***f*. A sensor measurement can comprise the sensor data or sensor values. If module **101** comprises a "point of presence" payment terminal, then a sensor measurement could comprise data read from a payment card. As contemplated herein, the terms "sensor measurement" and "sensor data" can be used interchangeably, and can also be considered functionally equivalent. Although a single sensor **101***f* is shown in FIG. **1***c*, a module **101** could include multiple sensors. Each of the multiple sensors **101***f* could include a sensor identity **151**, which could comprise a number or string to identify the sensor **101***f*. A sensor **101***f* could be external to module **101**, and also a plurality of sensors **101***f* may be used and they also can connect to module **101** when module **101** uses radio **101***z* as a base station for a WiFi network.

Actuator **101***y* could be a device to control a parameter or state for a monitored unit in M2M applications for module **101**, such as, but not limited to, changing a voltage or current, activating a switch or relay, turning on or off a microphone or speaker, activating or deactivating a light, and other examples are well known in the art. Actuator **101***y* could also be a speaker. Actuator **101***y* could be controlled by module **101** via a digital or analog output from CPU **101***b*, which could also be transmitted or sent via system bus **101***d* or a physical interface **101***a*. Although actuator **101***y* is illustrated as external to wireless module **101** in FIG. **1***c*, actuator **101***y* could also be internal to module **101**, and module **101** could include multiple actuators **101***y*. A module **101** could include multiple actuators **101***y* each with an actuator identity **152**. Sensors and actuators are well known to those of ordinary skill in the art, and thus are not described in additional detail herein.

Module **101** can include a Universal Serial Bus (USB) interface **101***v*. In accordance with an exemplary embodiment, module **101** can comprise a wireless module and include a radio **101***z*. Note that the use of a radio **101***z* is not required for module **101**, which could also obtain a connection to the IP Network **111** via a wired line such as Ethernet. Although not illustrated, radio **101***z* could include antennas for reception and transmission of RF signals, and even multiple antennas could be used. Although a single radio **101***z* is illustrated in module **101**, module **101** could also contain multiple radios **101***z*. Radio **101***z* can support wireless LAN standards such as, but not limited to, WiFi, Bluetooth, and Zigbee, or similar wireless LAN standards. Note that module **101** may also operate as a base station in a wireless LAN, such as, but not limited to, an 802.11 base station. When module **101** operates a wireless LAN, radio **101***z* can function as either a client/node and/or a base station **103** to support communication from other wireless nodes in physical proximity, such as, but not limited to, other nodes within an exemplary 50 meters. The other wireless nodes could comprise a sensor **101***f* and/or actuator **101***y*, and in this case a sensor could be referred to as a "networked sensor" and an actuator could be referred to as a "networked actuator".

In accordance with exemplary embodiments, module **101** can store module private key **112***a*, MNO public key **502**, and module identity **110**, and a symmetric key **127** in memory/RAM **101***e* during operation, such as when CPU **101***b* is active and the module **101** is connected to a network such as a wireless network **102** during data transmissions. Module private key **112***a* preferably is recorded in nonvolatile memory such as, but not limited to, flash memory **101***w*, so that module **101** has access to its private key **112***a* after the private key has been derived or loaded, including times when a battery **101***k* has been fully drained or removed from module **101** (if module **101** does not utilize a persistent power source such as land-line power). Symmetric key **127** can be a secure, shared private key for use with symmetric encryption or symmetric ciphering algorithms **211** (in FIG. **2***c* below). Symmetric key **127** may also include an expiration time **133**, such that symmetric key **127** may only be used by module **101** and/or eUICC **107** during a limited period of time, such symmetric key **127** remaining only valid for a day, or a week, or during a session (where the session comprises multiple messages and/or responses between a module **101** and a wireless network **102**), etc.

Module identity **110** is preferably a unique identifier of module **101**, and could comprise a number or string such as, but not limited to, a serial number, an international mobile subscriber identity number (IMSI), international mobile equipment identity (IMEI), or an Ethernet media access control (MAC) address. According to an exemplary embodiment, module identity **110** can also comprise a serial number or string that is written into hardware of module **101** upon manufacturing or distribution of module **101** (also depicted and described in connection with a step **511** in FIG. **5***b* below). In this case, module identity **110** could be recorded in a read only memory **101***c*, where read only memory **101***c* could not be easily erased or otherwise tampered with. Read only memory **101***c* could also comprise a protected memory and the address for accessing the module identity **101** within the ROM **101***c* could comprise a protected address.

A protected address can comprise an address accessible to a CPU **101***b* and readable by CPU **101***b* where the data within the protected address is not modified, changed, or updated by a CPU **101***b* under normal operating conditions. Also note that the protected address can comprise one form of a nonvolatile memory, where a memory records data. In exemplary embodiments module identity **110** may preferably be permanently or persistently associated with the physical hardware of module **101**, which can be helpful for the security procedures contemplated herein. Module identity **110** can function as a basic identifier for services from mobile network operator **104**, eUICC subscription manager **109**, wireless network **102**, M2M service provider **115**, or server **105** in order to properly identify module **101** among a plurality of modules. Module private key **112***a* and an associated module public key **112***b* could be unique to module **101** and uniquely associated with module identity **110**, according to a preferred embodiment.

MNO public key **502** in module **101** could be obtained from downloading the key over the IP Network **111**, or optionally also written into nonvolatile memory of module **101** upon manufacture or distribution. MNO public key **502** could be obtained using a domain name or Internet address that is recorded in nonvolatile memory upon the configuration of module **101**, such as, but not limited to, during installation or distribution, and module **101** could fetch the MNO public key **502** upon connecting to a wireless network **102** or other connection to the IP Network **111**. Additional elements besides those depicted in FIG. **1***c* could also be recorded in volatile memory **101***e*, which could comprise a RAM **101***e*. For example, cryptographic algorithms **141**

Petitioner Samsung Ex-1004, 0030

could also be recorded in RAM **101***e* as well. Note that values and related data can also be recorded in both RAM **101***e* and nonvolatile memory **101***w* at the same time, such that data in nonvolatile memory **101***w* allows module **101** to access the data after a shutdown state, but moving the same data into RAM **101***e* during an active state allows module **101** to more quickly perform operations using a CPU **101***b*. Other possibilities exist as well for the storage location of various values and data elements illustrated in FIG. **1***c* without departing from the scope of the present invention.

Module **101** may also contain cryptographic algorithms **141**, which may comprise a suite of algorithms or subroutines that can be utilized for (i) deriving a pair of keys comprising a public key and a private key, (ii) encrypting data using public keys, (iii) decrypting data using private keys, (iv) processing secure hash signatures using private keys, and (v) verifying secure hash signatures using public keys, and related software, firmware, or subroutines for implementing a cryptographic system, including symmetric ciphering algorithms. Cryptographic algorithms **141** could utilize publicly available software libraries within tools such as, but not limited to, OpenSSL maintained by The OpenSSL Project (http://www.openssl.org/), libgcrypt maintained by The Free Software Foundation (http://www.gnu.org/software/libgcrypt/), and similar libraries such as, but not limited to, libmcrypt and Crypto++. Note that cryptographic algorithms **141** could also use proprietary cryptographic libraries as well. In addition to implementing asymmetric encryption/ciphering, such as, but not limited to, used with RSA and ECC cryptography, cryptographic algorithms **141** can provide symmetric ciphering where a shared private key is utilized to both encrypt and decrypt, such as, but not limited to, with the Advanced Encryption Standard (AES) cipher suite.

As illustrated in FIG. **1***c*, module **101** may also contain a random number generator **128**. Random number generator **128** may contain a seed **128***b*. The creation of random numbers with a high degree of entropy may be important the use of cryptographic algorithms **141**. A plurality of the data as a source for a random number seed **128***b* 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 **101***z* measurements, clock **160** times or values, memory **101***e* or memory **101***w* states, operating system **101***h* states, actuator **101***y* states, and/or hardware **101***a* or **101***d* states). Note that values or data for each of the elements listed in the previous sentence could be utilized in a "module random seed file" instead of or in addition to a state. The use of a "module random seed file" with a random number generator **128** is also depicted and described in connection with FIG. **1***d* of U.S. patent application Ser. No. 14/084,141, filed Nov. 19, 2013 in the name of John Nix, which is hereby incorporated by reference in its entirety.

FIG. **1***d*

FIG. **1***d* is a graphical illustration for authenticating with a wireless network using a physical UICC, in accordance with conventional technology. FIG. **1***d* illustrates the components and interfaces for using a physical UICC in order to a module **101** conduct an authentication with a wireless network **102** according to wireless WAN standards which use a pre-shared secret key K recorded in the physical UICC **116**. The wireless network could be an LTE, LTE Advanced, or a 3G network, and also based on related standards. With a 3G network, the pre-shared secret key K is also known as "Ki". The module **101** can include a network application **101***x*, a UICC driver **114**, and a physical interface supporting the ISO/IEC 7816-3 electrical standards, such as the third edition published on Nov. 1, 2006. The physical UICC **116** can be a smart card in the form factor of a mini-SIM, micro-SIM, or nano-SIM, connected to the physical interface such as ISO/IEC 7816-3 and related electrical standards. The physical interface can include six electrical contacts known as C1 through C6, where C1 provides a power supply to the physical UICC **116**, C2 provides a reset signal input, C3 provides a clock signal input, etc. The network application **101***x* can comprise software or firmware for the module **101** to communicate with the wireless network **102** using the standards that include layer 2 messages between module **101** and wireless network **102** such as, but not limited to, radio resource control (RRC) messages, security mode commands, ciphering, and authentication. The network application **101***x* can communicate with a radio **101***z* (described in FIG. **1***c*) using the system bus **101***d*.

A network application **101***x* in a FIG. **1***d* can be similar or equivalent to a network application **101***x* depicted and described in connection with FIG. **1***b*. The UICC driver **114** can comprise a driver within a set of drivers **101***g* within module **101**, where drivers **101***g* are also depicted and described in connection with FIG. **1***b*. A physical UICC **116** can support other and additional functionality for a module **101** than the authentication functionality depicted in FIG. **1***b*, such as, but not limited to, (i) recording a set of network parameters equivalent to a set of network parameters **201** in FIG. **2***a* below in order to module **101** to identify and select a wireless network **102**, (ii) recording an address book with a list of phone numbers for user **113**, (iii) recording a list of recent SMS messages and telephone numbers dialed, and/or (iv) recording and implementing a personal identification number (PIN) in order for a user **113** to authenticate and access the module **101** with the UICC **116**, and other functionality of a physical UICC **116** is possible as well. The physical UICC **116** can also include (i) an IP Multimedia Services Identity Module (ISIM) application and data and/or a (ii) Universal Subscriber Identity Module (USIM) application for the module **101** to utilize when communicating with the wireless network **102**.

After power-up of the module **101** from a powered off state, the module **101** can use the UICC driver **114** to read data from the physical UICC **116** such as a set of network parameters **203** (depicted in FIG. **2***a* below) as well as an IMSI or equivalent value as a network module identity. The set of network parameters **203** or IMSI in a physical UICC **116** may not be encrypted (or associated with an eUICC profile **107***d*) and the set of network parameters can be directly read by the UICC driver **114**. The module **101** can use the set of network parameters to tune a radio **101***z* to particular frequencies for the wireless network **102** and search for a beacon signal from a base station **103**. The beacon signal can include codes such as a mobile country code (MCC) and mobile network code (MNC) that can match values in either the network parameters or IMSI. Upon finding and selecting a base station **103**, the module **101** can send a random access channel (RACH) message and subsequently an identity value recorded in the physical UICC **116** such as an IMSI, temporary mobile subscriber identity (TMSI), a globally unique temporary identity (GTUI), or a similar value to identify the module **101** using the physical UICC **116** with the wireless network **102**.

In order to authenticate a module **101** with the wireless network **102**, the wireless network **102** can record a set of authentication tokens or vectors associated with a network identity sent by the module **101**, such as a GTUI value. An authentication vector **117** for the module's **101** network

Petitioner Samsung Ex-1004, 0031

identity can comprise a vector or set of values that includes a random number (RAND) **118**, response (RES) **119**, a network authentication token (AUTN), and a sequence number. The value AUTN and sequence number is not shown in FIG. **1***d* and subsequent figures such as FIG. **1***e* and FIG. **3**, but the value AUTN and sequence number can be used by module **101** with a physical UICC **116** or eUICC **107** in order to authenticate the wireless network **102**. The sequence number can prevent replay attacks and the AUTN value can comprise a digital signature or message digest value the physical UICC **116** or eUICC **107** can also calculate using the RAND **118** value in order for the module **101** to authenticate the wireless network **102**. The values for the authentication vector **117** that includes a RAND **118** and a RES **119** can be calculated by a home subscriber server (HSS) for the mobile network operator **104** associated with the wireless network **102** and provided by the mobile network operator **104** to servers associated with the wireless network **102**. An exemplary format for the use of a RAND **118** with a response RES **119** is described in ETSI standard TR 131 900 v.10.0.0 and related documents. Other possibilities exist as well for the format, structure, and data elements within an authentication vector **117** without departing from the scope of the present invention.

In order to conduct an authentication of module **101**, after receiving a RACH message and the network module identity such as an IMSI, TMSI, or GTUI value, the wireless network **102** can send a RAND **118** from the authentication vector **117**. The module **101** can receive the RAND **118** value using the network application **101***x* and the radio **101***z*. The network application **101***x* can send the RAND **118** value to the UICC driver **114**, and the UICC driver **114** can send the RAND **118** value through the physical interface such as ISO/IEC 7816-3 to the physical UICC **116**. After receiving the exemplary RAND **118** message, in order to conduct an authentication, module **101** using a physical UICC **116** could take steps to demonstrate to a wireless network **102** that the physical UICC **106** records the same pre-shared secret key K for the network module identity as recorded by a mobile network operator **104** associated with the wireless network **102**. Physical UICC **116** can properly respond to the RAND **118** using message digest algorithms by calculating a secure hash value RES **119** using the RAND **118** and the recorded secret key K. The physical UICC **116** could use algorithms specified in ETSI TS 135 205-209, as well as subsequent and related standards, in order for the physical UICC **116** to calculate a secure hash value such as a RES **119**. The calculation and processing of a RES **119** using a RAND **118** and a secret key K is also depicted and described in connection with steps **306** and **311** of FIG. **3**. Other possibilities exist as well for a physical UICC **116** or an eUICC **107** to calculate a RES **119** value using a RAND **118** and a secret key K without departing from the scope of the present invention.

After the calculation of a RES **119** value in response to the RAND **118**, the physical UICC **116** can send the RES **119** to the UICC driver **114** through the physical interface such as ISO/IEC 7816-3. The device driver **114** can send the RES **119** value to the network application **101***x* and the network application **101***x* can send the RES **119** value to the wireless network **102** using a radio **101***z* and the base station **103**. The wireless network **102** can take steps to compare the received RES **119** with a recorded RES **119** value in the authentication vector **117**. If the received RES **119** matches the recorded RES **119** in the authentication vector **117** then the module **101** with the physical UICC **116** can be considered authenticated. The authentication of module **101** by wireless network **102** is also depicted and described in connection with a step **308***a* of FIG. **3**. After successful authentication, the module **101** and wireless network **102** can then take subsequent steps for a module **101** to have access to the IP network **111** including the public Internet, as well as configuring services such as voice and SMS.

FIG. **1***e*

FIG. **1***e* is a graphical illustration for authenticating with a wireless network using an eUICC, in accordance with exemplary embodiments. A module **101** with an eUICC **107** can perform the equivalent steps for authentication with a wireless network **102**, such that a module **101** can use an eUICC **107** instead of a physical UICC **116**. The wireless network **102** can perform the same steps as (i) recording an authentication vector **117** from a mobile network operator **104** associated with the wireless network **102**, (ii) receiving a RACH message and a network module identity such as a GTUI or TMSI from the module **101**, (iii) sending values from the authentication vector **117** including a RAND **118**, and (iv) receiving a RES **119** and comparing the received RES **119** with a recorded RES **119** in the authentication vector **117** in order to authenticate the module **101** using an eUICC **107** instead of a physical UICC **116**. In other words, the use of an eUICC **107** by module **101** can be transparent to a wireless network **102**, such that a module **101** with an eUICC **107** instead of a physical UICC **116** can be fully "backward compatible" with standards, software, and infrastructure deployed on a wireless network **102**.

A module **101** in FIG. **1***e* can include a network application **101***x*, an eUICC driver **129**, an eUICC **107**, and an operating system **101***h*. The network application **101***x* can be equivalent or similar to a network application **101***x* depicted and described in connection with FIG. **1***d* and FIG. **1***b* above. The use of an eUICC **107** instead of a physical UICC **116** within module **101** can also be transparent to network application **101***x*, via the use of eUICC driver **129**. In other words, in exemplary embodiments, the same or equivalent network application **101***x* can be used for either (i) a module **101** with a physical UICC **116** or (ii) a module **101** with an eUICC **107**, since the eUICC driver **129** can perform the identical input and output functions as a UICC driver **114** when communicating with the network application **101***x*. The use of an eUICC driver **129** is also depicted and described in connection with FIG. **1***b* above. The eUICC driver **129** can communicate with the network application **101***x* using the operating system **101***h*. The internal communication between network application **101***x* and eUICC driver **129** using an operating system **101***h* could comprise sharing memory **101***e*, such that network application **101***x* writes messages such as, but not limited to, an exemplary RAND **118** value into the shared memory **101***e* and eUICC driver **129** reads the values from the shared memory **101***e*. In another embodiment, the internal communication between network application **101***x* and eUICC driver **129** using an operating system **101***h* could comprise using loopback UDP ports within operating system **101***h*, such that network application **101***x* sends a UDP datagram with the RAND **118** value using a first UPD loopback port, and the eUICC driver **129** receives the UDP datagram with the RAND **118** value using a second UDP loopback port. Similar steps could be taken as well for an eUICC driver **129** to send data such as a RES **119** to the network application **101***x* using the operating system **101***h*.

As illustrated in FIG. **1***e*, eUICC driver **129** can also communicate with the eUICC **107** using the operating system **101***h*. Two differences between conventional technology illustrated in FIG. **1***d* and the exemplary embodiment

Petitioner Samsung Ex-1004, 0032

illustrated in FIG. **1***e* include (i) the eUICC driver **129** communicates with the eUICC **107** using operating system **101***h* instead of a physical interface such as ISO/IEC 7816-3 and related electrical standards, and (ii) the eUICC **107** can operate as a separate program or application within memory **101***e* or memory **101***w* instead of a physically separate application operating on a physical UICC **116**. The eUICC driver **129** can communicate with the eUICC **107** using the equivalent steps and procedures for an network application **101***x* to communicate with an eUICC driver **129** described in the paragraph above, including using shared memory or sending UDP loopback messages on internal UDP loopback ports. Other possibilities for the communication between eUICC driver **129** and eUICC **107** exist as well without departing from the scope of the present invention. In addition, although eUICC driver **129** and eUICC **107** are depicted in FIG. **1***e* and FIG. **1***b* as separate elements, programs, and/or processes for a module **101**, the eUICC driver **129** could be optionally combined with an eUICC **107** such that the network application **101***x* can communicate directly with the eUICC **107** using the operating system **101***h*.

The eUICC **107** can include an eUICC profile **107***d* which can contain the same information used by a physical UICC **116** in FIG. **1***d* above, including a set of network parameters, a network module identity, and a key K. In other words, the data recorded in a eUICC **107** in the form of a profile **107***d* can allow and support the eUICC **107** in FIG. **1***e* to operate in an equivalent manner as a physical UICC in FIG. **1***d* for the authentication steps illustrated in FIG. **1***d* and FIG. **1***e*. Although not illustrated in FIG. **1***e*, the eUICC **107** could also perform the similar or equivalent functions of a physical UICC including (i) recording a set of network parameters equivalent to a set of network parameters **201** in FIG. **2***a* below in order to module **101** to identify and select a wireless network **102**, (ii) recording an address book with a list of phone numbers for user **113**, (iii) recording a list of recent SMS messages and telephone numbers dialed, and/or (iv) recording and implementing a personal identification number (PIN) in order for a user **113** to authenticate and access the module **101** with the eUICC **107**. Other functionality of an eUICC **107** for a module **101** is possible as well without departing from the scope of the present invention.

As illustrated in FIG. **1***e*, the network application **101***x* in module **101** can receive a RAND **118** value from wireless network **102** in order to authenticate the module **101**. The network application **101***x* can send the RAND **118** value to the eUICC driver **129**. The eUICC **107** can read a RAND **118** value from the network application **101***x* using the eUICC driver **129**. After receiving the exemplary RAND **118** message, in order to conduct an authentication, module **101** using an eUICC **107** could take steps to demonstrate to a wireless network **102** that the module **101** records the same pre-shared secret key K for the network module identity as recorded by a mobile network operator **104** associated with the wireless network **102**. eUICC **107** can properly respond to the RAND **118** using message digest algorithms by calculating a secure hash value RES **119** using the RAND **118** and the recorded secret key K from the profile **107***d*. The eUICC **107** could use algorithms specified in ETSI TS 135 205-209, as well as subsequent and related standards, in order for the eUICC **107** to calculate a secure hash value such as a RES **119**. The calculation and processing of a RES **119** using a RAND **118** and a secret key K for an eUICC **107** is also depicted and described in connection with steps **306** and **311** of FIG. **3**. Other possibilities exist as well for an eUICC **107** to calculate a RES **119** value using a RAND **118** and a secret key K, without departing from the scope of the present invention. As illustrated in FIG. **1***e*, the eUICC **107** can send the RES **119** to the eUICC driver **129**, and the eUICC driver **129** can send the RES **119** to the network application **101***x*. The network application **101***x* can then send the RES **119** to the wireless network **102**, and the wireless network **102** could perform a step **308***a* as depicted and described in connection with FIG. **3** in order to authenticate the module **101** using the eUICC **107** and profile **107***d*.

FIG. **1***f*

FIG. **1***f* is a graphical illustration of an exemplary system that includes a module, a mobile network operator, and an eUICC in accordance with exemplary embodiments. System **199** in FIG. **1***f* can include a mobile network operator **104** and a module **101**. The mobile network operator **104** can communicate with the module **101** using a wireless network **102**, and the wireless network **102** could comprise the radio access portion of the mobile network operator **104**, such as a collection of base stations **103** using licensed radio spectrum such as, but not limited to, the 700 Mhz band for LTE, and other possibilities exist as well for the wireless network **102**. The mobile network operator **104** can include a server **105** with an IP address **106***a*. The server **105** with MNO **104** in FIG. **1***f* can comprise a Mobility Management Entity (MME) in LTE networks, or equivalent functionality to receive authentication requests from modules **101** with other wireless wide-area networking technology. The MME can support radio bearer activation/deactivation processes for the module **101** and authenticating the module **101** by recording an authentication vector **117**, where the authentication vector **117** can be received from an HSS.

The server **105** can comprise a server as depicted and described in connection with server **105** in FIG. **1***k* and FIG. **1***m* of U.S. patent application Ser. No. 14/084,141, filed Nov. 19, 2013 in the name of John Nix, which is hereby incorporated by reference in its entirety. The IP address **106***a* can include a subnet prefix **106***d* and an interface identifier **106***e*. The IP address **106***a* can comprise an IPV6 address, where the subnet prefix **106***d* comprises the first 64 bits of a 128 bit IPv6 address, and the interface identifier **106***e* can comprise the last 64 bits of a 128 bit IPv6 address as shown in FIG. **1***f*. Other nodes connected to the wireless network **102** can also include IPv6 addresses with different values for the subnet prefix **106***d* and the interface identifier **106***e*. A module **101** can include both a network application **101***x* and an eUICC **107**, where a network application **101***x* is depicted and described in connection with FIG. **1***b* and an eUICC **107** is depicted and described in connection with FIG. **1***a*, FIG. **1***b*, FIG. **1***c*, and FIG. **1***e*.

In an exemplary embodiment, different elements within module **101** can be associated with different IP addresses. The network application **101***x* can be associated with an IP address **106***b* and the eUICC **107** can be associated with an IP address **106***c*. The wireless network **102** could assign the module **101** the subnet prefix **106***d* used by module **101** with wireless network **102**, and an operating system **101***h* could assign the interface identifier **106***e* used by the network application **101***x* and the eUICC **107**. Other possibilities exist as well for the source of IP addresses in a system **199**, but an end result can comprise the eUICC **107** having a unique IPV6 address **106***c* such that a server **105** such as an MME can communicate with the eUICC **107** directly by sending a packet with a RAND **118** value from server **105** address **106***a* to eUICC **107** address **106***c*.

Although not illustrated in FIG. **1***f*, the exemplary IP addresses for server **105** and eUICC **107** can be associated

Petitioner Samsung Ex-1004, 0033

with port numbers, such that server **105** can use a first port number with the IP address **106***a* when sending a RAND **118**, and eUICC **107** could use a second port number with the IP address **106***c* when receiving the RAND **118**. Server **105** can use a third port number when receiving a RES **119**, and eUICC **107** could use a fourth port number when sending the RES **119**. The first and third port numbers could be the same value or number, and the second and fourth port numbers could be the same value or number. In an exemplary embodiment, the RAND **118** and RES **119** in system **199** can be formatted according to the UDP Lite protocol, as specified in IETF RFC 3828, which is also incorporated by reference herein. The term "UDP Lite" described in the present invention may also refer to any connectionless protocol supported on IP Network **111** and wireless network **102** where checksums may be partially disabled, thereby supporting the transfer of bit errors within a datagram.

As illustrated in FIG. **1***f*, an eUICC **107** operating in module **101** could be an application with a unique IPV6 address **106***c*, and the network application **101***x* utilize a different IPv6 address **106***b*. The two IP addresses could be on the same subnet **106***d* used by a module **101**, and the network application **101***x* could communicate with the eUICC **107** locally within module **101** using the two different IPV6 addresses **106***b* and **106***c*. The network application **101***x* could communicate with the eUICC **107** locally for exemplary "other data" depicted in FIG. **1***f*, which could comprise the storing of an address book in the eUICC **107**, reading a set of network parameters by the network application **101***x* from the eUICC **107** with the eUICC profile **107***d*, etc. In an exemplary embodiment, the eUICC **107** could communicate with the mobile network operator **104** for authentication, thus potentially bypassing the network application **101***x* for separate handling of RAND **118** and RES **119** values depicted in FIG. **1***e* above. The authentication messages comprising a RAND **118** and a RES **119** could be communicated between the eUICC **107** with IP address **106***c* to the mobile network operator **104** with IP address **106***a* without the use of a network application **101***x*.

The eUICC **107**, with an associated IP address **106***c* could also communicate with the eUICC subscription manager **109** by sending a packet from IP address **106***c* to an IP address of a server associated with the eUICC subscription manager, such as the exemplary data for a step **205** depicted and described in connection with FIG. **2***a* and FIG. **3** below. Note that the eUICC **107** with the IP address **106***c* can communicate with the eUICC subscription manager **109** without the wireless network **102**, but rather through an IP network **111**. The connectivity for the IP network **111** could be provided by a different wireless network **102** than the wireless network **102** associated with the MNO **104**. Although the use of a specific, unique IP address **106***c* for eUICC **107** is illustrated in FIG. **1***f*, an eUICC **107** does not require a separate IP address **106***c* in other embodiments, and the eUICC **107** could share an IP address **106***b* with a network application **101***x* or other processes or elements within module **101**.

FIG. **2***a*

FIG. **2***a* is a graphical illustration of an exemplary profile for an eUICC, including encrypted data, decryption steps, and decrypted data for the profile, in accordance with exemplary embodiments. Two exemplary forms of an eUICC profile are illustrated in FIG. **2***a*: an encrypted eUICC profile **107***c* and an eUICC profile **107***d*. As contemplated herein, an eUICC profile, such as the exemplary eUICC profile **107***c* and **107***d*, can be similar to profiles for an eUICC contemplated in ETSI specification TS 103 383 v12.2.0 and related standards, but with differences to the currently published standards, as described below. An eUICC profile **107***d* can comprise the data from an encrypted eUICC profile **107***c*, where (i) a first portion of the data, comprising ciphertext **208***a*, has been decrypted, and (ii) a second portion of the encrypted eUICC profile **107***c*, comprising ciphertext **208***b* remains encrypted. Thus, an encrypted eUICC profile **107***c* can include a first portion, or ciphertext **208***a* and a second portion, or ciphertext **208***b* as depicted in FIG. **2***a*. As contemplated herein, an encrypted eUICC profile **107***c* can be referred to as "profile **107***c*", and the eUICC profile **107***d* can be referred to as "profile **107***d*". Both profile **107***c* and profile **107***d* can include a profile identity **107***e*. Profile identity **107***e* can comprise a number or string such that various elements illustrated in FIG. **1***a* can properly refer to, select, and or identity a profile **107***c* or profile **107***d*, including elements such as a mobile network operator **104**, eUICC subscription manager **109**, module **101**, and/or an eUICC **107**.

A profile **107***c* or profile **107***d* in exemplary systems herein, including systems **100**, **300**, and **500** can comprise several different possible embodiments. The profiles could be recorded in a file or data set, and stored in nonvolatile memory associated with an eUICC **107**, such as, but not limited to, a flash memory **101***w*. As transferred across a wireless network **102** and/or IP network **111**, the encrypted eUICC profile **107***c* can be segmented into separate datagrams and transferred using a transport layer protocol such as TCP. An application layer protocol such as transport layer security (TLS) and additional ciphering at the data-link layer could be utilized as well, in addition to sending and receiving the data for a profile **107***c* as ciphertext **208***a* and **208***b*. The exemplary forms for a profile **107***c* and **107***d* in FIG. **2***a* can represent data for a file recorded in a module, such as, but not limited to, (i) storing in a volatile memory **101***e* when the profiles **107***c* or **107***d* are being processed or accessed by a CPU **101***b*, or (ii) storing in an nonvolatile memory such as flash memory **101***w* when the profile **107***c* and **107***d* are stored long term, including times when a battery **101***k* may be removed from module **101**.

Note that profile **107***c* with at least two distinct portions, comprising ciphertext **208***a* and ciphertext **208***b*, could be recorded in separate segments or in distinct location within module **101** or with an eUICC subscription manager **109**, and the two or multiple portions together can comprise a profile **107***c*. In other words, the portions of ciphertext **208***a* and **208***b* (and other data in a profile **107***c* or profile **107***d*) can be recorded in different locations while comprising a profile **107***c*. Other possibilities exist as well for the structure and recording of the exemplary data for a profile **107***c* and **107***d* without departing from the scope of the present invention. Although the label "Stored w/Subscription Manager **109**" is depicted with an encrypted eUICC profile **107***c*, the encrypted eUICC profile **107***c* can also be stored as the format depicted in FIG. **2***a* within a module **101** or an eUICC **107**, until at least a step **206** is performed to decrypt the first ciphertext **208***a*, as described in this FIG. **2***a* and FIG. **3** below.

A first portion of profile **107***c* can include ciphertext **208***a*, where ciphertext **208***a* can include a set of network parameters **201**, a first network module identity **202**, and a first key K **203**. Ciphertext **208***a* can include these elements in a ciphered string or file, such that a third party would not feasibly be able to ready the plaintext within ciphertext **208***a* without a key such as eUICC profile key **107***b*. Ciphertext **208***a* can comprise the set of network parameters **201**, the first network module identity **202**, and the first key K **203** as

Petitioner Samsung Ex-1004, 0034

plaintext ciphered with a eUICC profile key **107***b*, as depicted and described in connection with FIG. **2***b* below. The set of network parameters **201** could comprise a list of values and settings for a module **101** to utilize in connecting with a mobile network operator **104**. The set of network parameters **201** could include a list of numbers or strings for values such as (i) allowed frequencies or frequency bands to scan, (ii) preferred access lists for roaming onto other wireless networks, (iii) criteria for a module **101** to select base stations **103** in idle mode, (iv) support for emergency services, (v) supported languages or character encoding, (vi) codes to search for in beacons broadcast by a wireless network **102**, (vii) parameters for a radio **101***z* to use when connecting to a wireless network **102**, (viii) names or addresses for a server **105** associated with a MNO **104** in order for a module **101** to send data, etc.

A first network module identity **202** within a ciphertext **208***a* in profile **107***c* can comprise a subscriber identity or related identifier of module **101** when connected to a MNO **104** through a wireless network **102**. In an exemplary embodiment, the first network module identity **202** can comprise an international mobile subscriber identity (IMSI), a globally unique temporary identity (GTUI), a media access control (MAC) address, a temporary mobile subscriber identity (TMSI) or a similar number or string to identify a module **101** with wireless network **102**. Note that a network module identity such as the first network module identity **202** can be different than a module identity **110**, such that a network module identity can be assigned by a mobile network operator **104**, while a module identity **110** can be assigned by manufacturer. In other words, a network module identity such as the first network module identity **202** can change over time for a module **101**, while the module identity **110** can remain the same. The eUICC identity **107***a* can also remain the same value or number while a network module identity changes.

A first key K **203** within a ciphertext **208***a* in profile **107***c* can comprise a standards-based shared secret key K for use in wireless WAN networks based on ETSI, 3GPP, and related standards. As currently specified in ETSI/3GPP standards for LTE and LTE Advanced networks, the shared secret key K, (i) recorded in a SIM or UICC, and a MNO **104** HSS, and (ii) described in 3GPP TS 33.401 V12.9.0 and related standards, comprises a pseudo-random number with a length of 128 bits. The length of key K for standards-based wireless networks **102** may be extended in the future. The use of shared secret key K for authentication of a module **101**, and also for ciphering and data integrity, with a wireless network **102** that implements ETSI and/or 3GPP standards is also defined in the specifications ETSI TS 135 205-209 and related standards. Both the first key K **203** and the second key K **204** can comprise a shared secret key K as described in 3GPP TS 33.401 V12.9.0 FIGS. **6.2-1** and related standards. A mobile network operator **104** using the function of an authentication center, possibly within a home subscriber server (HSS) can generate or process authentication vectors **117** comprising an random number (RAND), an authentication token (AUTN), a response (RES), and a sequence number using the first key K **203** recorded in a eUCC profile **107***c* or **107***d* for the first network module identity **202**. Likewise, authentication vectors **117** can be generated by a HSS and sent to a MME for the second network module identity **209***a* with the second key K **204**.

In exemplary embodiments, the first key K **203** depicted in FIG. **2***a* is also depicted and described as operating as a standards-based shared secret key K in FIG. **3** below at a step **306**. Using the properties of a standards-based key K, a module **101** or an eUICC **107** can use the first key K **203** and a first random number RAND **118** received to process or calculate a first response RES **119**. Step **306** with a first key K **203** can comprise an authentication for a module **101** (comprising a "mobile phone", "mobile station", or "user equipment") within standards such as 3GPP TS 33.401 V12.9.0 and related standards using a shared secret key K. As contemplated herein, the use of the term "random number" can comprise a pseudo-random number with a high degree of information entropy that may not be purely mathematically random, but can be considered a random number and referred to as a random number for the purposes herein.

In an exemplary embodiment, as described in FIG. **2***e* and step **302***a* of FIG. **3** below, the first key K **203** can be optionally recorded in ciphertext **208***a* with an additional layer of encryption, such that the first key K **203** is recorded as a ciphertext **208***c* within ciphertext **208***a*. In other words, upon conversion of ciphertext **208***a* into plaintext using a profile deciphering algorithm **206**, the first key K **203** can retain an additional layer of encryption as ciphertext **208***c* with other data in a profile **107***d* that may be plaintext. This optional additional layer of encryption for the first key K **203** is also depicted within the profile **107***d*, where ciphertext **208***c* optionally remains in profile **107***d* after the conversion of ciphertext **208***a* into plaintext using a step **206**. As described below, the optionally additional layer of encryption for ciphertext **208***c* with the first key K **203** can be (i) processed into plaintext first key K **203** (ii) after a subsequent deciphering with an asymmetric ciphering algorithm **219** as illustrated in FIG. **2***e*.

Note that the additional layer of encryption for the first key K **203**, in the form of using a ciphertext **208***c*, can be optionally omitted and the first key K **203** could be plaintext after the conversion of the first portion of profile **107***c* as ciphertext **208***a* into plaintext in a profile **107***d* using a step **206**. Thus, the dashed lines around the first key K **203** as a ciphertext **208***c* indicate the use of ciphertext **208***c* is optional, depending on the security requirements for an MNO **104** when distributing electronically the first key K **203**. In another embodiment as described in FIG. **3**, the first key K **203** can comprise a null value, such as the value for a key K in order to support emergency services if module **101** has no valid UICC, and in this case the use of additional encryption via ciphertext **208***c* can be omitted for a first key K **203**. In a related embodiment, the first key K **203** can be omitted entirely from a profile **107***c* and profile **107***d*, and the eUICC **107** can subsequently use a null value for the first key K **203**.

A second portion of profile **107***c* can include ciphertext **208***b*, where ciphertext **208***b* can include a second key K **204***a* and a second network module identity **209***a*. Ciphertext **208***b* can be ciphered with a symmetric key **127**, where the ciphering and deciphering of a portion of ciphertext **208***b* is depicted and described in connection with FIG. **2***c* below. In an exemplary embodiment, the second network module identity **209***a* can comprise an international mobile subscriber identity (IMSI), a globally unique temporary identity (GTUI), a media access control (MAC) address, or similar number or string to identify a module **101**. In exemplary embodiments, the second network module identity **209***a* can be a different number or value than the first network module identity **202**. Although the second network module identity **209***a* is illustrated in FIG. **2***a* as internal to ciphertext **208***b*, the second module identity **209***a* could be external to ciphertext **208***b*, such as, but not limited to, the second network module identity **209***a* being within a profile **107***c* or

Petitioner Samsung Ex-1004, 0035

profile **107***d* and external to ciphertext **208***b*. In other words, in exemplary embodiments, the second network module identity **209***a* may optionally not be ciphered with the symmetric key **127**, while the second key K **204***a* can be ciphered with the symmetric key **127**. As contemplated herein, the term second network identity **209***a* comprises an encrypted second network identity **209***a*, where the second network identity **209** is the plaintext version of the encrypted second network identity **209***a*. Likewise, the term second key K **204***a* comprises an encrypted second key K **204***a*, where the second key K **204** is the plaintext version of the encrypted second key K **204***a*.

In another exemplary embodiment, the second network module identity **209** can comprise the same number or value as the first network module identity **202**, or the second network module identity **209** can be optionally omitted. In this case, if (A) the second network module identity **209** comprises the same number or value as the first network module identity **202**, or the second network module identity **209** is optionally omitted, then (B) the mobile network operator **104** can preferably support the use of two different shared secret keys K (i.e. first key K **203** and second key K **204**) for the same network module identity **202**. However, given the current functionality of an HSS and related infrastructure for wireless networks **102**, the use of two different network module identities (i.e. the first network module identity **202** and the second network module identity **209**) with two different shared secret keys K (i.e. first key K **203** and second key K **204**, respectively) may be more compatible or suitable for deployed and operational HSS infrastructure.

A second key K **204***a* (as an encrypted form of plaintext second key K **204**) within a ciphertext **208***b* in profile **107***c* can comprise a standards-based shared secret key K for use in wireless WAN networks based on ETSI, 3GPP, and related standards. The use of a second key K **204***a* (in an unencrypted form of second key K **204**) can be equivalent to a first key k **203**, but comprise a different random number. The second key K **204** can comprise a random number that is 128 bits in length in order to support 4G networks such as LTE that are widely deployed in 2013, although the length of either first key K **203** or second key K **204** may be a longer number in the future, such an exemplary 256 bits and other possibilities exist as well for the key length. A second key K **204** can also be used with standards-based authentication with a wireless network **102**, where the second key K **204** in FIG. **2***a* is also depicted and described as operating as a standards-based shared secret key K in FIG. **3** below at a step **311**.

The list of exemplary data for encrypted eUICC profile **107***c* and an eUICC profile **107***d* comprises an exemplary set, and the profiles could also include additional data to the exemplary data illustrated in FIG. **2***a*. The additional data for a profile **107***c* or **107***d* could include (i) a set of cryptographic parameters for eUICC **107**, (ii) a set of cryptographic algorithms, such as the exemplary cryptographic algorithms described within ETSI TS 135 205-209 and related standards, (iii) a name or address for an eUICC subscription manager **109** associated with the profile **107***c*, (iv) a name or address for a server **105** associated with a mobile network operator **104**, (v) a digital signature of the profile **107***d* processed with a private key from either eUICC subscription manager **109** or MNO **104**, (vi) a date or timestamp for processing the profile **107***c* or **107***d*, (vii) and similar or related values for a module **101** and/or eUICC **107** to utilize the profiles. This exemplary additional data which is not depicted in FIG. **2***a* could be included within or external to any of ciphertext **208***a* and ciphertext **208***b*.

Note that the profile identity **107***e* may preferably be external to ciphertext **208***a* and ciphertext **208***b*, in order that module **101** and/or eUICC **107** can take steps to identify a profile **107***c* or **107***d*. In addition, although a single profile **107***c* and profile **107***d* are illustrated in FIG. **2***a*, a module **101** and/or an eUICC **107** could include a plurality of profiles **107***c* and/or **107***d*, where each of the plurality of profiles could comprise different data associated with different wireless networks **102**. In an exemplary embodiment, more than one profile **107***c* or profile **107***d* could be associated with the same wireless network **102**, such that a mobile network operator **104** can prefer for the same module **101** to utilize different network access credentials over time, such that the same module **101** could use a different key K and a different network module identity with the same wireless network **102** or mobile network operator **104** over time. Different profiles **107***c* or **107***d* can also be identified by the use of a different profile identity **107***e*. Each profile **107***c* can be associated with an eUICC profile key **107***b* as an encryption key (shown in FIG. **2***b* below), although multiple profiles **107***c* could also share the same eUICC profile key **107***b*.

A module **101** can receive a profile **107***c* using a step **205**. A profile **107***c* can be recorded with an eUICC subscription manager **109** before being received by a module **101**. As depicted in FIG. **2***a*, a module **101** can receive the profile **107***c* at a step **205** using the IP network **111**. The use of a step **205** by a module **101** is depicted and described in connection with FIG. **3** below. The module **101** can receive the profile **107***c* using a network that is different than wireless network **102** associated with the network access credentials comprising the first key K **203** and the first network module identity **202**. In an exemplary embodiment, module **101** can receive the profile **107***c* in a step **205** using an initial wireless network **102**, where module **101** connects with and authenticates with the initial wireless network **102** using an initial eUICC profile **107***d* different than the eUICC profile **107***d* depicted in FIG. **2***a*. Or, module **101** could receive a profile **107***c* using a wireless LAN network or a wired connection via a physical interface **101***a* such as a USB interface **101***v*. In another exemplary embodiment, module **101** can receive the profile **107***c* from a manufacturer, distributor, end user, or technician taking steps to load the profile **107***c* into a nonvolatile memory within module **101** or eUICC **107**. Upon receipt of a profile **107***c* by module **101**, the module **101** can record or store the profile **107***c* with an eUICC **107**.

A module **101** can use an eUICC **107** to decrypt the first portion or ciphertext **208***a* in a profile **107***c* using a step **206**. Before a step **206**, a module **101** can receive an eUICC profile key **107***b*, where the eUICC profile key **107***b* can comprise a symmetric ciphering key. The use of a step **206** by module **101** and/or eUICC **107** is also depicted and described in connection with FIG. **2***b* and FIG. **3** below. Note that both eUICC subscription manager **109** and module **101** can record profile **107***c* with ciphertext **208***a* for a period of time, and the step **206** can be taken (i) after receiving eUICC profile key **107***b* and (ii) before module **101** authenticates with a wireless network **102** using the eUICC profile **107***c*. A step **206** can covert the ciphertext **208***a* into plaintext, such that an eUICC **107** can read the values in order to authenticate with a wireless network **102** using the first key K **203**. By encrypting the first network module identity **202** and the first key K **203**, these network access credentials can remain secure, such that a profile **107***c* can be transferred in normal physical media (such as disks, drives, or files trans-

Petitioner Samsung Ex-1004, 0036

ferred electronically) or in communications channels outside the control of a mobile network operator **104** and/or eUICC subscription manager **109**.

As depicted in FIG. **2***a*, after a step **206** to convert profile **107***c* into profile **107***d*, where the ciphertext **208***a* is decrypted using the eUICC profile key **107***b*, the ciphertext **208***b* with the second key K **204***a* can remain encrypted and thus the second key K can continue to remain secure within a profile **107***d*. In addition, although ciphertext **208***b* is depicted in a profile **107***c* as external to, or separate from, ciphertext **208***a*, ciphertext **208***b* could optionally be included within ciphertext **208***a*. In this case, where ciphertext **208***b* is within ciphertext **208***a* for a profile **107***c*, the result of a step **206** to generate a profile **107***d* can remain the same, where the ciphertext **208***a* can be decrypted by step **206** and ciphertext **208***b* remains encrypted in the resulting profile **107***d* from a step **206**.

A module **101** can use an eUICC **107** to decrypt the second portion or ciphertext **208***b* in a profile **107***d* using a step **207**. Before a step **207**, a module **101** can take the previous steps **205** and **206** in order to record a profile **107***d* with an eUICC **107**. Before a step **207**, module **101** can receive a symmetric key **127**, where the symmetric key **127** can comprise a symmetric ciphering key. In exemplary embodiments, module **101** can receive the symmetric key **127** from a mobile network operator **104** after a user associated with module **101** performs a separate authentication step **308***b* as depicted and described in connection with FIG. **3** and FIG. **4** below. By a mobile network operator **104** only sending symmetric key **127** after the second authentication step **308***b*, the second key K **204** can remain secured, while a user is allowed to access the wireless network **102** (perhaps temporarily or with other constraints such as limiting access to the Internet but allowing emergency calls) using the first key K **203**.

In this manner and by using a second, separate authentication step **308***b* before sending symmetric key **127**, the decryption of network access credentials such as the second key K **204** can remain in the control of a mobile network operator **104**, thereby increasing the security of exemplary systems illustrated herein, such as systems **100**, **300**, and **500**. By ciphering the second key K **204** with symmetric key **127**, security over conventional technology for an eUICC can be increased for both a user and a mobile network operator. With conventional technology for an eUICC, where only the first key K **203** is used for authentication and ciphering of data between module **101** and wireless network **102**, the decryption of the first key K **203** can be outside the control of a mobile network operator **104**. With conventional technology contemplated for an eUICC, an end user outside the control or a contractual relationship with mobile network operator **104**, including possibly fraudulent users or imposters of valid users, could (i) take steps to obtain a plaintext first key K **203** and associated plaintext first network module identity **202** and (ii) use the credentials to fraudulently access the wireless network **102**. In contrast and as contemplated herein, the symmetric key **127** to decrypt the second key K **204***a* can preferably be only made available to users who authenticate with mobile network operator using a step **308***b* as described below (or an equivalent step or related commercial arrangements between a user and a mobile network operator **104**).

In exemplary embodiments, use of two sets of network access credentials comprising at least the first key K **203** and the second key K **204** allows a user with an eUICC profile **107***c* to connect to the wireless network **102** using the first key K **203**, such that the module **101** can have connectivity to the mobile network operator **104** via the wireless network **102** (and also IP network **111**) in order to conduct separate authentication steps **308***b*. The security steps for a mobile network operator **104** to control the decryption of the first key K **203** can be lowered (thus making the distribution of profile **107***c* simpler, less costly, and less complex), while a mobile network operator **104** can retain full control over the decryption of the second key K **204***a* into a usable second key K **204** associated with the second network module identity **209**.

The use of a step **207** by module **101** with an eUICC is also depicted and described in connection with FIG. **2***c* and FIG. **3** below. A module **101** can record profile **107***d* with ciphertext **208***b* for a period of time, and the step **207** can be taken (i) after recording profile **107***d*, and (ii) before module **101** authenticates with a wireless network **102** using the second key K **204**. A step **207** can covert the ciphertext **208***b* into plaintext, such that an eUICC **107** can read the values in order to authenticate with a wireless network **102** using the second key K **204**.

A step **207** can convert the encrypted second key K **204***a* into a plaintext key K **204**. As illustrated in FIG. **2***a*, a step **207** can also convert the encrypted network module identity **209***a* into a plaintext network module identity **209** as well. As discussed above in this FIG. **2***a*, the network module **209** can be optionally omitted from a step **207**, such that the plaintext network module identity **209** could be recorded in a profile **107***d*, and the plaintext network module identity **209** could be included in the first portion, or ciphertext **208***a*, in a profile **107***c*. In another embodiment, the second network module identity **209** can be received by module **101** from wireless network **102** after the module authenticates using the first key K **203**. Although not illustrated in FIG. **2***a*, an eUICC **107** can continue to record the plaintext network module identity **209** and plaintext second key K **204** in an eUICC profile after the second key K **204** is decrypted using the symmetric key **127**. The module **101** can record the second key K **204** in a protected memory address within ROM **101***c* or nonvolatile memory **101***w*.

For embodiments where the first key K **203** is recorded within a ciphertext **208***c* in a profile **107***d* after a step **206**, the first key K **203** can be converted from ciphertext **208***c* into a plaintext first key K **203** using a key deciphering step **217** as depicted and described in connection with FIG. **2***e* below. The key deciphering step **217** could use an asymmetric ciphering algorithm **219** with input of (i) ciphertext **208***c* and (ii) the eUICC private key **215** in order to output the plaintext first key K **203**. As described above, the use of a ciphertext **208***c* can be optionally omitted, and the first key K **203** could be recorded as plaintext in a profile **107***d*. In this case, a step **217** for data in profile **107***d* can be omitted, and thus step **217** with ciphertext **209***c* is depicted in FIG. **2***a* with a dashed line.

Although the first key K **203** and the second key K **204***a* are depicted in FIG. **2***a* as recorded within an eUICC profile **107***c* or eUICC profile **107***d*, the first key K **203** and the second key K **204***a* can be (i) recorded in a nonvolatile memory of module **101**, such as, but not limited to, a flash memory **101***w*, and (ii) without the use of an eUICC **107**. In other words, embodiments contemplated herein can be used without an eUICC **107**, such that (i) a module **101** can use a first key K **203** to authenticated with a wireless network **102**, (ii) after authentication with the first key K **203**, the module can receive a symmetric key **127** to decrypt the second key K **204***a* into second key K **204**, and (iii) the module can authenticate with the wireless network **102** using the second key K **204**. In other words, an eUICC **107**

Petitioner Samsung Ex-1004, 0037

can be omitted and a module **101** can perform the same steps for (i) receiving encrypted network access credentials and (ii) decrypting the encrypted network access credentials without requiring the use of an eUICC **107**.

In embodiments where a module **101** does not include an eUICC **107**, the module can record the first key K **203** and the encrypted second key K **204***a* in a file or memory address without requiring the use of a profile **107***c* and **107***d*. For example, the first key K **203** could be recorded in a regular, physical UICC, and the second key K **204***a* could also be recorded in a regular, physical UICC as well. The regular, physical UICC could (i) receive the symmetric key **127** and decrypt the second key K **204***a*, and (ii) subsequently record the decrypted second key K **204**. The module **101** and UICC could use the decrypted second key K **204** to authenticate with the wireless network **102** where the first key K **203** was previously used. Other possibilities exist as well for a module **101** to (i) use a first key K **203** and an encrypted second key K **204***a* without departing from the scope of the present invention.

FIG. **2***b*

FIG. **2***b* is a graphical illustration for ciphering and deciphering a profile using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments. An eUICC profile **107***d* can be (i) ciphered using a profile ciphering algorithm **210** and (ii) deciphered with a profile deciphering algorithm **206**. Both the profile ciphering algorithm **210** and the profile deciphering algorithm **206** can include a symmetric ciphering algorithm **211** and the use of an eUICC profile key **107***b*. An eUICC subscription manager **109**, or another node outside a module **101** as illustrated in FIG. **1***a*, can use a profile ciphering algorithm **210** to encrypt an eUICC profile **107***c*. The processing and computational steps for performing a profile ciphering algorithm **210** could be conducted on a server associated with the eUICC subscription manager **109**. The server associated with the eUICC subscription manager **109** can be similar to a server **105** illustrated in FIG. **1***a*, with the difference being the server associated with the eUICC subscription manager **109** can be co-located, associated with, or under the operational control of an eUICC subscription manager **109**. Data for an eUICC profile **107***d* used in a profile ciphering algorithm **210** can comprise the exemplary data illustrated for a profile **107***d* in FIG. **2***a* above, and an eUICC subscription manager **109** could receive the data for the profile **107***d* from a mobile network operator **104**. The mobile network operator **104** could process, generate, or derive the exemplary values in a profile **107***d* that can include the network parameters **201**, the first network module identity **202**, the first key K **203**, and the ciphertext **208***b*. As contemplated herein, the MNO **104** could also function as a eUICC subscription manager **109**, and thus in embodiments the profile **107***d* could be generated by a MNO **104** as well.

Symmetric ciphering algorithm **211** in a profile ciphering algorithm **210** can utilize a key such as an eUICC profile key **107***b* to encrypt or cipher data. Examples of symmetric ciphers for a symmetric ciphering algorithm **210** include (i) an Advanced Encryption Standard (AES) cipher, as specified in Federal Information Processing Standards (FIPS) Publication 197, and (ii) Triple Data Encryption Standard (Triple DES), as described in NIST Special Publication 800-67 Revision 1, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (Revised January 2012)". Other symmetric ciphers and/or combinations of symmetric ciphers can be utilized as well for a symmetric ciphering algorithm **210** without departing from the scope of the present invention. In general, a symmetric ciphering algorithm **211** in a profile ciphering algorithm **210** (and other steps for symmetric ciphering contemplated herein) can accept input of plaintext and a key, and using the two sets of input data, the symmetric ciphering algorithm **211** can perform multiple rounds of mixing, substituting, rotating, and/or perform XOR functions with the input in order to produce a ciphertext output. Although not illustrated in FIG. **2***b* and FIG. **2***c*, a set of cryptographic parameters can also be input into symmetric ciphering algorithms **211** in order to specify parameters or configurations of the symmetric ciphering algorithm **211**, such as, but not limited to, the selection of 128, 192, or 256 bits with AES.

A cipher key used with a symmetric ciphering algorithm **211**, such as, but not limited to, the exemplary eUICC profile key **107***b* can comprise a random or pseudo-random number, with an appropriate length or number of bits for the symmetric ciphering algorithm **211**. The exemplary eUICC profile key **107***b* for use in a profile ciphering algorithm **210** could be shared between an eUICC subscription manager **109** and an eUICC **107** in a module **101** in several different ways. The eUICC profile key **107***b* could be recorded in or with the eUICC **107** upon manufacturing of module **101**. The eUICC profile key **107***b* could be securely received by a module **101** using a wireless network **102** from the eUICC subscription manager **109** before the module **101** performs a step that includes a profile deciphering algorithm **206**. An encrypted eUICC profile key **107***b* could be received by module **101** and then decrypted by module **101** using an asymmetric ciphering algorithm **219** as depicted and described in connection with FIG. **2***e* below. The eUICC profile key **107***b* could also be derived by a module **101** and an eUICC subscription manager **109** (or another server performing the steps in a profile ciphering algorithm **210**) using a key exchange such as, but not limited to, a Diffie-Hellman key exchange or an Elliptic Curve Diffie-Hellman key exchange.

Other possibilities exist as well for a module **101** and an eUICC subscription manager **109** (or another server performing the steps in a profile ciphering algorithm **210**) to securely share a eUICC profile key **107***b* without departing from the scope of the present invention. In addition, although a single eUICC profile key **107***b* is illustrated in FIG. **2***b*, an eUICC subscription manager **109** and an eUICC **107** could use multiple eUICC profile keys **107***b*, including embodiments where a first encrypted eUICC profile **107***c* is associated with a first eUICC profile key **107***b* and a second encrypted eUICC profile **107***c* is associated with a second eUICC profile key **107***b*. Further, each encrypted eUICC profile **107***c* could be uniquely associated with a different eUICC profile key **107***b*. Each of the different eUICC profile keys **107***b* could be securely transferred between the eUICC **107** and the eUICC subscription manager **109** using either (i) asymmetric ciphering **219** as illustrated in FIG. **2***e* below, or (ii) a key exchange, as depicted and described in connection with step **303** of FIG. **3** below.

With a profile ciphering algorithm **210**, the symmetric ciphering algorithm **211** can accept input of (i) the eUICC profile key **107***b*, and (ii) and an eUICC profile **107***d* plus an optional security token **212**, in order to output an encrypted eUICC profile **107***c*. The encrypted eUICC profile **107***c* can be reasonably secured, such that deciphering the profile **107***c* without the eUICC profile key **107***b* would be infeasible. After ciphering with a symmetric ciphering algorithm **211**, deciphering the ciphertext without the cipher key would require extensive dedicated computational resources such as hundreds of servers or more for many years or longer. The optional security token **212** can include a string or number

Petitioner Samsung Ex-1004, 0038

in order to enhance the security of the ciphertext output by a symmetric ciphering algorithm **211**. The optional security token **211** could comprise a random number or other value, such that the input and output of a symmetric ciphering algorithm **211** is properly padded, where the length of input and output are appropriate for the symmetric ciphering algorithm.

Although the input of eUICC profile **107***d* is depicted in FIG. **2***b* with a label of "plaintext", the eUICC profile **107***d* in a profile ciphering algorithm **210**, the "plaintext" eUICC profile **107***d* can include encrypted data such as ciphertext **208***b*, where ciphertext **208***b* can include encrypted data ciphered with a different key than eUICC profile key **107***b*. In other words, a profile **107***c* can include multiple layers of ciphering, where different layers use different cipher keys, and the exemplary a profile ciphering algorithm **210** with the eUICC profile key **107***b* can be used to encrypt the ciphertext **208***a* illustrated in FIG. **2***a* above. As noted above with FIG. **2***a*, ciphertext **208***b* can be either (i) included inside ciphertext **208***a*, or (ii) remain external to ciphertext **208***a*.

After a server associated with an eUICC subscription manager **109** generates the output of an encrypted profile **107***c* from a profile ciphering algorithm **210**, the encrypted profile **107***c* can be transferred to module **101** through either unsecured channels, or channels that are not under the full control of an eUICC subscription manager **109** or a mobile network operator **104** associated with the profile **107***c*. The module **101** can receive the profile **107***c* through an IP network **111**, including using the public Internet, or a manufacturer, distributor, technician, or end user could load the profile **107***c* into the module (such as, but not limited to, using a USB interface **101***v*). This initial loading of profile **107***c* by a manufacturer, distributor, technician, or end user may be required for the first use or startup of a module **101**, but then module **101** may preferably receive additional or subsequent profiles **107***c* at later times using IP network **111** and other automated, electronic means using a network including a wireless network **102**.

A module **101** or an eUICC **107** within module **101** can process the encrypted profile **107***c* using a profile deciphering algorithm **206** as depicted in FIG. **2***b* and also depicted and described in FIG. **2***a*. Note that the module **101** or eUICC **107** could record the encrypted profile **107***c* for a period of time, and take the steps to decrypt the profile **107***c* in a profile deciphering algorithm **206** after receiving the eUICC profile key **107***b* associated with the profile **107***c*. Or the eUICC profile key **107***b* could be recorded in a module **101** or with an eUICC **107** before profile **107***c* is received, and the steps for a profile deciphering algorithm **206** could be performed after the receipt of an instruction from an eUICC subscription manager **109** or at a specified time or under specified conditions (such as a module **101** needing or preferring to connect to a wireless network **102** for the first time). An exemplary use and sequence for a profile deciphering algorithm **206** is depicted and described in connection with FIG. **3** below. Other possibilities exist as well for the time that a module **101** or an eUICC **107** can process a profile deciphering algorithm **206** without departing from the scope of the present invention. As contemplated herein, the use of the term "step **206**" can refer to the use of a profile deciphering algorithm **206**, and a "step **207**" can refer to the use of a key K deciphering algorithm **207**, etc.

A profile deciphering algorithm **206** can include a symmetric ciphering algorithm **211**. The symmetric ciphering algorithm **211** can be equivalent to or the same as the symmetric ciphering algorithm **211** in a profile ciphering algorithm **210** operated by a server and as described above. The symmetric ciphering algorithm **211** can accept input of the eUICC profile key **107***b* as a cipher key. The module **101** or eUICC **107** could securely receive the eUICC profile key **107***b* using the steps described above in connection with a profile ciphering algorithm **210**. An exemplary transfer or key exchange for module **101** to receive eUICC profile key **107***b* is also described in FIG. **2***e* and FIG. **3** below. The symmetric ciphering algorithm **211** in a profile deciphering algorithm **206** can also accept input of the encrypted eUICC profile **107***c*, which could comprise ciphertext **208***a*.

The symmetric ciphering algorithm **211** in a profile deciphering algorithm **206** can decrypt the ciphertext **208***a* in order to output the profile **107***d*, where the ciphertext **208***a* is converted to plaintext. Ciphertext **208***b* in a profile **107***c* can remain encrypted using the symmetric key **127** after a profile deciphering algorithm **206**. In other words, the profile deciphering algorithm **206** can convert a portion of the profile **107***c* into plaintext, where the portion comprises ciphertext **208***a*. As depicted in FIG. **2***a* above, exemplary plaintext in a profile **107***d* resulting from a profile deciphering algorithm **206** can include a first network module identity **202** and the first key K **203**. The resulting plaintext from a profile deciphering algorithm **206** can also optionally include a security token **212**. Security token **212** could comprise the string or value also optionally input into the symmetric ciphering algorithm **211** in a profile ciphering algorithm **210**. The security token **212** can include a padding value to make the length of the security token **212** and profile **107***d* a desired value for the symmetric ciphering algorithm **211** or other requirements such as making the encrypted profile **107***c* a desired length.

FIG. **2***c*

FIG. **2***c* is a graphical illustration for ciphering and deciphering a key K using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments. A second key K **204***a* can be (i) ciphered using a key K ciphering algorithm **213** and (ii) deciphered with a key K deciphering algorithm **207**. Both the key K ciphering algorithm **213** and the key K deciphering algorithm **207** can include a symmetric ciphering algorithm **211** and the use of a symmetric key **127**. A mobile network operator **104** can use a key K ciphering algorithm **213** to encrypt the second key K **204***a*. The processing and computational steps for performing a key K ciphering algorithm **213** could be conducted on a server associated with the mobile network operator **104** such as a server **105** illustrated in FIG. **1***a*. Other possibilities exist as well for the location or association of a computer to process a key K ciphering algorithm **213** without departing from the scope of the present invention.

A key K ciphering algorithm **213** can include a symmetric ciphering algorithm **211**. The symmetric ciphering algorithm **211** can similar to the symmetric ciphering algorithm **211** as depicted and described in connection with FIG. **2***b* above. A symmetric ciphering algorithm **211** can include a collection of different symmetric ciphers, such that a first symmetric cipher comprising the AES cipher could be used in a FIG. **2***b*, while a different symmetric cipher could be used in a FIG. **2***c*. Or, the same algorithm within symmetric ciphering algorithm **211** can be used in a symmetric ciphering algorithm **211** in FIG. **2***b* and FIG. **2***c*. The symmetric ciphering algorithm **211** in a key K ciphering algorithm **213** can accept input of a symmetric key **127** and plaintext in the form of a second key K **204**. The second key K **204** could represent a random number, such as, but not limited to, an exemplary 128 random number currently used as a shared secret key K in standard LTE networks and a different length for second

Petitioner Samsung Ex-1004, 0039

key K **204** could be used as well. The second key K **204** could be derived or processed by the function of an authentication center with a home subscriber server (HSS). Although not illustrated in FIG. **2***c*, but as illustrated in FIG. **2***a*, the plaintext as input into a symmetric ciphering algorithm **211** can also include a second network module identity **209**. The input into a symmetric ciphering algorithm **211** for a key K ciphering algorithm **213** can also include a number, value, or string for a security token **212**. The use of a security token **212** is depicted and described in connection with FIG. **2***b* above. Thus, a mobile network operator **104** could also use a key K ciphering algorithm **213** to encrypt other data in addition to a second key K **204**.

The symmetric key **127** input into a symmetric ciphering algorithm **211** in a key K ciphering algorithm **213** can comprise a random number processed or generated by a server **105**, where the server **105** is associated with a mobile network operator **104**. The server processing or deriving a symmetric key **127** can comprise or be associated with an HSS for an LTE or LTE advanced network. As illustrated in FIG. **2***c*, the symmetric key **127** can comprise a cipher key for the symmetric ciphering algorithm **211**. A cipher key used with a symmetric ciphering algorithm **211**, such as, but not limited to, the exemplary symmetric key **127** can comprise a random or pseudo-random number, with an appropriate length or number of bits for the symmetric ciphering algorithm **211** in a key K ciphering algorithm **213**. Using the input of the symmetric key **127** and the plaintext second key K **204**, the symmetric ciphering algorithm **211** could output an encrypted second key K **204***a*. As illustrated in FIG. **2***c* and FIG. **2***a* above, the encrypted second key K **204***a* could be included in ciphertext **208***b*. The symmetric ciphering algorithm **211** in a key K ciphering algorithm **213** may also optionally include a security token **212**, as illustrated.

After processing the ciphertext **208***b*, the mobile network operator **104** can either (i) include the ciphertext **208***b* in a profile **107***d* and send the profile **107***d* to an eUICC subscription manager **109**, or (ii) send the ciphertext **208***b* directly an eUICC subscription manager **109** for the eUICC subscription manager **109** to include the ciphertext **208***b* in a profile **107***d*. Ciphertext **208***b* could be recorded in or with an eUICC profile **107***d*, where an eUICC subscription manager **109**, or another server associated with an eUICC subscription manager **109** can subsequently encrypt the eUICC profile **107***d* using a profile ciphering algorithm **210** depicted and described in connection with FIG. **2***b* above. Other possibilities exist as well for the timing an sequence of steps for transferring and recording a ciphertext **208***b* output from a key K ciphering algorithm **213** without departing from the scope of the present invention. After profile **107***d* with ciphertext **208***b* has been created, the profile **107***d* can be ciphered with a profile ciphering algorithm **210** to create an encrypted profile **107***c*, as illustrated in FIG. **2***b* above.

The exemplary symmetric key **127** for use in a key K ciphering algorithm **213** could be shared between a module **101** with an eUICC **107** and the mobile network operator **104** in several different ways. The symmetric key **127** could be sent from the mobile network operator **104** (possibly using a server **105**) to a module **101** after (i) the module properly authenticates with the mobile network operator **104** and/or a wireless network **102** associated with the MNO **104** using the first key K **203**, and (ii) a user **113** associated with the module **101** authenticates with the MNO **104**. Note that if MNO **104** sends the symmetric key **127** to module **101** after module **101** uses the first key K **203** to authenticate, then the ciphering or encryption of the channel used to send the symmetric key K **127** can be within the control of MNO **104** (whereas the communications channel and ciphering keys used to send encrypted profile **107***c* may be outside the control of MNO **104**). The symmetric key K **127** could also be derived by a module **101** and an MNO **104** using a key exchange, where the symmetric key K **127** could be derived using a RAND **118** value received by the module **101** after authenticating with the first key K **203**, where the module **101** and/or eUICC **107** derives the symmetric key K **127** using the RAND **118** value and the first key K **203**. Other possibilities exist as well for a module **101** and a mobile network operator **104** to securely share a symmetric key **127** without departing from the scope of the present invention.

A module **101** or an eUICC **107** within module **101** can process the ciphertext **208***b* using a key K deciphering algorithm **207** as depicted in FIG. **2***c*. Note that the module **101** or eUICC **107** could record the ciphertext **208***b* for a period of time, and take the steps to decrypt the ciphertext **208***b* with a key K deciphering algorithm **207** after receiving or deriving the symmetric key **127**. Or the symmetric key **127** could be recorded in a module **101** or with an eUICC **107** before ciphertext **208***b* is decrypted, and the steps for a key K deciphering algorithm **207** could be performed after the receipt of an instruction from the MNO **104** to decrypt the second key K **204***a*. An exemplary use and sequence for a key K deciphering algorithm **207** is depicted and described in connection with FIG. **3** below. Other possibilities exist as well for the time that a module **101** or an eUICC **107** can process a key K deciphering algorithm **207** without departing from the scope of the present invention.

A key K deciphering algorithm **207** can include a symmetric ciphering algorithm **211**. The symmetric ciphering algorithm **211** can be equivalent to or the same as the symmetric ciphering algorithm **211** in a key K ciphering algorithm **213** performed by an MNO **104** and as described in this FIG. **2***c* above. The symmetric ciphering algorithm **211** can accept input of the symmetric key **127** as a cipher key. The module **101** or eUICC **107** could securely receive or derived the symmetric key **127** using the steps described above in connection with a key K ciphering algorithm **213**. The symmetric ciphering algorithm **211** in a key K deciphering algorithm **207** can also accept input of the encrypted key K **204***a*, which could comprise ciphertext **208***b*. Additional data, such as, but not limited to a second module identity **209***a* could optionally be included within ciphertext **208***b*.

The symmetric ciphering algorithm **211** in a key K deciphering algorithm **207** can decrypt the ciphertext **208***b* in order to output the plaintext second key K **204**, such that the ciphertext **208***b* is converted to plaintext. The resulting plaintext from a key K deciphering algorithm **207** can also optionally include a security token **212**. Security token **212** could comprise the string or value also optionally input into the symmetric ciphering algorithm **211** in a key K ciphering algorithm **213**. The security token **212** can include a padding value to make the length of the security token **212** and second key K **204***a* a desired value for the symmetric ciphering algorithm **211** or other requirements such as making the ciphertext **208***b* a desired length.

FIG. **2***d*

FIG. **2***d* is a graphical illustration of a public key and a private key for an eUICC, in accordance with exemplary embodiments. An eUICC **107** within a module **101** can include an eUICC private key **215**, which can be associated with an eUICC public key **214**. The eUICC private key **215** and eUICC public key **214** can comprise a public key infrastructure (PKI) key pair for eUICC **107**. The eUICC

Petitioner Samsung Ex-1004, 0040

subscription manager **109** can record the eUICC public key **214** along with an eUICC identity **107***a*, such that the eUICC subscription manager **109** can properly associate one of a plurality of eUICC public keys **214** with the proper eUICC **107**. Although not illustrated in FIG. **2***d*, an eUICC subscription manager **109** could record the eUICC public key **214** and an associated eUICC identity **107***a* in a database. The use of an eUICC ID **107***a* is also depicted and described in connection with FIG. **3** below.

The eUICC private key **215** and eUICC public key **214** could be processed using RSA algorithms or elliptic curve cryptography (ECC) algorithms, and other possibilities exist as well for the format of PKI keys without departing from the scope of the present invention. An ECC key length of 283 bits provides security similar to an RSA key length of approximately 2048 bits, and in an exemplary embodiment the eUICC key pair can utilize an ECC algorithm, although an RSA algorithm or other algorithms for PKI keys could also be utilized by an eUICC **107**. The eUICC private key **215** can be processed or derived using a random number. eUICC public key **214** can comprise a key recorded in an X.509 certificate that also includes a module identity **110** and/or eUICC identity **107***a*, although the use of an X.509 certificate with an eUICC public key **214** is not required. The eUICC public key **214** in the form of an X.509 certificate can optionally be signed by a certificate authority. The keys can support standards such as, but not limited to, the International Organization for Standardization (ISO) ISO/IEC 9594 series of standards (herein incorporated by reference) and the Internet Engineering Task Force (IETF) RFC 5280 titled "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (herein incorporated by reference), including future updates to these standards.

Several possibilities exist for the source of an eUICC private key **215** and eUICC public key **214**. The eUICC private key **215** and eUICC public key **214** be generated using standard software tools such as, but not limited to, Openssl, libmcrypt, and/or and Crypto++, and other tools to generate public and private keys exist as well. Public and private keys as contemplated herein could be recorded in a file such as, but not limited to, a *.pem file (Privacy-enhanced Electronic Mail), a file formatted according to Basic Encoding Rules (BER), Canonical Encoding Rules (CER), or Distinguished Encoding Rules (DER), or as text or binary file. Other formats for public and private keys may be utilized as well, including proprietary formats. A module **101** could derive the PKI key pair using a set of cryptographic algorithms and a key pair generation algorithm. 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 **101***f* and/or a clock **160** in order to obtain a random number with a high degree of information entropy.

A manufacturer of module **101** or an eUICC subscription manager **109** could also derive the eUICC private key **215** and eUICC public key **214** in a server, and load the eUICC private key **215** into a nonvolatile memory of module **101** before distribution of the module **101**. The manufacturer of module **101** could send or make available the eUICC public key **214** to an eUICC subscription manager **109**. The module **101** could send record the eUICC public key **214** and send the eUICC public key **214** along with the eUICC identity **107***a* (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 **170***c*.

Although FIG. **2***d* illustrates an eUICC private key **215** and eUICC public key **214**, a module **101** could use a PKI key pair associated with module **101** instead of being associated with an eUICC **107** in order to use an asymmetric ciphering algorithm as depicted in FIG. **2***e* below. In other words, a module **101** and an eUICC subscription manager **109** could use a module private key **112***a* and a module public key **112***b* in order to obtain the same functionality of an eUICC private key **215** and an eUICC public key **214**. A module private key **112***a* and a module public key **112***b* for a module **101** could have the same properties and characteristics for an eUICC private key **215** and an eUICC public key **214** as described herein. Other possibilities exist as well for the source or use of a PKI key pair for an eUICC private key **215** and eUICC public key **214** without departing from the scope of the present invention.

In exemplary embodiments, both the eUICC subscription manager **109** and the eUICC **107** can include a set of digital signature algorithms **221**, in order to sign and verify messages between (i) an eUICC **107** and eUICC subscription manager **109**, and (ii) eUICC subscription manger **109** and MNO **104**. Digital signature algorithms **221** can also verify signatures such as, but not limited to, comparing that (i) a first secure hash value received from a sending node matches (ii) a second secure hash value calculated using a recorded public key associated with the sending node. Digital signature algorithms **221** can utilize algorithms in National Institute of Standards (NIST) "FIPS 186-4: Digital Signature Standard", or IETF RFC 6979 titled "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)". The use of ECDSA algorithm within a set of digital signature algorithms **221** may be preferred if keys such as, but not limited to, eUICC private key **215** and eUICC public key **214** are based on elliptic curve cryptography. Digital signature algorithms **221** could also include an RSA digital signature algorithm (DSA) for use with RSA-based public and private keys. Other PKI standards or proprietary techniques for securely generating digital signatures and verifying digital signatures may be utilized as well in digital signature algorithms **221**. As depicted and described in connection with FIG. **3** below, a digital signature algorithm **221** can be used in a step **205** in order to authenticate an eUICC **107** operating in a module **101** with an eUICC subscription manager **109**.

As illustrated in FIG. **2***d*, the eUICC subscription manager **109** may also be associated with an eUICC subscription manager public key **220** and an eUICC subscription manager private key **222**, and the two keys can comprise a PKI key pair for the eUICC subscription manager **109**. The eUICC subscription manager public key **220** and an eUICC subscription manager private key **222** can be formatted and processed by algorithms equivalent or similar to the algorithms and format for the eUICC public key **214** and the eUICC private key **215** described in this FIG. **2***d* above. The eUICC subscription manager public key **220** can optionally be signed by a certificate authority. An eUICC **107** can use the digital signature algorithms **221** and the eUICC subscription manager public key **220** to verify a digital signature from the eUICC subscription manager **109**. Although not illustrated in FIG. **2***d*, the eUICC **107** or module **101** could also record a public key associated with the mobile network operator **104**, and use the public key associated with the mobile network operator **104** to verify a digital signature from the mobile network operator **104** using the digital signature algorithms **221**.

Petitioner Samsung Ex-1004, 0041

FIG. **2***e*

FIG. **2***e* is a graphical illustration for ciphering and deciphering a key for an eUICC using an asymmetric ciphering algorithm using a PKI key pair, in accordance with exemplary embodiments. An eUICC subscription manager **109** could process or calculate a key ciphering algorithm **216** and a module **101** or eUICC **107** could process or calculate a key deciphering algorithm **217**. The eUICC key ciphering algorithm **216** can use an asymmetric ciphering algorithm **219** with an input of (i) an eUICC public key **214** as a cipher key and (ii) the eUICC profile key **107***b* as plaintext in order to output ciphertext of an encrypted eUICC key **218**. The plaintext eUICC profile key **107***b* can comprise a random number of appropriate length for processing a profile ciphering algorithm **210** and profile deciphering algorithm **206** as depicted and described in connection with FIG. **2***b* above. As illustrated in FIG. **2***e*, the input into a key ciphering algorithm **216** could also include an optional security token **212**, where a security token **212** is depicted and described in connection with FIG. **2***b* above.

An asymmetric ciphering algorithm **219** within a key ciphering algorithm **216** and a key deciphering algorithm **217** an comprise an algorithm for utilizing public key infrastructure (PKI) techniques to both (i) encrypt plaintext with a public key and (ii) decrypt plaintext with a private key. Example algorithms within asymmetric ciphering algorithm **219** include an RSA algorithm and an elliptic curve cryptography (ECC) algorithm, and other asymmetric ciphering algorithms could be utilized as well. The use and application of RSA algorithms and cryptography are described within IETF RFC 3447 titled "Public-Key Cryptography Standards (PKCS) #**1**: RSA Cryptography Specifications Version 2.1", herein incorporated by reference, among other published standards for the use of RSA algorithms. The use of an RSA algorithm in an asymmetric ciphering algorithm **219** for encryption and decryption, can also be processed according to the description of the RSA algorithm according to the Wikipedia entry for "RSA (algorithm)" as of Sep. 9, 2013, which is incorporated by reference herein. The use and application of an ECC algorithm for asymmetric ciphering algorithm **219** can conform with algorithms within IETF RFC 6090 titled "Fundamental Elliptic Curve Cryptography Algorithms" (herein incorporated by reference), among other published standards using ECC. Asymmetric ciphering algorithm **219** can also utilize elliptic curve cryptography algorithms for the Wikipedia entry for "Elliptic curve cryptography" as of Sep. 9, 2013, which is incorporated by reference herein.

ECC algorithms (with corresponding ECC-based PKI keys) may utilized for asymmetric ciphering algorithm **219** according to exemplary preferred embodiments in order to maintain high security with smaller key lengths, compared to RSA, thereby helping to comparably reduce the message lengths, radio frequency spectrum utilization, and processing power required by module **101**. RSA algorithms (with corresponding RSA-base PKI keys) for asymmetric ciphering algorithm **219** may be utilized in other embodiments in order to maintain compatibility with deployed or legacy software and systems that supports RSA based keys and algorithms.

After an eUICC subscription manager **109** uses a eUICC key ciphering algorithm **216** to convert a plaintext eUICC profile key **107***b* into a ciphertext as an encrypted eUICC key **218**, the eUICC subscription manager can send the ciphertext to the module **101**. The eUICC subscription manager could send the ciphertext as an encrypted eUICC key **218** to module **101** using an IP network **111**, and the IP network **111** could comprise the public Internet. In this manner, the module **101** can securely receive the encrypted eUICC key **218** in order to perform, process, or calculate a key deciphering algorithm **217**. Third parties with access to the encrypted eUICC key **218** would not feasibly be able to read the plaintext eUICC profile key **107***b*, even with access to the eUICC public key **214**. The module **101** could receive the encrypted eUICC key **218** along with an eUICC profile identity **107***e* in order to determine a profile **107***c* associated with the encrypted eUICC key **218**, where a subsequent step (after deciphering the encrypted eUICC key **218**) could comprise a profile deciphering algorithm **206**. The module **101** could receive the encrypted eUICC key **218** either before or after receiving the profile **107***c*.

After receiving the encrypted eUICC key **218**, the module **101** or eUICC **107** could decrypt the encrypted eUICC key **218** using a key deciphering algorithm **217**. A key deciphering algorithm **217** can include a asymmetric ciphering algorithm **219**. The asymmetric ciphering algorithm **219** can be equivalent to or the same as the asymmetric ciphering algorithm **219** in a key ciphering algorithm **216** operated or processed by an eUICC subscription manager **109** as described in this FIG. **2***e* above. The asymmetric ciphering algorithm **219** in a key deciphering algorithm **217** can accept input of the eUICC private key **215** as a cipher key. The asymmetric ciphering algorithm **219** in a key deciphering algorithm **217** can also accept input of the encrypted eUICC key **218** as a ciphertext. The key deciphering algorithm **217** can use an asymmetric ciphering algorithm **219** with an input of (i) an eUICC private key **215** as a cipher key and (ii) the encrypted eUICC key **218** as ciphertext in order to output plaintext of an eUICC profile key **107***b*. As illustrated in FIG. **2***e*, the plaintext could also optionally include a security token **212**. After processing a plaintext eUICC profile key **107***b* from a key deciphering algorithm **217**, module **101** or eUICC **107** could use the plaintext eUICC profile key **107***b* in order to perform a profile deciphering algorithm **206** as illustrated in FIG. **2***b*.

Although exemplary embodiments can include the use of a key ciphering algorithm **216** and a key deciphering algorithm **217** in order to securely transfer the eUICC profile key **107***b* from an eUICC subscription manager **109** to a module **101**, a key ciphering algorithm **216** and a key deciphering algorithm **217** can be omitted in other exemplary embodiments. For example, if the eUICC subscription manager and module **101** or eUICC **107** support the use of a secure key exchange such as Diffie-Hellman or ECDH, then the eUICC profile key **107***b* could be mutually derived by the two nodes and the encrypted eUICC key **218** would not need to be transferred through an IP network **111** between the two nodes.

In another embodiment, as depicted in FIG. **2***e*, the key ciphering algorithm **216** and key deciphering algorithm **217** may also be used with ciphertext **208***c* with an encrypted first key K **203** and a plaintext of the first key K **203**, if a profile **107***d* includes ciphertext **208***c* with encrypted first key K **203**. In this case, a mobile network operator **104** could perform the key ciphering algorithm **216** with input of (i) the plaintext first key K **203** and (ii) the eUICC public key **214** in order to output ciphertext **208***c*. The ciphertext **208***c* can include the encrypted first key K **203**, although the ciphertext **208***c* could also include other data such as the network parameters **201**. The MNO **104** could send the ciphertext **208***c* (with the encrypted first key K) to the eUICC subscription manager **109** in a step **302***b* in FIG. **3** for inclusion in the profile **107***d* and profile **107***c*. As depicted in FIG. **2***e*, a module **101** or eUICC **107** could perform the key deci-

Petitioner Samsung Ex-1004, 0042

phering algorithm **217** on the ciphertext **208***c* with the first encrypted key K **203** in order to obtain the plaintext first key K **203**. In this manner, the first key K **203** is not shared as plaintext with any entities besides the MNO **104** and a module **101** with the eUICC **107**. In other words, a MNO **104** can use a key ciphering algorithm **216** to prevent the sharing of a plaintext first key K **203** with an eUICC subscription manager **109**.

In addition, although FIG. **2***e* illustrates an eUICC subscription manager as performing the eUICC key ciphering algorithm **216** and the module **101** or eUICC **107** as performing the eUICC key deciphering algorithm **217**, an alternative embodiment contemplates that the eUICC subscription manager **109** performs the eUICC key deciphering algorithm **217** and the module **101** or eUICC **107** performs the eUICC key ciphering algorithm **216**. In this alternative embodiment, the module **101** can (i) derive the eUICC profile key **107***b*, and (ii) send the ciphertext comprising the encrypted eUICC key **218** to the eUICC subscription manager **109**. In this alternative embodiment, the module **101** can (i) use the eUICC subscription manager public key **220** to cipher the derived eUICC profile key **107***b*, (ii) send the encrypted eUICC profile key **107***b* to the eUICC subscription manager **109**, and (iii) the eUICC subscription manager **109** can decrypt the encrypted eUICC profile key **107***b* using the eUICC subscription manager private key **222**. In this alternative embodiment, the eUICC subscription manager **109** could (i) use the eUICC key deciphering algorithm **217** to decrypt the encrypted eUICC key **218** received from the module **101**, and then (ii) subsequent encrypt the profile **107***d* into a profile **107***c* using a profile ciphering algorithm **210** as depicted and described in connection with FIG. **2***b* above.

FIG. **3**

FIG. **3** is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments. System **300** can include an eUICC subscription manager **109**, an IP network **111**, a mobile network operator **104**, a module **101**. A module **101** can include a network application **101***x* and an eUICC **107**. The network application **101***x* can perform the operations for communicating with the wireless network **102** (*i*) at the data-link layer using standards for PLMN networks such as, but not limited to exemplary radio resource control standards within ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification", which is herein incorporated by reference, and (ii) at the network layer using Internet Protocol. Other standards for communication at the data-link layer between a network application **101***x* and a mobile network operator **104** can be utilized as well without departing from the scope of the present invention. The (i) mobile device **101**, using the network application **101***x*, and (ii) the mobile network operator **104** can send and receive data using the wireless network **102** depicted and described in connection with FIG. **1***a*. Although a single module **101** is illustrated in system **300** in FIG. **3**, a system **300** could include a plurality of modules **101**.

The network application **101***x* and the eUICC **107** can send and receive data locally within the module **101** using an operating system **101***h* and/or a system bus **101***d*. The network application **101***x* and the eUICC **107** can send and receive data locally within the module **101** using an eUICC driver **128** as depicted and described in connection with FIG. **1***b* and FIG. **1***e*. The module **101**, using a network application **101***x*, can send and receive data with the eUICC subscription manager **109** using the IP network **111**. As illustrated in FIG. **3**, the module **101** can send and receive data with the eUICC subscription manager **109** in a step **205** using an initial network.

The initial network could comprise a different wireless network **102** than a wireless network **102** (*i*) for the mobile network operator **104**, and (ii) used for a first authentication **304** and a second authentication **310**. In other words, module **101** can send and receive data for an eUICC profile **107***c* through a initial network that is different than the wireless network **102** associated with the mobile network operator **104**. The network application **101***x* could support different standards for wireless networking technologies, such that the different wireless network **102** used to access the eUICC subscription manager **109** could comprise exemplary networks such as WiFi or LTE Advanced, and the network application **101***x* could use LTE to communicated with the mobile network operator **104**. Other possibilities exist as well for the network application **101***x* to support communication with a variety of different networks without departing from the scope of the present invention.

The left side of network application **101***x* in FIG. **3** for communication with the mobile network operator **104** can comprise communication through a radio **101***z* with the wireless network **102**, and the right side of network application **101***x* can comprise internal communication within module **101** as described in the paragraph above and also FIG. **1***e* above. The internal communication between network application **101***x* and eUICC **107** using an operating system **101***h* could comprise either (i) sharing memory **101***e*, where module **101** writes data such as, but not limited to, an exemplary RAND **118** value and eUICC **107** reads the values from the shared memory **101***e*, or (ii) using loopback UDP ports within operating system **101***h*, such that network application **101***x* sends a UDP datagram with the RAND **118** value using a first UPD loopback port, and the eUICC **107** receives the UDP datagram with the RAND **118** value using a second UDP loopback port. For an operating system **101***h* within module **101** using IPv4 addresses, the addresses used for the UDP loopback ports could comprise addresses in the range of the 127.0.0.0/8 address block. For an operating system **101***h* within module **101** using IPV6 addresses, the addresses used for the UDP loopback ports could comprise an :1 address. In another embodiment illustrated in FIG. **1***f* above, the eUICC **107** can communicate with the MNO **104** directly for embodiments where the eUICC **107** includes an IP address **106***c*.

At a step **301**, a module **101** can record an eUICC identity **107***a*, an address **109***a* of an eUICC subscription manager **109**, and an eUICC private key **215** associated with the eUICC **107**. A manufacturer, distributor, technician, end user, or installer of module **101** could record the data for a step **301** in module **101**, or the data could be downloaded or accessed separately via an IP network **111**, including the public Internet. Other data could be included in a step **301** as well, such as, but not limited to, the software or firmware comprising the eUICC **107**, an eUICC profile key **107***b*, an eUICC public key **214**, an eUICC subscription manager public key **220**, an eUICC driver **128**, an initial profile **107***d* or **107***c*, and policy rules for allowing access to the profiles, and other additional data could be included in a step **301** as well. Additional optional data for recording with an eUICC **107** in a step **301** are depicted on the second line of step **301** in FIG. **3**.

In an exemplary embodiment, a manufacturer of module **101** records the exemplary data for an eUICC **107** in a step **301**, such that a module **101** can being operations and

Petitioner Samsung Ex-1004, 0043

connecting to an initial wireless network **102** upon power-up in order to establish initial communications, including allowing the communication with the eUICC subscription manager **109** through the initial wireless network **102**. As noted above in this FIG. **3**, an initial wireless network **102** used for the eUICC **107** to access the eUICC subscription manager **109** can be different than the wireless network **102** used to access the mobile network operator **104**. The address **109***a* of an eUICC subscription manager **109** could comprise either an IP address or a domain name, and in an exemplary embodiment the address **109***a* comprises a domain name and the module **101** can query for the IP address associated with the domain name for address **109***a* via either a domain name system (DNS) query or a secured DNS query (DNSSEC). A module **101** can connect with an initial wireless network **102** (different than the depicted wireless network **102** in FIG. **3**) after a step **301** in order to communicate with an eUICC subscription manager **109**.

At a step **302***a*, an eUICC subscription manager **109** could record data for the eUICC **107**. The data could include (i) an eUICC identity **107***a*, (ii) a profile **107***c*, (iii) an eUICC public key **214**, (iv) an eUICC subscription manager public key **220** and private key **222**, (v) an eUICC profile key **107***b* with an associated eUICC profile identity **107***e*, (vii) a module identity **110** (for embodiments where the module identity **110** for the eUICC **107** is known before the eUICC **107** sends and receives data with the eUICC subscription manager **109**), (viii) and parameters for a symmetric ciphering algorithm **211** and an asymmetric ciphering algorithm **219** used by the eUICC **107**. The parameters for a symmetric ciphering algorithm **211** and an asymmetric ciphering algorithm **219** used by the eUICC **107** could specify the ciphers used, such as (i) selecting an exemplary 128 or 192 bit keys for use with an AES cipher for a symmetric ciphering algorithm **211** used with a eUICC **107** and eUICC identity **107***a*, and (ii) selecting an exemplary elliptic curve or RSA algorithm for use with an asymmetric ciphering algorithm **219**. The eUICC subscription manager **109** could also record related data for the operation of eUICC **107** with eUICC subscription manager **109** in a step **302***a*.

At a step **302***a*, the eUICC subscription manager **109** could receive the profile **107***d* from the mobile network operator **104**, and an exemplary profile **107***d* is depicted and described in connection with FIG. **2***a*. Or, eUICC subscription manager **109** could receive a subset of data for the exemplary profile **107***d* from the MNO **104** in a step **302***a* without receiving the entire profile **107***d*. As one example, the MNO **104** may not know the eUICC profile identity **107***e* for the eUICC profile **107***d*, and thus the MNO **104** may not send the complete profile **107***d* but the MNO **104** could send data for the profile **107***d* to the eUICC subscription manager **109** in a step **302***a*. In an exemplary embodiment, the eUICC subscription manager **109** could receive a subset of data for the profile **107***d* using the IP network **111** over a secured link or connection to the MNO **104**. The profile **107***d* in a step **302***a* could include both ciphertext **208***b* and plaintext of a set of network parameters **201**, a first network module identity **202**, and a first key K **203**. As depicted and described in connection with FIG. **2***a*, the ciphertext **208***b* could comprise an encrypted second key K **204***a*. The ciphertext **208***b* could also include the second network module identity **209***a*. In an exemplary embodiment, the plaintext first key K **203** could be optionally omitted from being received from an MNO **104** in a step **302***a*, and the eUICC subscription manager **109** can receive the first key K **203** in the form of a ciphertext **208***c* below in a step **302***b*. The eUICC subscription manager **109** could use a server or a plurality of servers similar to a server **105** in order to take the processing and communication steps described herein for an eUICC subscription manager **109** in this step **302***a* and also additional steps for an eUICC subscription manager **109** described throughout FIG. **3**.

After a module **101** powers up and established connectivity with the IP network **111**, an eUICC **107** operating in a module **101** could then perform a step **205** in order to receive an eUICC profile **107***c* using the IP network **111**. The use and operation of a step **205** is also depicted and described in connection with FIG. **2***a* above. In a step **205**, an eUICC **107** could send an eUICC identity **107***a* to the eUICC subscription manager **109**. The module **101** could use a network application **101***x* to send the eUICC identity **107***a*, such as the network application **101***x* writing data with the eUICC identity **107***a* to a physical interface **101***a*, and the physical interface **101***a* could include a radio **101***z*. Or, using the exemplary embodiment illustrated in FIG. **1***f* above, the eUICC **107** could be associated with an IP address **106***c*, and the eUICC **107** could send the eUICC identity **107***a* to the eUICC subscription manager **109** without using a separate network application **101***x* associated with the wireless network **102**. During a step **205** for a module **101** or eUICC **107**, an eUICC subscription manager **109** could receive the eUICC identity **107***a* and perform a step **302***b*. In an exemplary embodiment, both a module identity **110** and an eUICC identity **107***a* could be sent by an eUICC **107** or a module **101** in a step **205**. Or, the eUICC identity **107***a* could comprise a module identity **110**, and the module identity **110** could be sent in a step **205**. Other possibilities exist as well for identifying a module **101** or an eUICC **107** with an eUICC subscription manager **109** without departing from the scope of the present invention.

In an exemplary embodiment, a message with the eUICC identity **107***a* in a step **205** could include a digital signature, where the digital signature is processed using (i) the eUICC private key **215** recorded in a step **301** and (ii) a digital signature algorithm **221**. The message with the eUICC identity **107***a* and a digital signature in a step **205** could preferably include a random number or string, including a nonce or a "number used once" such as, but not limited to, an exemplary security token **212** in order to prevent replay attacks.

An eUICC subscription manager **109** can take several actions in a step **302***b* after receiving an identity for the eUICC **107** or module **101**. A first action in a step **302***b* could comprise authenticating an eUICC **107** or a module **101** based on the eUICC identity **107***a* received in the message. In a step **302***b*, eUICC subscription manager **109** can authenticate the message with eUICC identity **107***a* according to message digest, or using the eUICC profile key **107***b* which could be recorded in the eUICC **107** in a step **301** above. In addition, the eUICC subscription manager could authenticate using a digital signature algorithm **221**, where the message with the eUICC identity **107***a* could include a digital signature, as described in the paragraph above.

Both the eUICC **107** and the eUICC subscription manager **109** could use the eUICC profile key **107***b* as a cipher key with a symmetric ciphering algorithm **211** to encrypt/decrypt data sent with the eUICC identity **107***a*, where the successful encryption and decryption of data with eUICC identity **107***a* using the eUICC profile key **107***b* on both ends could be confirmation that the eUICC **107** or module **101** is authenticated, since both parties would only be able to mutually successfully encrypt and decrypt by sharing the same eUICC profile key **107***b*. In another embodiment, the eUICC profile key **107***b* could be used as a private key with a digital

Petitioner Samsung Ex-1004, 0044

signature algorithm **211** (instead of the eUICC private key **215**), in order for the eUICC **107** with the eUICC **107***a* to be authenticated. For embodiments where the module **101** with the eUICC **107** sends a digital signature with the eUICC identity **107***a*, the eUICC subscription manager **109** could use the eUICC identity **107***a* to select the eUICC public key **214** or eUICC profile key **107***b* from a database. In this manner, the eUICC subscription manager **109** could communicate with a plurality of eUICCs **107** and select the appropriate keys using the eUICC identity **107***a*.

A second action in a step **302***b* could comprise the eUICC subscription manager **109** authenticating with an eUICC **107** or a module **101**. The eUICC subscription manager **109** could also authenticate with an eUICC **107** at a step **302***b* within a step **205**, such that eUICC **107** can confirm an identity of the eUICC subscription manager **109**, using any of the same or equivalent steps described in the paragraph above for an eUICC **107** to authenticate with an eUICC subscription manager **109**. The eUICC subscription manager **109** could send the eUICC **107** a digital signature processed using a digital signature algorithm **221** and the eUICC subscription manager private key **222**. The eUICC **107** could verify the digital signature using a eUICC subscription manager public key **220** (which could be recorded with an eUICC **107** in a step **301**). The eUICC **107** could also receive data encrypted with a eUICC profile key **107***b*, and successful decryption of the data by the eUICC **107** using a symmetric ciphering algorithm **211** could confirm the eUICC subscription manager **109** also holds the eUICC profile key **107***b*. Note that a system **300** could include multiple eUICC keys **107***b*, such that a first eUICC profile key **107***b* is used with a step **301** and step **205** in FIG. **3**, and a second eUICC profile key **107***b* could be used with a subsequent step **206** below. Other possibilities exist as well for an eUICC **107** and an eUICC subscription manager **109** to perform a 2-way authentication in a step **205** and a step **302***b* in FIG. **3** without departing from the scope of the present invention.

In another exemplary embodiment, where data received from an MNO **104** does not include a plaintext first key K **203** for inclusion in a profile **107***d*, for a third action in a step **302***b*, the eUICC subscription manager **109** could send the eUICC identity **107***a* (or the module identity **110**) and the eUICC public key **214** to the MNO **104**. In this embodiment, the MNO **104** could also use the key ciphering algorithm **216** depicted and described in connection with FIG. **2***e* above in order to encrypt the first key K **203** with the eUICC public key **214**. The output of an MNO **104** using a key ciphering algorithm **216** could comprise a ciphertext **208***c* of an encrypted first key K **203**. Thus, at a step **302***b* for the embodiment described in this paragraph, the eUICC subscription manager **109** could receive the first key K **203** for a profile **107***d* as ciphertext **208***c* (instead of a plaintext first key K **203** for profile **107***d* in FIG. **2***a*), In this manner, the first key K **203** in a profile **107***d* could be recorded as ciphertext **208***c*, which is also depicted and described as an optional format for the first key K **203** in FIG. **2***a* and FIG. **2***e*.

In an exemplary embodiment, the MNO **104** can send the ciphertext **208***c* only after a user **113** conducts a separate authentication step **308***b* below. In other words, a step **308***b* could also be used concurrently with a step **302***b*, where the step **302***b* includes the receipt of an encrypted first key K **203** in a ciphertext **208***c*. In this manner, the MNO **104** can retain control over the release of an encrypted first key K **203**, such that the first key K **203** in a ciphertext **208***c* is only received by an eUICC subscription manager **109** in a step **302** or a eUICC **107** in a step **205** after a user **113** (associated with the module **101** with the eUICC **107**) authenticates with the MNO **104**. In this embodiment, a separate authentication step **308***b* below can be optionally omitted, and the use of an encrypted second key K **204***a* in ciphertext **208***b* can also be omitted. In this embodiment, a user **113** of the module **101** can access the wireless network **102** of the mobile network operator **104** using the first key K **203** which has been (i) encrypted by the mobile network operator **104** using a key ciphering algorithm **216** in a step **302***b*, and (ii) only available to module **101** or eUICC **107** (or eUICC subscription manager **109**) after a user **113** conducts an authentication step **308***b* with MNO **104**.

After the eUICC subscription manager **109** receives and/or processes all the data for a profile **107***d*, including subsets of data from a MNO **104** described for this step **302***b* above, a fourth action in a step **302***b* could comprise the eUICC subscription manager **109** ciphering a profile **107***d* using a profile ciphering algorithm **210**, in order to convert profile **107***d* with plaintext into a profile **107***c* with ciphertext. Some elements in a profile **107***c* could remain plaintext as well, such as the exemplary profile identity **107***e*. The eUICC subscription manager **109** could use an eUICC profile key **107***b*, where the eUICC profile key **107***b* in a profile ciphering algorithm **210** can be different than an eUICC profile key **107***b* used to authenticate eUICC **107** with eUICC identity **107***a*. Or, the same eUICC profile key **107***b* could be used to both cipher profile **107***d* and authenticate eUICC **107**. Note that this fourth action in a step **302***b* could also take place at an earlier time than at step **302***b*, such that eUICC subscription manager **109** could assemble and cipher the profile **107***d* into a profile **107***c* at an earlier time, such as before receiving the eUICC identity **107***a*, or concurrent with a step **301***a*. Other possibilities exist as well for the timing and sequence for an eUICC subscription manager to assemble and process a profile **107***c* without departing from the scope of the present invention.

After a step **302***b*, the eUICC subscription manager **109** can send the authenticated eUICC **107** a profile **107***c* in a step **205**, as depicted in FIG. **3**. Either the eUICC subscription manger **109** or the eUICC **107** can select the profile **107***c* to be received by the eUICC **107**. In one embodiment, a module **101** can search for radio beacons from base stations **103** for wireless networks **102** surrounding the module **101**, and upon finding new possible wireless network **102** to connect with, the module **101** or eUICC **107** could query or request the eUICC subscription manager **109** for a profile **107***c* associated with a mobile network operator **104** for a radio beacon observed by the module **101**. Commercial business arrangements among the user of module **101**, the eUICC subscription manager **109**, and the mobile network operator **104** can determine the availability of a profile **107***c* for a module **101** with an eUICC **107**.

In another embodiment, the eUICC subscription manager **109** could periodically send the module **101** and/or eUICC **107** new profiles **107***c* as they become available to a user **113** of a module **101** or available to the eUICC subscription manager **109**. In a preferred embodiment, the eUICC subscription manager **109** can send the profile **107***c* to the module **101** using a network application **101***x*, where the network application **101***x* forwards the data to the eUICC **107**. As described above in this FIG. **3**, the network application **101***x* could communicate with the eUICC **107** using the operating system **101***h* as illustrated in FIG. **1***e*, and other possibilities exist as well. Note that eUICC subscription manager **109** sends the profile **107***c*, where the network access credentials (including the first key K **203**) are

Petitioner Samsung Ex-1004, 0045

encrypted with an eUICC profile key **107***b*, and in this manner intermediate nodes on the IP network **111** would not feasibly be able to read the data within the profile **107***c*.

In an exemplary embodiment, the eUICC subscription manager **109** can send the module **101** a pointer, uniform resource locator (URL), domain name, or related address for a location of the eUICC profile **107***c* in a step **205** as opposed to the actual, full profile **107***c*. In this embodiment, the module **101** could receive the pointer, uniform resource locator, domain name, or related address for the location of the eUICC profile **107***c* and subsequently download the eUICC profile **107***c* from an IP address associated with the pointer, uniform resource locator, domain name, or related address for a location of the eUICC profile **107***c*.

As depicted in FIG. **3**, after receiving the profile **107***c* from the eUICC subscription manager **109** in a step **205**, the eUICC **107** can receive data for decrypting the profile **107***c* in a step **303**. Note that if eUICC profile key **107***b* (in the form of a symmetric key as illustrated in FIG. **2***b*) has already be shared between the eUICC **107** and the eUICC subscription manager **109** before a step **206** below, then a step **303** could separately be omitted. For example, if an eUICC profile key **107***b* has been recorded with an eUICC **107** in a module **101** by a manufacturer of module **101**, then that eUICC profile key **107***b* could be used in a step **206** below, and a separate step **303** could be omitted. In other exemplary embodiments, the eUICC **107** can receive data for processing or deriving the eUICC profile key **107***b* for a step **206** below using the step **303** illustrated in FIG. **3**. A step **303** can include the receipt by eUICC **107** of either (i) an encrypted eUICC key **218**, or (ii) data for a key exchange. The encrypted eUICC key **218** received by an eUICC **107** in a step **303** could comprise an eUICC profile key **107***b* that is ciphered using a key ciphering algorithm **216** illustrated in FIG. **2***e*. For embodiments where data for a key exchange is received in a step **303**, the algorithms used with a key exchange could comprise a Diffie Hellman key exchange, or an Elliptic Curve Diffie Hellman key exchange (ECDH).

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**. A summary of ECDH is included in the Wikipedia article titled "Elliptic Curve Diffie-Hellman" (http://en.wikipedia.org/wiki/Elliptic_curve_Diffie % E2%80%93Hellman from Sep. 24, 2013, which is herein incorporated by reference. An ECDH key exchange in a step **303** could comprise the message received by a eUICC **107** including a common base point G. The base point G could also be sent from an eUICC **107** to eUICC subscription manager **109**. The base point G for an ECDH key exchange in a step **303** could also be recorded with the eUICC in a step **301** above, and in this case the message at a step **303** received by an eUICC **107** could comprise a signal to initiate or use a key exchange for deriving the eUICC profile key **107***b*. Note that the eUICC subscription manager **109** and the eUICC **107** could take additional steps to process the eUICC profile key **107***b* after an ECDH key exchange at step **303**, such as taking the output of an ECDH key exchange and inputting that output into a secure hash algorithm in order to obtain the eUICC profile key **107***b*. Other algorithms besides an ECDH or Diffie Hellman key exchange can be utilized as well at a step **303**, including a key exchange according to the American National Standards Institute (ANSI) standard X-9.63.

After completing a step **303**, an eUICC **107** operating in a module **101** could read and utilize the eUICC profile key **107***b*. In embodiments where the eUICC profile key **107***b* in a step **303** above comprises an encrypted eUICC key **218**, a step **217** from FIG. **2***e* can be utilized by the eUICC **107** in order to decrypt the eUICC key **218** into a plaintext of eUICC profile key **107***b*. The plaintext eUICC profile key **107***b* can be used by the eUICC **107** in a step **206** to decrypt (x) the profile **107***c* received in a step **205** above into (y) a profile **107***d*. The use of an eUICC profile key **107***b* for a step **206** is also depicted and described in connection with FIG. **2***a* above and also FIG. **2***b*. Plaintext within a profile **107***d* can be read after a step **206**, although in exemplary embodiments and as illustrated in FIG. **2***a*, the profile **107***d* can continue to record ciphertext **208***b* and ciphertext **208***c*.

In an exemplary embodiment, after a step **206** in FIG. **3** to convert received profile **107***c* to profile **107***d*, if (A) a ciphertext **208***c* that includes the first key K **203** is present in profile **107***d* (as depicted in FIG. **2***a* above), then (B) eUICC **107** could also use a key deciphering algorithm **217** on ciphertext **208***c* in order to extract the plaintext first key K **203**. Note that ciphertext **208***a* could be ciphered by an eUICC subscription manager **109** (using a profile ciphering algorithm **210**) and ciphertext **208***b* and/or ciphertext **208***c* could be encrypted by a mobile network operator **104** (using a key ciphering algorithm **216**). In other words, a module **101** with an eUICC **107** can use (i) a profile deciphering algorithm **206** with an eUICC profile key **107***b* to decrypt ciphertext **208***a*, (ii) a key deciphering algorithm **217** with an eUICC private key **215** to decrypt ciphertext **208***c*, and/or (ii) a key K deciphering algorithm **207** with a symmetric key **127** to decrypt ciphertext **208***b*.

After reading plaintext in profile **107***d*, module **101** could then utilize the profile **107***d* to conduct a first authentication **304** with the mobile network operator **104**. As depicted in FIG. **3**, the first authentication **304** can comprise (i) module **101** sending an attach message **305** with network module identity **202**, (ii) the eUICC **107** and module **101** receiving a RAND **118**, (iii) the eUICC **107** using a step **306** in order to calculate a RES **119**, and (iv) the module **101** sending the RES **119**. Although not illustrated in FIG. **3**, a first authentication **304** could include other data such as receiving the equivalent of an "OK" message upon successful authentication, the receipt of additional network parameters **202** after successful authentication, etc. The module **101** can use a profile **107***d* from a step **206** above in order to conduct the first authentication **304**. The profile **107***d* in an eUICC **107** could be selected and activated in order to connect with a wireless network **102** associated with mobile network operator **104**. As contemplated herein and throughout the present invention, an activated profile **107***d* can comprise a selected and enabled network access application state as illustrated in Figure D.1 of ETSI TS 103 383 v.2013-02 for the activated profile **107***d*, and other possibilities exist as well. As illustrated in FIG. **3** after a step **206**, the module **101** can use a network application **101***x* in order to attach to the wireless network **102** and communicate with the mobile network operator **104**.

Within a first authentication **304**, the module **101** can send a first attach message **305**, and the first attach message **305** can include the first network module identity **202**. With a 4G LTE network, the first attach message **305** could comprise a radio resource connection request message, or a similar message could be utilized with other wireless networking standards as well, such as LTE Advanced or WiMAX. An exemplary radio resource connection request is described in section 5.3.3 within ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification",

which is herein incorporated by reference. Although not illustrated in FIG. **3**, the module **101** and wireless network **102**/mobile operator **104** could take additional related steps before sending the exemplary first attach message **305**, such as, but not limited to, module **101** synchronizing a clock **160** with wireless network **102**, module **101** sending a message on a random access control channel (RACH) in order to have a timeslot and frequencies for sending the first attach message **305**, etc.

As depicted in FIG. **3**, after receiving and processing the first attach message **305**, the mobile network operator can send a first random number (RAND) **118**. Although not illustrated in FIG. **3**, a network authentication token "AUTN" and a sequence number could be sent with the first RAND **118**. An exemplary format for the use of a RAND **118** with a response RES **119** is described in ETSI standard TR 131 900 v.10.0.0 and related documents. In a first authentication **304** the module **101** and the eUICC **107** can receive the first RAND **118**. The eUICC **107** can conduct a step **306** with an input of the first RAND **118** and the first key K **203** in order to calculate a first RES **119**. The use of a RAND **118** with a RES **119** in a step **306** could comprise a general use of a message digest authentication, and another exemplary message digest authentication is also described in IETF RFC 2617, titled "HTTP Authentication: Basic and Digest Access Authentication". After receiving the exemplary first RAND **118** message, in order to conduct a first authentication **304**, module **101** using an eUICC **107** could take steps to demonstrate to MNO **104** that module **101** has access to the same first key K **203** as recorded by the MNO **104** in a step **302***a* or step **302***b* above. MNO **104** could record the expected RES **119** value with a set of authentication vectors **117** for the first network module identity **202**, as depicted in FIG. **1***d* and FIG. **1***e*.

Module **101** can properly respond to a challenge/nonce (such as a first RAND **118**) in a message digest authentication by sending a secure hash value calculated using (i) the challenge/nonce and (ii) the first key K **203**. The secure hash value can comprise the first RES **119**. In exemplary embodiments, eUICC **107** and wireless network **102** could use algorithms specified in ETSI TS 135 205-209, as well as subsequent and related standards, in order for module **101** using eUICC **107** to (i) calculate a secure hash value, and (ii) process related steps for a first authentication **304**. After processing a first RES **119** in a step **306** using the first key K **203**, the eUICC **107** could send the first RES **119** to the network application **101***x* in module **101**. Module **101** could then send the first RES **119** to the mobile network operator **104** using the wireless network **102**, as depicted in FIG. **3** and thereby complete a first authentication step **304** for the module **101**.

In another embodiment for a first authentication step **304**, (i) module **101** could send (i) the first network module identity **202** a digital signature processed using a digital signature algorithm **221** and the eUICC private key **215**, and (ii) MNO **104** could verify the digital signature using a digital signature algorithm **221** and the eUICC public key **214**. Other possibilities exist as well for steps within a first authentication **304** using a eUICC private key **215** with the first network module identity **202** or the eUICC identity **107***a* in a first authentication step **304** without departing from the scope of the present invention. In an exemplary embodiment, as depicted in FIG. **1***f* above, the eUICC **107** could include an IP address **106***c* with an interface identifier **106***e* associated with the eUICC **107**, and in this case the module **101** could send the first RES **119** value from the eUICC **107** to the MNO **104** through the wireless network **102**.

In a step **308***a* the mobile network operator **104** can receive the first RES **119**. A server **105** such as a mobility management entity (MME) for the mobile operator network **104** associated with the wireless network **102** could compare the received first RES **119** with an internally recorded RES **119** from the authentication vector **117**. As noted above, the authentication vector **117** could be received by the server **105** from the HSS of the mobile network operator **104** before a step **308***a*. If the received first RES **119** matches the internally stored first RES **119** value, the wireless network **102** and mobile network operator **104** can consider or process that the module **101** is authenticated for a step **308***a*. The wireless network **102**, the MNO **104**, and the module **101** can take subsequent steps (not shown) for the module **101** to access the IP network **111**, in order to conduct authentication of the module **101** or a user associated with the module **101** with a second factor in a step **308***b* below.

In a step **308***b*, the mobile network operator **104** can conduct a separate authentication of either a user **113** associated with a module **101** or the module **101** using a second factor. In other words, the mobile network operator **104** can use a step **308***b* to authenticate the user **113** of module **101** or the module **101** using steps and a process that is different than the first authentication **304**. Note that this use of a separate authentication step **308***b* can be different than conventional technology used in authenticating a module **101** in a step **304**, since other values and tokens besides the first key K **203** can be used in the authentication step **308***b*. The additional authentication step **308***b* can be useful for a mobile network operator **104** to authenticate a module **101** with an eUICC **107** and profile **107***d*, since the profile **107***d* with the first key K **203** may be transferred to module **101** in a communications channel outside the control of mobile network operator **104**. As one example, the profile **107***d* with the first network key K **203** could be transferred to an eUICC **107** from the eUICC subscription manager **109** using an IP network **111**, as depicted in FIG. **3** in a step **205**. The mobile network operator **104** may not have control over the IP network **111** used in a step **205**. The mobile network operator **104** may not have control over the security keys and algorithms used to encrypt the profile **107***d* into a profile **107***c*, and thus the security of the first key K **203** upon which the MNO **104** depends for authentication and ciphering of data with module **101** may be outside the control of MNO **104**. As one example, the MNO **104** may not be able to separately authenticate the identity of a user of module **101** with the eUICC **107**, before the profile **107***d* was received by module **101** and eUICC **107** in a step **205**.

Consequently, without a separate authentication step **308***b* the user **113** of module **101** with the eUICC **107** may be unknown to MNO **104**, and a separate identity of the user **113** or module **101** (other than network module identity **202**) may preferably be authenticated in a step **308***b*. Thus, a MNO **104** may use a separate authentication step **308***b* in order to authenticate a user **113** of module **101** with the eUICC **107** and the first key K **203** in exemplary embodiments. The user **113** can have a contractual or business relationship with MNO **104** in order to pay for voice and/or data services from the MNO **104**, and thus the MNO **104** can preferably identify and authenticate a user **113** in a step **308***b*.

A step **308***b* can comprise the authentication and/or secure identification of (i) a user **113** of module **101** or (ii) module **101** using a second factor. Although a step **308***b* is depicted

Petitioner Samsung Ex-1004, 0047

in FIG. **3** as being performed after a first authentication **304**, a step **308***b* could be performed before a step **304** (including with a step **302***b* as described in step **302***b* above). The use of a second factor in an authentication step **308***b* can comprise a two-factor authentication, where the first factor can be the successful completion of authentication using a step **304** and step **308***a* described above. The steps for authenticating a user **113** or module **101** in a step **308***b* could comprise many different forms without departing from the scope of the present invention. In one embodiment, where the user **113** of module **101** comprises a subscriber to telecommunication and data services from MNO **104**, the user **113** could present identification to a representative of the MNO **104** in a step **308***b*. The identification could be in the form of a physical identity such as, but not limited to, a drivers license or a passport (along with a value that can be associated with the eUICC profile **107***d* such as the module identity **110** or the eUICC identity **107***a*). The representative of the MNO **104** could record the identification in a web browser with connectivity to a database shared by a server **105**.

In another embodiment of an authentication of a user **113** of module **101** (with the eUICC profile **107***d* recorded with an eUICC **107** in module **101** from a step **205**) could enter information into a web page provided by MNO **104**, where the user **113** first (i) authenticates on the web page and then (i) enters identification information for the module **101** or eUICC **107**. The user **113** could first authenticate with the MNO **104** via a web page by entering a valid identity and a password (where the identity and password for the web page in a step **308***b* could be previously established between the user **113** and the MNO **104** before a step **308***b*). In another embodiment for a step **308***b*, a user **113** could call a telephone number operated by or associated with a MNO **104** and provide identification information via voice or entering information such as dual-tone multi-frequency (DTMF) digits via interactive voice response (IVR). The identification information could include either a credit card number or a personal identification number (PIN) for the user **113** (where the PIN may be previously shared or established between the user **113** and the mobile network operator **104**). The user **113** could also send a text message to MNO **104** from module **101** (*i*) using the module **101** authenticated link with MNO **104** established in a first authentication **304**, where (ii) the text message include identification information for a user **113**.

In accordance with preferred exemplary embodiments for the verification of an identity of user **113** in a step **308***b* (including an authentication of user **113** in a step **308***b*), the user **113** can send data to a MNO **104** from module **101** using a data connection via wireless network **102** associated with (and established after) the first authentication **304**. In this manner, data and voice connectivity between the MNO **104** and module **101** could be established with a first authentication step **304**, and the user **113** and MNO **104** can conduct an authentication step **308***b* (or equivalently a verification of an identity of the user **113**) to confirm the identity of the user **113** via the established data and voice connectivity using the wireless network **102**. In other words, the user **113** could verify or authenticate an identity of the user **113** of module **101** through the wireless network **102** in a step **308***b*, where (a) module **101** had conducted a first authentication step **304** and **308***a* with MNO **104** using the first key K **203** recorded in a profile **107***d*, in order to (b) support or conduct a separate verification or authentication of a user **113**. In an exemplary embodiment, the user **113** could enter identifying information for a step **308***b* in a web page accessed through a user interface **101***j* on module **101**, where data connectivity for the web page is provided to module **101** through the wireless network **102** after a first authentication step **304**.

The authentication or verification of user **113** identity in a step **308***b* can comprise authenticating module **101** with a second factor, where the first factor can comprise the first key K **203** and the second factor can comprise information provided by a user **113** in a step **308***b*. Other possibilities exist as well for those of ordinary skill in the art for (a) a user **113** of module **101** with the first key K **203** to (b) authenticate or verify an identity of the user **113** in a step **308***b* without departing from the scope of the present invention. In these exemplary embodiments for a user **113** to authenticate or verify an identity for the user **113** for module **101** with the MNO **104**, the MNO **104** could record information or data received from the user **113** in a database, such that a server **105** for MNO **104** sends the symmetric key **127** in a step **309** below after an identity of the user **113** is verified or authenticated in a step **308***b*. In exemplary embodiments illustrated in FIG. **3**, the module **101** can access the wireless network **102** with the first key K **203** in order to (i) establish communication with the IP network **111**, (ii) support authentication of a user **113** in a step **308***b* through the IP network **111**, and then (iii) subsequently receive a symmetric key **127** in order to decrypt a ciphertext **208***b* with a second key K **204***a*.

In other exemplary embodiments, module **101** could comprise a module supporting "machine-to-machine" applications and communications, and the module could be different than a traditional mobile phone or smartphone for (i) placing voice telephone calls or (ii) supporting a user interface **101***j* in the form of a touch screen and web browser. The module **101** could include a sensor **101***f* for collecting data and an actuator **101***y* for controlling or changing a state associated with a monitored unit for the module **101**. In these embodiments, and as depicted and described in connection with FIG. **1***a*, module **101** can be associated with an M2M service provider **115**, and the M2M service provider **115** could be associated with a plurality of modules **101**, as opposed to an individual with a telephone number for voice services to module **101**.

Each of the different modules **101** in the plurality of modules **101** could include different values for module identities **110**, eUICC identities **107***a*, profile identities **107***e*, and the first network module identities **202**. In these embodiments for a step **308***b* where the module **101** supports M2M applications for an M2M service provider **115**, in a step **308***b* in FIG. **3**, the MNO **104** could verify that (a) module **101** with eUICC **107** and the profile **107***d* from a step **304** is (b) properly associated with an M2M service provider **115**. In exemplary embodiments, the MNO **104** ould conduct a step **308***b* by securely or properly determining that an identity from module **101** is associated with M2M service provider **115**, and an exemplary identity for module **101** include any of a module identity **110**, an eUICC identity **107***a*, a profile identity **107***e*, and/or the first network module identity **202**.

In exemplary embodiments where module **101** supports M2M application and the module **101** is associated with an M2M service provider **115**, MNO **104** could take several possible actions in a step **308***b* for authenticating or verifying that an identity from module **101** in FIG. **3** is associated with an M2M service provider **115**. The proper association of an identity of module **101** with M2M service provider **115** may be necessary or useful for contractual and business relationships between MNO **104** and M2M service provider **115**, such as, but not limited to, allowing MNO **104** to bill

Petitioner Samsung Ex-1004, 0048

or invoice M2M service provider **115** for data services that MNO **104** provides to module **101**. In a first exemplary embodiment for a step **308***b* in FIG. **3** where module **101** supports M2M applications with a M2M service provider **115**, MNO **104** could securely send to M2M service provider **115** an identity of module **101**, such as, but not limited to module identity **110**, eUICC identity **107***a*, profile identity **107***e*, and/or the first network module identity **202** through an IP network **111**. The MNO **104** could also send the identity of module **101** in a query or request message. Although not illustrated in FIG. **3**, the MNO **104** could also send the M2M service provider **115** a digital signature received from module **101** before a step **308***b*, where the digital signature was (i) processed by module **101** using a digital signature algorithm **221** and an eUICC private key **215**, and (ii) sent from the module **101** to the MNO **104**.

In a step **308***b*, the M2M service provider **115** could (i) receive the identity of module **101** (such as, but not limited to module identity **110**, eUICC identity **107***a*, profile identity **107***e*, and/or the first network module identity **202**), (ii) verify or determine the identity of module **101** properly belongs to M2M service provider **115**, and (iii) send a response confirming the module **101** with the identity is validly associated the M2M service provider **115**. The response from the M2M service provider **115** (or data within a message from M2M service provider **115** to MNO **114**) for a step **308***b* can comprise a second factor for MNO **104** in authenticating module **101** with eUICC **107** and profile **107***d*. In this manner, MNO **104** can confirm module **101** with the first network identity **202** is authenticated or verified as belonging to or being associated with M2M service provider **115** in a step **308***b*.

In another exemplary embodiment for a step **308***b*, the M2M service provider **115** could also send MNO **104** a list of pre-authorized identities for one or a plurality of modules **101** before a step **308***b* (and in this case the list can comprise the second factor to authenticate module **101**). MNO **104** could query the list of identities received upon receiving an identity of module **101**, such as, but not limited to, the first network module identity **202** received in the first attach message **305**. Other possibilities exist as well for an MNO **104** to authenticate or verify that an identity of module **101** is associated with a M2M service provider **115** in a step **308***b* without departing from the scope of the present invention.

After successfully verifying or confirming in a step **308***b* that module **101** in FIG. **3** is associated with a known user **113** or M2M service provider **115**, MNO **104** can send a symmetric key **127** in a step **309**. A network application **101***x* in the module **101** can receive the symmetric key **127** and the module **101** can forward the symmetric key **127** to the eUICC **107**. As depicted and described in connection with FIG. **2***a* and FIG. **2***c*, the symmetric key **127** can be used by module **101** to decrypt the ciphertext **208***b*, where the ciphertext **208***b* can include a second key K **204***a*. The symmetric key **127** can also previously be used by MNO **104** to encrypt the ciphertext **208***b*. The ciphertext **208***b* could be delivered to eUICC subscription manager **109** for including the ciphertext **208***b* in the profile **107***d*, as described above in step **302***a*. The ciphertext **208***b* could be sent to module **101** from the eUICC subscription manager **109** across the IP network **111** as profile **107***c* in a step **205** as described above in this FIG. **3**.

In exemplary embodiments, the MNO **104** can send the symmetric key **127** in a step **309** through the wireless network **102**, where the connection between module **101** and MNO **104** could be initiated by the first attach message **305** and authenticated by a first authentication **304**. Since the MNO **104** controls the nodes and ciphering steps for the transmission of symmetric key **127**, the symmetric key **127** can be securely sent by MNO **104** and received by module **101** with ciphering and keys used at the data-link layer under the control of MNO **104** (whereas MNO **104** may not control the keys and ciphering of sending the first key K **203**). Also note no entities, including the module **101**, a user **113**, an M2M service provider **115**, an eUICC subscription manager **109**, or unauthorized third parties could feasibly read the ciphertext **208***b* with the second key K **204***a* until they receive the symmetric key **127**.

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**. As described in connection with a key ciphering algorithm **216** in FIG. **2***e*, the MNO **104** could select and read the eUICC public key **214** (using a received associated identity such as the first network module identity **202**), and use an asymmetric ciphering algorithm **219** to encrypt the symmetric key **127**. 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** and the asymmetric ciphering algorithm **219**. For a step **309** in FIG. **3**, the use of encryption for a symmetric key **127** with an asymmetric ciphering algorithm **219** is optional, and the symmetric key **127** could be sent in a form where encryption is applied at the data-link layer according to standards for the wireless network **102**. Other possibilities exist as well for a module **101** to securely receive a symmetric key **127** in a step **309** without departing from the scope of the present invention. As described above in connection with a step **302***b*, in exemplary embodiments, the module **101** receives the symmetric key **127** after the MNO **104** authenticates or verifies that a user **113** or M2N service provider **115** is associated with module **101**, and until the receipt of the symmetric key **127** the ciphertext **208***b* cannot be feasibly decrypted.

After a step **309**, a module **101** with an eUICC **107** can use the symmetric key **127** to decrypt ciphertext **208***b*, where ciphertext **208***b* can include the second key K **204***a*. A module **101** or eUICC **107** can use a key K deciphering algorithm **207** with input from the received symmetric key **127** and the ciphertext **208***b* from profile **107***d* to output a plaintext second key K **204**. Although not illustrated in a step **207** in FIG. **3**, but as illustrated in a step **207** in FIG. **2***a*, a module **101** can use an eUICC **107** to also decrypt a second network module identity **209***a* for the second key K **204** using the symmetric key **127**. The second network module identity **209***a* can be recorded in the ciphertext **208***b*. The second network module identity **209***a* can be different than the first network module identity **202**, such as a different number or value for an IMSI. The second network module identity **209***a* can be the same length as the first network module identity **202**. The use and operation of a key K deciphering algorithm **207** is also depicted and described in connection with FIG. **2***a* and FIG. **2***e* above.

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 **101***w* such that the plaintext second key K **204** remains available to module **101** after power or a battery **101***k* is removed from module **101**. The plaintext second key K **204** could also be recorded in a protected memory within module **101**, such that the operating system **101***h* or CPU **101***b* may prevent read or write access to the protected memory by other processes than the eUICC **107**.

Petitioner Samsung Ex-1004, 0049

In other words, with a protected memory, other applications such as, but not limited to, applications that are downloaded from an "app store" or equivalent and installed by end users on the module **101** may be prevented by the operating system **101***h* from having access to the plaintext second key K **204** recorded in the protected memory.

In another embodiment, a module **101** may optionally not store the plaintext second key K **204** in nonvolatile memory, such that the second key K **204** continues to be recorded for a long-term basis only as ciphertext **208***b* in a nonvolatile memory such as flash **101***w*. The module **101** could perform a key K deciphering algorithm **207** each time a plaintext second key K **204** is needed for authentication purposes, including related key derivation of a CK and IK plus other derived keys. In this manner (by storing the second key K **204** in ciphertext **208***b* in module **101**) a plaintext second key K **204** may not be (i) stored in module **101** for a relatively long time such as several hours or longer, and also (ii) recorded outside a nonvolatile memory.

In another embodiment, (A) the plaintext second key K **204** is recorded only in a volatile memory within CPU **101***b* such as a register or cache memory, where access to the register or cache memory is limited to the eUICC **107**, and (B) after a successful authentication using the second key K **204**, such as, but not limited to, a second authentication **311** below, the plaintext second key K **204** is flushed from the register or cache memory within CPU **101***b*. In this manner, after (A) a first time that module **101** conducts a step **207** to obtain a plaintext second key K **204** and the module **101** completes a full power cycling, then (B) the plaintext second key K **204** may not be recorded in any of a volatile memory, a non-volatile memory, or a protected memory within module **101** (but module **101** could record an encrypted second key K **204***a* in a ciphertext **208***b*).

For the embodiments where the second key K **204** is not recorded as plaintext in a nonvolatile memory within module **101**, the module **101** can perform a step **207** with a ciphertext **208***b* recorded in a nonvolatile memory a second time to process or obtain the plaintext second key K **204**. In other words, the second key K **204** can be recorded on a long-term basis as a ciphertext **208***b* for eUICC **107** within module **101**, in an exemplary embodiment, thereby increasing the security of the second key K **204**. In this case, either (i) the symmetric key **127** could be recorded in a nonvolatile memory **101***w* in order to allow decrypting of the ciphertext **208***b*, or (ii) the module **101** could receive the symmetric key **127** a second time by conducting a step **309** a second time. The module **101** can reconnect with the wireless network **102** and the MNO **104** using the first network identity **202** and the first key K **203** a second time, after the module **101** has already received the symmetric key **127** a first time. The MNO **104** may optionally authenticate the user **113** or M2M service provider **115** a second time such as a second step **308***b* (before sending the symmetric key **127** a second time) in order to confirm a second use of the first key K **203** is authorized.

After a module **101** with an eUICC **107** processes a key K deciphering algorithm **207** to obtain a plaintext second key K **204**, the module **101** can connect with the wireless network **102** and mobile network operator **104** using the second network module identity **209** and the second network key **204**. The module **101** using a network application **101***x* could send a second attach message **305** with the second network module identity **209**. In another embodiment, the module **101** could send the second attach message **305** with the first network module identity **202**, and in this case the MNO **104** could record from the previous steps **302***b* and **308***b* that a key K associated with the first network module identity **202** should change to the second key K **204**.

But, given existing deployed infrastructure and systems for a mobile network operator **104**, the use of two different keys K with the same network module identity may be more difficult to support, and for this case and with preferred embodiments, the module **101** attaches with the MNO **104** the second time with the second network module identity **209** that has been deciphered from (i) a ciphertext **208***b* in a step **207** above, or (ii) a ciphertext **208***a* in a step **206** above. The second attach message **305** can be equivalent to the first attach message **305**, but with a change of module **101** sending the second network module identity **209**. With a 4G LTE network, the second attach message **305** could comprise a radio resource connection request message, or a similar message could be utilized with other wireless networking standards as well, such as LTE Advanced or WiMAX. An attach message such as **305** in FIG. **3** could also comprise module **101** using a globally unique temporary identity (GTUI) that can be associated with the second network module identity **209**. Other possibilities exist as well for the format or structure of an attach message **305** without departing from the scope of the present invention.

After sending the second attach message **305**, the module **101** with a eUICC **107** can conduct a second authentication **310** with the mobile network operator **104**. The module **101** and eUICC **107** could take the equivalent steps as the first authentication **304** depicted and described in this FIG. **3**, but with a difference of using the second network module identity **209** and the second key K **204**. In a second authentication **310**, the mobile network operator **104** could send the module **101** a second RAND value **118** through the wireless network **102**. A server **105** associated with MNO **104**, such as, but not limited to, a HSS could have previously processed an authentication vector **117** comprising at least (i) the second RAND value **118**, (ii) a network authentication token AUTN and sequence number (not shown), and (iii) a response value RES **119** for the second network module identity **209** and the second key K **204**. The server **105** or HSS associated with the MNO **104** could send the authentication vector **117** to a server or MME that module **101** communicates with through the wireless network **102**. The module **101** could receive the second RAND **118** using the network application **101***x*, and forward the second RAND **118** to the eUICC **107**. The communication steps between a network application **101***x* and an eUICC **107** in FIG. **3** could also use the steps depicted and described in connection with FIG. **1***e*.

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**. The MNO could record the second key K **204** in an authentication vector **117** a step **302***a* or step **302***b* above. Module **101** can properly respond to a challenge/nonce (such as a second RAND **118**) in a message digest authentication by sending a secure hash value calculated using (i) the challenge/nonce and (ii) the second key K **204**. The secure hash value can comprise the second RES **119**. In exemplary embodiments, the eUICC **107** and wireless network **102** could use algorithms specified in ETSI TS 135 205-209, as well as subsequent and related standards, in order for module **101** using eUICC **107** to (i) calculate a secure hash value, and (ii) process related steps

Petitioner Samsung Ex-1004, 0050

for a second authentication **310**. After processing a second RES **119** in a step **311** using the second key K **204**, the eUICC **107** could send the second RES **119** to the network application **101***x* in module **101**. Module **101** could then send the second RES **119** to the mobile network operator **104** using the wireless network **102**, as depicted in FIG. **3** and thereby complete a second authentication step **310** for the module **101**. In an exemplary embodiment, as depicted in FIG. **1***f* above, the eUICC **107** could include an IP address **106***c* with an interface identifier **106***e* associated with the eUICC **107**, and in this case the module **101** could send the second RES **119** value from the eUICC **107** to the MNO **104** through the wireless network **102**.

At a step **312**, the mobile network operator can receive the second RES **119** from the module **101** using the wireless network **102**. A server **105** for the mobile operator network **104** associated with the wireless network **102** could compare the received second RES **119** with an internally recorded RES **119**. The server **105** could receive an authentication vector **117** comprising at least the second RAND **118**, second RES **119**, and AUTN token for the second network module identity **209** before sending the second RAND **118** in a step **310** above. If the received second RES **119** matches the internally stored second RES **119** value, the wireless network **102** and mobile network operator **104** can consider or process that the module **101** is authenticated for a step **312**. The wireless network **102**, the MNO **104**, and the module **101** can take subsequent steps (not shown) for the module **101** to access the IP network **111**, including allowing module **101** to place and receive telephone calls and/or access the public Internet.

In an exemplary embodiment that utilizes the steps illustrated in FIG. **3**, the first key K **203** can comprise a null value or the number zero, which is contemplated in standards and supported by commercial wireless networks **102** in order to support emergency services for a module **101** without a valid UICC or eUICC. The MNO **104** and wireless network **102** can provide limited access to the IP network **111**, such that a user **113** of module **101** with a null or zero value for the first key K **203** could performs steps to authenticate or verify the user **113** identity in a step **308***b*. The limited access to the IP network **111** may not include access to the public Internet, but could include access to a server such as a web server for the user **113** to enter identification information. The data-link layer may not be encrypted due to the use of a null value for the first key K **203**, but the application or transport layer could secure communication from a web browser on the module **101** to the web server, such as using transport layer security (TLS). Other possibilities exist as well for ciphering or securing data at the application or transport layer in a step **308***b* to authenticate a user **113** without encryption at the data-link layer (such as without encryption by the wireless network **102** due to a null value for first key K **203**). In this embodiment where the first key K **203** comprises a null or zero value, after authentication of a user **113** or M2M service provider **115** in a step **308***b*, the second key K **204** used with a second authentication **310** can comprise a regular key K such as a non-null value or a random number.

FIG. **4**

FIG. **4** is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments. The processes and operations, described below with respect to all of the logic flow diagrams may include the manipulation of signals by a processor and the maintenance of these signals within data structures resident in one or more memory storage devices. For the purposes of this discussion, a process can be generally conceived to be a sequence of computer-executed steps leading to a desired result.

These steps usually require physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, or otherwise manipulated. It is convention for those skilled in the art to refer to representations of these signals as bits, bytes, words, information, elements, symbols, characters, numbers, points, data, entries, objects, images, files, or the like. It should be kept in mind, however, that these and similar terms are associated with appropriate physical quantities for computer operations, and that these terms are merely conventional labels applied to physical quantities that exist within and during operation of the computer.

It should also be understood that manipulations within the computer are often referred to in terms such as listing, creating, adding, calculating, comparing, moving, receiving, determining, configuring, identifying, populating, loading, performing, executing, storing etc. that are often associated with manual operations performed by a human operator. The operations described herein can be machine operations performed in conjunction with various input provided by a human operator or user that interacts with the computer.

In addition, it should be understood that the programs, processes, methods, etc. described herein are not related or limited to any particular computer or apparatus. Rather, various types of general purpose machines may be used with the following process in accordance with the teachings described herein.

The present invention may comprise a computer program or hardware or a combination thereof which embodies the functions described herein and illustrated in the appended flow charts. However, it should be apparent that there could be many different ways of implementing the invention in computer programming or hardware design, and the invention should not be construed as limited to any one set of computer program instructions.

Further, a skilled programmer would be able to write such a computer program or identify the appropriate hardware circuits to implement the disclosed invention without difficulty based on the flow charts and associated description in the application text, for example. Therefore, disclosure of a particular set of program code instructions or detailed hardware devices is not considered necessary for an adequate understanding of how to make and use the invention. The inventive functionality of the claimed computer implemented processes will be explained in more detail in the following description in conjunction with the remaining Figures illustrating other process flows.

Further, certain steps in the processes or process flow described in all of the logic flow diagrams below must naturally precede others for the present invention to function as described. However, the present invention is not limited to the order of the steps described if such order or sequence does not alter the functionality of the present invention. That is, it is recognized that some steps may be performed before, after, or in parallel other steps without departing from the scope and spirit of the present invention.

The processes, operations, and steps performed by the hardware and software described in this document usually include the manipulation of signals by a CPU or remote server and the maintenance of these signals within data structures resident in one or more of the local or remote memory storage devices. Such data structures impose a physical organization upon the collection of data stored within a memory storage device and represent specific

Petitioner Samsung Ex-1004, 0051

electrical or magnetic elements. These symbolic representations are the means used by those skilled in the art of computer programming and computer construction to most effectively convey teachings and discoveries to others skilled in the art.

At step **401**, a module **101** can connect with a first wireless network **102**. The first wireless network **102** could comprise a public land mobile network, a local area network such as WiFi, or the use of white-space spectrum. The module **101** could connect with the first wireless network **102** in order to obtain access to IP network **111** which could comprise the public Internet, although the IP network **111** could comprise a private network in some embodiments. Although not depicted in FIG. **4**, a step **401** could also comprise the module **101** connecting to a wired network through USB interface **101***v*. Upon conclusion of a step **401** the module **101** can use an IP address such as IP address **106***b* in FIG. **1***f* in order to communicate with an eUICC subscription manager **109**. As illustrated in FIG. **1***f*, in an exemplary embodiment the eUICC **107** could also have an IP address **106***c* after a step **401**, although the use of an IP address for eUICC **107** is not required and the module **101** can be associated with one IP address for all external communications.

The module **101** can then use a step **205** in order to receive an eUICC profile **107***c*. The eUICC profile **107***c* could be received from the eUICC subscription manager **109** using the wireless network **102** and/or IP network **111** from a step **401** above. The module **101** could record the received eUICC profile **107***c* with the eUICC **107**, including sending the eUICC profile **107***c* to the eUICC **107** or sharing memory **101***e* or **101***w* between the eUICC **107** and a network application **101***x*. The module **101** could use a network application **101***x* in order to receive the eUICC profile **107** from the eUICC subscription manager in a step **205**, as depicted and described in connection with FIG. **3**. The module **101** with an eUICC **107** could then decrypt the profile **107***c* in a step **206** using an eUICC profile key **107***b*. The eUICC profile key **107***b* could be recorded with an eUICC **107** before a step **206**. The module **101** and/or eUICC **107** could receive the eUICC profile key **107***b* using a step **303** as depicted and described in connection with FIG. **3**. The eUICC profile key **107***b* could be received using a key exchange, such as a Diffie-Hellman key exchange or an ECDH key exchange. Or, the eUICC profile key **107***b* could be recorded with the eUICC **107** by a module manufacturer. Other possibilities exist as well for a module **101** to record an eUICC profile key **107***b* before a step **206** without departing from the scope of the present invention. A module **101** and/or an eUICC **107** could use a profile deciphering algorithm **206** in a step **206**, as depicted and described in connection with FIG. **2***a* and FIG. **2***b*. Upon conclusion of a step **206**, a profile **107***d* could be recorded in an eUICC **107**.

In a step **402**, a module **101** can then select and activate the profile **107***d* from a step **206** in order to connect with a second wireless network **102**. A module **101** could take several possible steps in order to select and activate the profile **107***d*. A module **101** could use radio **101***z* to search for radio beacons from base stations **103** for wireless networks **102** surrounding the module **101**, and upon finding the second wireless network **102** to connect with, the module **101** could select the profile **107***d*. The profile **107***d* 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 **107***d*. A module **101** could receive an instruction from an eUICC subscription manager **109** in order to activate the profile **107***d*, where the instruction could be received through the first wireless network **102** in a step **401** above.

In another embodiment, a module **101** or eUICC **107** could query the eUICC subscription manager **109** through the first wireless network **102** before activating the profile **107***d* in a step **402**. Commercial business arrangements among the user **113** of module **101**, the eUICC subscription manager **109**, and the mobile network operator **104** can determine the timing for activating a profile **107***d* for a module **101** with an eUICC **107** in a step **402**, such as a user **113** entering a new contract for service with a MNO **104** for the profile **107***d*. As contemplated herein and throughout the present invention, an activated profile **107***d* can comprise a selected and enabled network access application state as illustrated in Figure D.1 of ETSI TS 103 383 v.2013-02 for the activated profile **107***d*. Other possibilities exist as well for a module **101** to activate a profile **107***d* in a step **402** without departing from the scope of the present invention.

In a step **304** in FIG. **4**, a module **101** using eUICC **107** can conduct a first authentication **304** with the second wireless network **102**, using the first key K **203** recorded in the activated profile **107***d*. The module **101** could also send the first network module identity **202** from a profile **107***d* to the mobile network operator **104** in a step **304** in FIG. **4**. The second wireless network **102** in a step **304** in FIG. **4** can be associated with a mobile network operator **104**. The use of a first authentication **304** is also depicted and described in connection with FIG. **3** above. As noted in a first authentication **304**, the first key K **203** could comprise a key with a null value in an exemplary embodiment, although a random number could be used for a first key K **203** as well. As depicted in FIG. **4**, the steps **401** through **304** could comprise substeps within a step **403**. The combined substeps comprising a step **403** can be used by a module **101** in exemplary embodiments including an embodiment illustrated in FIG. **6** below.

Although not depicted in FIG. **4**, the mobile network operator **104** can conduct a separate step **308***b* to authenticate module **101** or a user **113** of module **101** using a second factor after a step **304**. As described in a step **308***b* above, the second factor could comprise verifying or authenticating an identity of a user **113** associated with module **101**. Note that the authentication of a user **113** can be conducted through the module **101** accessing a server **105** or a web page through the IP network **111** via the second wireless network **102** after the first authentication **304** using the first key K **203** (including embodiments where the first key K **203** comprises a null value).

In a step **309**, the module **101** can receive a key from the second wireless network. The key in a step **309**, as depicted in FIG. **3** above, can comprise a symmetric key **127** in order to decrypt a ciphertext **208***b* within profile **107***d*. As also contemplated and described in connection with a step **309** in FIG. **3**, the key could comprise a module **101** receiving a ciphertext that includes a symmetric key **127** that has been ciphered with a key ciphering algorithm **216** using an asymmetric ciphering algorithm **219** and the eUICC public key **214**, as illustrated in FIG. **2***e*. For a key ciphering algorithm **216** used with a step **309**, (i) the symmetric key **127** can comprise the plaintext (as opposed to the eUICC profile key **107***b* depicted in FIG. **2***e*), and (ii) the MNO **104** could operate the key ciphering algorithm **216** instead of the eUICC subscription manager **109** depicted. In this embodiment of a step **309**, a module **101** and/or an eUICC **107** could receive the key in the form of a ciphertext of sym-

Petitioner Samsung Ex-1004, 0052

metric key **127** in a step **309** and decrypt the ciphertext of symmetric key **127** with the eUICC private key **215** in order to read a plaintext symmetric key **127**.

In a step **207** in FIG. **4**, the module **101** and/or eUICC **107** can decrypt the ciphertext **208***b* with the second key K **204***a* using the symmetric key **127**. The module **101** can use a key K deciphering algorithm **207** as depicted and described in connection with FIG. **2***c* above in order to read and record a plaintext second key K **204** from the ciphertext **208***b* in the profile **107***d*, where the profile **107***d* was previously decrypted and recorded using a step **206** above. As depicted in FIG. **2***a*, the ciphertext **208***b* can also include a second network module identity **209***a*, so the eUICC **107** can also read the plaintext second network module identity **209** in a step **207**, if a second network module identity **209***a* is included in a ciphertext **208***b*. In an exemplary embodiment, the second plaintext key K **204** is recorded in a protected, nonvolatile memory such as, but not limited to, a flash memory **101***w*. In this embodiment, the protected nonvolatile memory could comprise a memory address designated by the module **101**, CPU **101***b*, operating system **101***h*, a module program **101***i*, or the eUICC **107** as a memory address that can only be written and read by the eUICC **107**. Other possibilities exist as well to those of ordinary skill in the art for a plaintext second key K **204** to be recorded in a protected, nonvolatile memory in a step **207** without departing from the scope of the present invention.

In another embodiment, as described in a step **207** in FIG. **3**, the module **101** could record the encrypted second key K **204***a* in a nonvolatile memory, along with a symmetric key **127** (or an encrypted symmetric key **127** ciphered by a key ciphering algorithm **216**). The module **101** or eUICC **107** could decrypt the encrypted symmetric key **127** in order to decrypt the ciphertext **208***b* that contains the second key K **204***a* each time the module **101** or eUICC **107** needs to read a plaintext second key K **204** for an conducting an authentication step **310**, plus the subsequent derivation of additional keys such as CK and IK, Kasme, Kupenc, etc. using the plaintext second key K **204** and a RAND **118** value.

After reading a plaintext second key K **204** from a ciphertext **208***b* in a step **207** using the symmetric key **127**, the module **101** and/or eUICC **107** can conduct a second authentication **310** step using the plaintext second key K **204**, in order to authenticate with the second wireless network **102**. The second wireless network **102** can comprise the same wireless network **102** the module **101** communicates with in a step **304** above. The use of a plaintext second key K **204** in a second authentication **310** step is depicted and described in connection with FIG. **3**.

Although not illustrated in FIG. **4**, the module **101** could send a detach message or equivalent to temporarily disconnect from the second wireless network **102** after a step **309** and before a step **310** illustrated in FIG. **4**. A step **310** can comprise the module **101** sending a radio resource connection request to the second wireless network **102** with a network module identity associated with the second key K **204**. A step **310** can be completed by a module **101** and/or an eUICC **107** sending a RES **119** value calculated using (i) a RAND **118** received and (ii) the second key K **204**.

Although not illustrated in FIG. **4**, after a step **310** by a module **101** and/or an eUICC **107**, the MNO **104** could verify the RES **119** and then the module **101** and the wireless network **102** associated with the MNO **104** could take subsequent steps for a module **101** to have access to the IP network **111** including the public Internet. The module **101** and/or eUICC **107** could derive session keys (such as, but not limited to a key CK) for encrypting data through the wireless network using a RAND **118** received in a step **310** and the second key K **204**, and the module **101** and/or eUICC **107** could also derive an integrity key for a session (such as, but not limited to, an integrity key IK). Using an authenticated module **101** from a step **310**, the MNO **104** can meter services rendered to a module **101** after a step **310** in order to bill or invoice a user **113** or M2M service provider **115**.

FIG. **5***a*

FIG. **5***a* is a graphical illustration of a public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments. An eUICC **107** within a module **101** can include an eUICC private key **215**, which can be associated with an eUICC public key **214**. The eUICC private key **215** and eUICC public key **214** can comprise a public key infrastructure (PKI) key pair for eUICC **107**. The MNO **104** can record the eUICC public key **214** along with an eUICC identity **107***a*, such that the MNO **104** can properly associate one of a plurality of eUICC public keys **214** with the proper eUICC **107**. Although not illustrated in FIG. **5***a*, a MNO **104** could record the eUICC public key **214** and an associated eUICC identity **107***a* in a database. The MNO **104** could receive the eUICC public key **214** and the eUICC identity **107***a* from an eUICC subscription manager **109** through an IP network **111** in a step **302***a* or step **302***b* of FIG. **3**. The use of, source, and additional details regarding an eUICC public key **214** and eUICC private key **215** are also depicted and described in connection with FIG. **2***d* above.

The mobile network operator **104** could also be associated with an MNO private key **501** and an MNO public key **502**, which could comprise a PKI key pair for the mobile network operator. The mobile network operator **104** could process or derive the PKI key pair using steps and algorithms equivalent to the steps and algorithms for an eUICC **107** to obtain the eUICC public key **214** and eUICC private key **215**. The PKI keys depicted in FIG. **5***a* could be processed using RSA algorithms or elliptic curve cryptography (ECC) algorithms, and other possibilities exist as well for the format of PKI keys without departing from the scope of the present invention. The public keys in FIG. **5***a* can comprise keys recorded in an X.509 certificate, although the use of an X.509 certificates with public keys **214** and **502** are not required. The public key **214** and **502** in the form of an X.509 certificate can optionally be signed by a certificate authority. As illustrated in FIG. **5***a*, the mobile network operator public key **502** can be recorded in the eUICC profile **107***d*. The MNO **104** could send the MNO public key **502** to the eUICC subscription manager **109** in a step **302***a* or **302***b* depicted and described in FIG. **3**, and the eUICC subscription manager **109** could include the MNO public key **502** in the profile **107***d*. An eUICC profile **107***d* could also include the additional data for an eUICC profile **107***d* as depicted and described in FIG. **2***a*, in addition to the MNO public key **502**.

As illustrated in FIG. **5***a*, the MNO **104** and eUICC **107** can both record a key derivation algorithm **503**. Exemplary key derivation algorithm **503** could support a Diffie Hellman key exchange, an Elliptic Curve Diffie Hellman (ECDH) key exchange (ECDH), or similar algorithms for each node to mutually derive a key using public and private keys. For embodiments where (A) eUICC public key **214**, eUICC private key **215**, MNO public key **502**, and MNO private key **501** utilize (i) elliptic curve cryptography (ECC) and (ii) a common, shared elliptic curve, then (B) a key derivation algorithm **503** in FIG. **5***a* can comprise an algorithm for conducting an ECDH key exchange. The use of an ECDH key exchange was also described and contemplated between

Petitioner Samsung Ex-1004, 0053

an eUICC subscription manager **109** and an eUICC **107** in step **303** in FIG. **3** above. For embodiments where a key derivation algorithm **503** supports a Diffie Hellman key exchange, the key derivation algorithm **503** could record a multiplicative group of integers modulo p, where p is prime, and g is a primitive root mod p. In exemplary embodiments, p can be sufficiently large, such as, but not limited to, and exemplary prime number of at least 250 digits, and g can be a small number, such as, but not limited to, the number **5**. In exemplary embodiments, additional values pertaining to the operation of a key derivation algorithm **503** can be transferred between two nodes using a token **505** described in a FIG. **5***b* and FIG. **5***c* below.

FIG. **5***b*

FIG. **5***b* is a graphical illustration of deriving a second key K using public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments. A mobile network operator **104** could process a MNO key exchange algorithm **504** in order to output or determine a second key K **204**. A module **101** with an eUICC **107** could process an eUICC key exchange algorithm **505** in order to output or determine the same second key K **204**. The MNO key exchange algorithm **504** and the eUICC key exchange algorithm **505** could include a key derivation algorithm **503**, and a key derivation algorithm **503** is also depicted and described in connection with FIG. **5***a* above. The MNO **104** and module **101** could share or communicate a key exchange token **506** in order to operate the key exchange algorithm **505**. In this manner, a module **101** with an eUICC **107** and a mobile network operator **104** could mutually derive or share the second key K **204** without MNO **104** transmitting or sending the second key K **204**, even in an encrypted form such as a second key K **204***a* in a ciphertext **208***b*, to either (i) eUICC subscription manager **109** in a step **302***a* or step **302***b*, or (ii) to a module **101** in a profile **107***c*.

For a MNO key exchange algorithm **504**, a mobile network operator **104** using a server **105** could input the mobile network operator private key **501**, the eUICC public key **214**, and a key exchange token **506** into a key derivation algorithm **503** in order to output the second key K **204**. Note that the key derivation algorithm **503** in both a MNO key exchange algorithm **504** and an eUICC key exchange algorithm **505** can include additional or separate processing steps than those contemplated in a Diffie-Hellman key exchange and an ECDH key exchange. Additional steps than those contemplated in a Diffie-Hellman key exchange or ECDH key exchange for a key derivation algorithm **503** include transforming key output by these key exchange protocols into a key length and format compatible and suitable for a key K for use with wireless networks. In a key derivation algorithm **503**, the output of a Diffie-Hellman key exchange and an ECDH key exchange could be input into a secure hash algorithm, such as SHA-256, which could then be truncated to select a 128 bit second key K **204** using a key derivation algorithm **503**. For a MNO key exchange algorithm **504**, the security key exchange token **506** can depend upon the algorithm used in a key derivation algorithm **503**.

For embodiments where key derivation algorithm **503** comprises a Diffie-Hellman key exchange, the key exchange token **506** can comprise integer values of p and g. Or, with a Diffie-Hellman key exchange the security key exchange token **506** sent from a MNO **104** could comprise a value equal to g^a mod p where (x) the values or p and g have been previously shared between MNO **104** and eUICC **107**, and (y) the value "a" can comprise the MNO private key **501**. A security key exchange token **506** received by MNO **104** for input into a key derivation algorithm for a eUICC **107** could comprise a value of g^b mod p, where b comprises the eUICC private key **215**. For embodiments where key derivation algorithm **503** comprises an ECDH key exchange, the key exchange token **506** can a common base point G. The base point G could also be (i) recorded in an eUICC profile **107***d*, or (ii) sent from a mobile network operator **104** to module **101**, or (iii) sent from the module **101** to the mobile network operator **104**. Other algorithms besides an ECDH or Diffie Hellman key exchange can be utilized as well at a step **503**, including a key exchange according to the American National Standards Institute (ANSI) standard X-9.63, and a key exchange token **506** could include a number or value associated with these other algorithms for a key derivation algorithm **503**.

For an eUICC key exchange algorithm **505**, a module **101** with an eUICC **107** could input the eUICC private key **215** and the mobile network operator public key **502** into a key derivation algorithm **503**. Note that the input into the key derivation algorithm **503** could also optionally include a key exchange token **506**. The key derivation algorithm **503** in an eUICC key exchange algorithm **505** could accept the input and output the second key K **204**. The key derivation algorithm **503** in an eUICC key exchange algorithm **505** could be equivalent to the key derivation algorithm **503** in a MNO key exchange algorithm **504** described above. The key exchange token **506** in an eUICC key exchange algorithm **505** could comprise a value similar to the key exchange token **506** used in a MNO key exchange **504** described above. In a Diffie-Hellman key exchange for a key derivation algorithm **503** in a eUICC key exchange algorithm **505**, the key exchange token **506** can comprise a value of either (i) integers p and g as described in a MNO key exchange **504**, or (ii) number g^a mod p. In an ECDH key exchange for key derivation algorithm **503** in a eUICC key exchange algorithm **505**, the key exchange token **506** can comprise a base point G. A key derivation algorithm **503** can output a second key K **204**. Other possibilities exist as well for the use of PKI keys and tokens in key exchange algorithms for those of ordinary skill in the art without departing from the scope of the present invention.

FIG. **5***c*

FIG. **5***c* is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments. System **500** can include an eUICC subscription manager **109**, an IP network **111**, a mobile network operator **104**, a mobile device **101**. A module **101** can include a network application **101***x* and an eUICC **107**. The operation of a system **500** can be similar to a system **300** in FIG. **3**, except for the steps noted in this FIG. **5***c* where different steps can be taken than those within a FIG. **3**. As depicted for a system **500** in FIG. **5***c*, like numerals for steps and messages for a system **500** in FIG. **5***c* can comprise like steps and messages within a FIG. **3**. Different numerals discussed below can comprise different steps or messages for a system **500**. Many of the same steps common for a system **500** in FIG. **5***c* and a system **300** in FIG. **3** will be summarized in this FIG. **5***c*, while differences between the two systems (including the use of different numerals for different steps or messages) are described in more detail herein. As described in a step **302***a* and **302***b* in FIG. **3**, a mobile network operator **104** can send the eUICC subscription manager **109** information for a profile **107***d* in a step **302***a* or **302***b*, where the information can include the network parameters **201**, the first network module identity **202**, and the first key K **203**. The listed exemplary data for a

Petitioner Samsung Ex-1004, 0054

profile **107***d* from the previous sentence are also discussed for a profile **107***d* in FIG. **2***a*.

For a step **507** in a system **500**, the MNO **104** can omit sending an encrypted second key K **204***a* in a ciphertext **208***b* within the data for the profile **107***d*. In other words, the profile **107***d* can omit the second key K **204** in either a plaintext or ciphertext form after a step **507** in a system **500**. The second key K **204** for a module **101** with eUICC **107** can be derived by a mobile network operator **104** in a MNO key exchange algorithm **504** and an eUICC key exchange algorithm **505** below in FIG. **5***c*. Thus, in an embodiment illustrated in FIG. **5***c*, the second key K **204** for a second authentication **310** does not need to be transferred to the eUICC subscription manager **109** from MNO **104** for the eUICC subscription manager **109** to include in a profile **107***d*. Similarly, in a system **500**, the second key K **204** does not need to be transferred to the eUICC **107** in a profile **107***c*. In embodiments where (x) the MNO sends network access credentials such as the first and second network module identities **202** and **209***a* and a first key K **203** are sent in a step **302***b*, then (y) a step **507** to omit the sending of the second key K **204** could take place with a step **302***b* instead of the step **302***a* as depicted. The MNO **104** can send the first and second network module identities **202** and **209***a* and a first key K **203** in a step **302***a* or a step **302***b* to the eUICC subscription manager **109**. The MNO **104** can send to the eUICC subscription manager **109** the first and second network module identities **203** and **209***a* and a first key K **203** in a profile **107***d* in a step **302***a* or **302***b*, and the eUICC subscription manager **109** could receive the first and second network module identities **202** and **209***a* and a first key K **203** in a step **302***a* or a step **302***b*. Other possibilities for combinations of data sent from a MNO **104** to an eUICC subscription manager **109** in a step **302***a*, **302***b*, and **507** without departing from the scope of the present invention.

As depicted in FIG. **5***c*, an eUICC **107** in module **101** could perform steps **301**, then step **205** to receive a profile **107***c*, then receive an eUICC profile key **107***b*, and then convert the profile **107***c* into a profile **107***d* using the eUICC profile key **107***b* in a step **206**. The eUICC profile key **107***b* could also be (i) ciphered with a key ciphering algorithm **216**, sent from the eUICC subscription manager **109** as an encrypted eUICC profile key **218**, (ii) and then deciphered by a module **101** and/or eUICC **107** with a step **217**, as described in connection with FIG. **2***e* above. The module **101** and/or an eUICC **107** could (i) receive an encrypted eUICC profile key **107***b* in the form of an key **218** and (ii) use a key deciphering algorithm **217** to decrypt the encrypted eUICC profile key **107***b* in order (iii) to read a plaintext eUICC profile key **107***b* and then (iv) use the plaintext eUICC profile key **107***b* to decrypt the ciphertext **208***a*.

As depicted in FIG. **5***c*, after a module **101** sends a eUICC identity **107***a* and receives an eUICC profile **107***c* in a step **205**, the module **101** can conduct a step **206** in order to decrypt a ciphertext **208***a* that can include a first key K **203** using an eUICC profile key **107***b*. For the embodiments contemplated in FIG. **5***c*, where the second key K **204** can be derived or determined using a key exchange in steps **504** and **505** below, the second network module identity **209***a* can be included in the ciphertext **208***a* (as opposed to being included in the ciphertext **208***b* as depicted in FIG. **2***a*). One reason can be that a ciphertext **208***b* can be omitted from an eUICC profile **107***d* in embodiments where the second key K **204** can be mutually derived by the eUICC **107** and the MNO **104**, so there may be no need to include a separate ciphertext **208***b* within the eUICC profile **107***d*.

After reading a first network module identity **202** and the first key K **203**, the module **101** can conduct a first authentication **304**. Note that the first key K **203** can comprise key with a null value, as contemplated in wireless network **102** standards which support the use of emergency services where a module **101** may not include a valid first key K **203**. In this case where the first key K **203** comprises a null value, the use of a ciphertext **208***a* can also be optionally omitted, such that the receipt of an eUICC profile key **107***b* and the use of a ciphertext **208***a* could also be optionally omitted and a profile **107***c* could include plaintext for the first key K **203** and network module identity **202**. As depicted and described in connection with FIG. **3**, a module **101** and MNO **104** could conduct a first authentication step **304** in order to authenticate the module **101** using the first key K **203**. The first key K could comprise a non-null value in exemplary embodiments. A step **306** to calculate a first RES **119** value using the first key K **203** from a profile **107***d* could be included in a first authentication step **304**.

The mobile network operator **104** could compare the first received RES **119** with a recorded RES **119** in order to authenticate the module **101** with the eUICC **107** in a step **308***a*. A mobile network operator **104** can authenticate the module **101** using a step **308***a* in order to provide access to the IP network **111**, and the access to the IP network **111** can be limited (such as, but not limited to excluding access to the public Internet after a step **308***a*). The module **101** could use access to the limited or restricted IP network **111** in order for a user **113** of module **101** to conduct an authentication with the mobile network operator **104** using a second factor, as described in a step **308***b* in FIG. **3**.

After authenticating the module **101** with the first network module identity **202** and the first key K **203** in a step **308***a*, the mobile network operator **104** could authenticate a user **113** or verify a M2M service provider **115** is associated with the module **101** in a step **308***b*. The authentication of a user **113** or M2M service provider **115** in a step **308***b* could comprise authenticating module **101** and/or eUICC **107** with a second factor, where the second factor comprises or includes a secure association of a user **113** or M2M service provider **115** with the module **101**. As described in FIG. **3** above, a step **308***b* could result in the secure association of an identity for the user **113** or the M2M service provider **115** with an identity of the module **101**. After conduction a step **308***b* as depicted and described in connection with FIG. **3** above, the MNO **104** can record the second network module identity **209** in the eUICC profile **107***d* is associated with a particular user **113** or a particular M2M service provider **115**.

In a step **308***b*, the MNO **104** can also determine (i) the first network module identity **202** used in step **304** is associated with other identities such as module identity **110**, profile identity **107***e*, eUICC identity **107***a*, and the second network module identity **209**. By (i) authenticating a user **113** or (ii) verifying an identity for module **101** is associated with a M2M service provider **115** in a step **308***b*, MNO **104** can determine the second network module identity **209** (used in a subsequent authentication step **310**) belongs to or is associated with a particular user **113** or M2M service provider **115**. In other words, without a separate authentication step **308***b* in FIG. **5** and FIG. **3**, MNO **104** may not be able to securely determine that the second network module identity **209** from a profile **107***d* belongs to a particular user **113** or M2M service provider **115**. For embodiments where the module **101** is associated with a M2M service provider **115**, then a step **308***b* in FIG. **5***c* could comprise the MNO **104** verifying that an identity received in

Petitioner Samsung Ex-1004, 0055

a first authentication **304** (such as, but not limited to, the first network module identity **202**) is associated with an M2M service provider **115**, such as checking the identity in a list of identities for modules **101** belonging to M2M service provider **115**.

After successfully authenticating or verifying an identity of a user **113** or an M2M service provider **115** is associated with module **101** in a step **308***b*, MNO **104** could process an MNO key exchange algorithm **504** in order to record a second key K **204** for use in a subsequent second authentication **310** for module **101**. The second authentication **310** can use different network access credentials (i) associated with the module **101** and (ii) obtained by module **101** using an eUICC key exchange algorithm **505**. Although not illustrated in FIG. **5***c*, a MNO **104** could obtain the data for processing a MNO key exchange algorithm **504** in several different ways. A MNO **104** could receive the eUICC public key **214** for an MNO key exchange algorithm **504** from either (i) the module **101** or eUICC **107** directly after the first authentication **304** or (i) the eUICC subscription manager **109** in a step **302***b* above, where the eUICC subscription manager **109** could record the eUICC public key **214**. Other possibilities exist as well for a MNO **104** to receive an eUICC public key **214** associated with an identity for module **101** such as the eUICC identity **107***a*. The recording of an eUICC public key **214** with an MNO **104** is also depicted and described in connection with FIG. **5***a* above.

For a MNO key exchange algorithm **504** in FIG. **5***c*, the MNO **104** could also input a key exchange token **506** and a MNO private key **501**, in addition to the eUICC public key **214**, as illustrated in FIG. **5***b* above. After performing a MNO key exchange algorithm **504** in FIG. **5***c*, the MNO **104** can record the second key K **204** for the second module identity **209** (which is associated with the first module identity **202** in the profile **107***d*). As contemplated for a key exchange token **506** in FIG. **5***a* and FIG. **5***c*, the key exchange token **506** could be any of the cases (A) initially processed, derived, or determined by the MNO **104**, (B) shared between the MNO **104** and module **101** with the eUICC **107**, such as, but not limited to, recording the key exchange token **506** in the profile **107***d*, or (C) initially processed, derived, or determined by module **101**. FIG. **5***c* illustrates an embodiment for case (A) with key exchange token **506**, where the MNO **104** derives or determines the key exchange token **506** value and subsequent sends the key exchange token **506** value to the module **101** with the eUICC **107**. The MNO **104** can send the key exchange token **506** in a message **508**, and a network application **101***x* for the module **101** can receive the key exchange token **506** in the message **508** and forward the key exchange token **506** to the eUICC **107**. For case (A) the MNO **104** can omit sending the key exchange token **506** until after the user **113** or M2M service provider **115** for module **101** has been successfully authenticated or verified in a step **308***b*.

In a related embodiment to the embodiment depicted in FIG. **5***c*, for case (B) with key exchange token **506**, a separate message **508**, to communicate or transfer the key exchange token **506** between the MNO **104** and module **101** after a step **504**, can optionally be omitted, since both sides (MNO **104** and module **101**) could record the key exchange token **506** before a step **505** by a module **101** with an eUICC **107** below. For case (B), the MNO **104** could send a signal in a message **508** to the module **101** that the authentication step **308***b* of a user **113** or an M2M service provider **115** has been successfully completed, and thus module **101** could proceed with an eUICC key exchange algorithm **505** using the recorded key exchange token **506**.

For case (C) with key exchange token **506**, the eUICC **107** could derive or determine the key exchange token **506** and subsequently send the key exchange token **506** to the MNO in a message **508**. In this case (C), the MNO **104** could receive the key exchange token **506** (*i*) before processing the MNO key exchange algorithm **504**, and (ii) using the connection with the module **101** from the first authentication **304**. For case (C), the MNO **104** can require the successful completion of an authentication step **308***b* for a user **113** or M2M service provider **115** before accepting the key exchange token **506** from the module **101**.

In another exemplary embodiment, step **504** and step **505** can use different values for the key exchange token **506**, and both MNO **104** and module **101** can send the tokens **506** in a message **508** to the other node. In exemplary embodiments, a message **508** comprising the key exchange token **506** can be transferred through the IP network **111**, where access to the IP network **111** can be enabled by the first authentication **304** with the first key K **203**. Other possibilities exist as well for the transfer of a key exchange token **506** between a MNO **104** and a module **101** with an eUICC **107** for conducting a key exchange without departing from the scope of the present invention.

As depicted in FIG. **5***c*, a module **101** with an eUICC **107** can conduct an eUICC key exchange algorithm **505** in order to determine or read a second key K **204**. As depicted and described for an eUICC key exchange algorithm **505** in FIG. **5***b* above, the module **101** can input an MNO public key **502**, an eUICC private key **215**, and the key exchange token **506** into a key derivation algorithm **503** in order to output the second key K **204**. Note that the number, value, or sequence of bits for the second key K **204** determined by a MNO **104** in a step **504** can be equal to the number, value, or sequence of bits for the second key K **204** determined by a module **101** with an eUICC **107** in a step **505**. The mutual derivation of the second key K **204** by a MNO **104** in a step **504** and a module **101** in a step **505** can be different and superior to conventional technology for either (i) a physical UICC or (ii) an eUICC, since the second key K **204** does not need to be transferred in either physical or electronic form, where the electronic form could include encrypting the second key K **204** into a ciphertext. Supporting the derivation of a second key K **204** as depicted and described herein can be superior to the electronic or physical distribution of a key K, since a different second key K **204** can be utilized by repeating steps **504** and **505** a second time, such as with a different key exchange token **506**. In this manner, the second key K **204** associated with the second network module identity **209** could be rotated or changed periodically, thereby increasing the security of a system **500** compared to the use of a static, non-changing second key K **204** for the lifetime of a module **101** with a profile **107***d*.

After a step **505** in FIG. **5***c*, the subsequent steps and messages for communication between the module **101** and the MNO **104** can be the same or equivalent to those in FIG. **3** after a step **207**. In other words, the second key K **204** as used by a module **101** and/or eUICC **107** for embodiments in a FIG. **5***c* can be equivalent or similar to the processing and recording steps depicted and described in FIG. **3**, upon module **101** with an eUICC **107** reading the second key K **204** in a step **207** in FIG. **3**. In a system **500**, the module **101** or eUICC **107** could record the second key K **204** in a protected, nonvolatile memory as described in a step **207** of FIG. **3**. Other possibilities exist as well without departing from the scope of the present invention for the location or techniques of storing the second key K **204** resulting from a step **505**.

Petitioner Samsung Ex-1004, 0056

As depicted and described in connection with FIG. **6** below, the module **101** could record the second key K **204** in a volatile memory (and not storing the second key K **204** in nonvolatile memory), including potentially only within a register or cache memory of CPU **101***b*. In this manner, the security of the derived second key K **204** can be enhanced, since upon or after power off of a module **101**, a third party could not probe or read nonvolatile memory looking for the second key K **204**. Since a volatile memory could be flushed upon loss of power or other circumstances, a MNO **104** and module **101** could repeat the steps **504** and **505**, respectively, including the transfer of a key exchange token **506**, a subsequent time when a module **101** needs to process or derive a new, subsequent second key K **504**. In other words, a module **101** can conduct a step **505** with a different key exchange token **506** at a later time after the first instance of a step **505** in order to derive a different, subsequent second key K **204**.

After deriving the second key K **204** in a step **505** in FIG. **5***c*, the module **101** with the eUICC **107** can authenticate with the MNO **104** using the wireless network **102**, the second network module identity **209**, the second key K **204**. The module **101** could conduct a second authentication **310** with the mobile network operator using the second key K **204**, as depicted in FIG. **5***c*, which is also equivalent to the second authentication **310** depicted in FIG. **3** above. Note that the module **101** could detach or disconnect from the wireless network **102** (*i*) after a sending/receiving a message **508** with key exchange token **506** and (ii) before sending the exemplary second attach message **303** with the second network module identity **209**.

The eUICC **107** within module **101** could use (i) the second key K **204** from a step **505**, and (ii) a second RAND **118** value from the MNO **104** to calculate a second RES **119** value in a step **311**. The eUICC **107** can send the second RES **119** to the network application **101***x*, and the module **101** can send the second RES **119** to the mobile network operator **104** through the wireless network **102**. The MNO **104** could compete the second authentication in a step **312** by verifying the second RES **119** is correct using (i) the second key K **204** derived by the MNO **104** in a step **504** above, and (ii) the second RAND **118** value sent to the module **101**. Upon successful authentication using the second key K **204**, as depicted and described in connection with FIG. **3**, the module **101** and MNO **104** could take subsequent steps after a step **312** for the module **101** to have access to the IP network **111** and also the public Internet.

In another embodiment contemplated in FIG. **5***c*, the mobile network operator **104** can send the second key K **204** to the module **101** using the wireless network **102** in a message **508**. In other words, the exemplary token **506** in FIG. **5***c* could comprise the second key K **204**, as opposed to an exemplary key exchange token **506**. In this embodiment, the use of a key derivation algorithm **503** in a step **504** could use input of a random number from random number generator **128** into the key derivation algorithm **503** (instead of PKI keys), and the output could be the second key K **204**. Or, the key derivation algorithm **503** in a step **504** could simply assign a random number to the second key K **204**. After a step **308***b* and step **504**, the mobile network operator **104** could send the second key K **204** in a message **508**. The second key K **204** in a message **508** could be encrypted using a key ciphering algorithm **216**. The message **508** with the second key K **204** as the token **506** could be received by the module **101** and decrypted using a key deciphering algorithm **217**. In another embodiment, the token **506** received by a module **101** could comprise (i) the second key K **204** as plaintext at the application layer, but (ii) ciphered at the data-link layer using the first RAND value from a step **304** and the first key K **203**. Other possibilities exist as well for a token **506** to comprise a second key K **204** without departing from the scope of the present invention.

The order of many of the steps and messages depicted within a system **500** could be changed without departing from the scope of the present invention. For example, a step **504** could also be conducted concurrently with a step **302***b* (instead of with a step **308***b*), such that a mobile network operator **104** could calculate a second key K **204** using a MNO key exchange algorithm **504** at the same time when MNO **104** sends the first network module identity **202** and first key K **203** to the eUICC subscription manager **109**. After receiving (i) an eUICC identity **107***a* from an eUICC subscription manager **109** and (ii) and an eUICC public key **214** in a step **302***b*, the mobile network operator **104** can process a MNO key exchange algorithm **504** in order to calculate or process a second key K **204**.

In an exemplary embodiment, a mobile network operator **104** could receive a list of eUICC public keys **214** and eUICC identities **107***a* from an M2M service provider **115** before eUICC subscription manager **109** receives the eUICC identity **107***a* in a step **205**. The MNO **104** could use the data received from a M2M service provider **115** (including a list of eUICC identities **107***a* and eUICC public keys **214**) in order to derive the second key K **204** using a MNO key derivation algorithm **504** and the key exchange token **506**. The MNO **104** could send the key exchange token **506** to an eUICC subscription manger **109** before the eUICC subscription manager **109** participates in a step **205** as illustrated in FIG. **5***c*, and the eUICC subscription manager **109** could include the key exchange token **506** with the eUICC profile **107***c*, such that module **101** could receive the key exchange token **506** in the eUICC profile **107***c*.

In this embodiment (which can also comprise a case (B) for the transfer of key exchange token **506** for a message **508** as described above), a module **101** using an eUICC **107** with profile **107***d* and key exchange token **506** could potentially derive the second key K **204** before a step **308***b*, but in preferred embodiments the mobile network operator **104** does not allow the use of the second key K **204** until after an authentication step **308***b* of a user **113** or M2M service provider **115**. In another embodiment, the values for the first network module identity **202** and the second network module identity **209** could be the same or equal, such that the module **101** uses the same network module identity for both first authentication **304** and a second authentication **310**. In this case, the MNO **104** can support a change in key K used with the first network module identity **202** from the first key K **203** to the second key K **204**. The first key K **203** can be included in a profile **107***d*, but the second key K **204** can be derived by an MNO **104** using a step **504** and a module **101** using a step **505**. Other possibilities exist as well for a MNO **104** and a module **101** to mutually derive a second key K **204** for use with an eUICC **107** without departing from the scope of the present invention.

FIG. **6**

FIG. **6** is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments. An exemplary system **500** depicted and described in connection with FIG. **5***c* can also support the repeated derivation of a second key K **204** for a MNO **104** and module **101** with an eUICC **107**. The use and support for different second keys K **204** over time can increase security, since the second key K **204** can be securely and periodically rotated, thereby

Petitioner Samsung Ex-1004, 0057

enhancing the security and efficiency of a system **500**, compared to either (i) physically changing a UICC each time a new key K is desired, or (ii) querying, downloading, and selecting a new profile **107***c* or profile **107***d* each time the use of a different key K is desired (including steps to communicate and record a second key K **204** in the profile **107***d*). In other words, the use of multiple second keys K **204** over time can be accomplished for the same profile **107***d*.

A step **403** in FIG. **6** can comprise a module **101** with an eUICC **107** conducting the substeps for a step **403** as depicted and described in connection with FIG. **4**. In a step **403**, a module **101** could connect with a first wireless network **102**, receive an eUICC profile **107***c*, decrypt the profile **107***c* using an eUICC profile key **107***b*, activate the profile **107***d*, and authenticate with a second wireless network **102** using a first key K **203** from the profile **107***d*. As noted above, other possibilities exist as well for a module **101** to record an eUICC profile **107***d*, such as the loading of a profile **107***d* by a manufacturer, without departing from the scope of the present invention.

After successful authentication of the module **101** at the conclusion of a substep **304** in a step **403**, a user **113** associated with the module **101** could conduct an authentication step **308***b* with the mobile network operator **104**. A step **308***b* can be useful for a mobile network operator **104** to authenticate or securely associate (i) a module **101** with (ii) a legal entity contractually responsible for the services used by a module **101**. The use of a step **308***b* is also described in FIG. **3**. Note that module **101** could be associated with an M2M service provider **115** instead of a mobile phone subscriber such as an individual, and in this case the M2M service provider **115** could take steps before a step **308***b* in order to inform or confirm with MNO **104** that module **101** with an identity such as module identity **110** or the first network module identity **202** belongs to or is associated with the M2M service provider **115**.

In other words, a MNO **104** may not have control over the distribution or recipient of a profile **107***c* from an eUICC subscription manager **109** in a step **403**, and a user authentication in a step **308***b* allows a MNO **104** to confirm, verify, or establish a contractual relationship with a user **113**. Business contracts and procedures for an MNO **104** to provide service to a module **101** with an eUICC **107** with profile **107***d* could require that a user **113** successfully completes an authentication step **308***b* (with example steps described in FIG. **3** above), before the MNO **104** provides service such as voice calls or access to the public Internet. The second factor in a step **308***b* can be data communicated between the MNO **104** and the user **113** to confirm an identity of the user **113**. Examples of data for the second factor in a step **308***b* are described in connection with a step **308***b* in FIG. **3**. The first factor contemplated in a system **300** or system **500** can be the successful receipt of a RES **119** value in a first authentication **304**. Upon conclusion of the step **308***b* the MNO **104** could securely determine and record that a module **101** with the first network module identity **202** and/or the second network module identity **209** from the profile **107***d* is associated with an authenticated user **113**.

The module **101** could then perform a step **508** in order access a key exchange token **506**. As described for a key exchange token **506** in FIG. **5***c*, the module **101** could receive the token **506** in a step **508** (case A), or the module **101** could send the token **506** in a step **508** (case B). Step **508** can comprise sending or receiving the message **508** from FIG. **5***c*. The key exchange token **506** could comprise a key exchange token **506** as depicted and described in connection with FIG. **5***b*. Or, as described for a message **508** in FIG. **5***c*, the key exchange token **506** could comprise the second key K **204**, such as the second key K **204** encrypted by MNO **104** with a key ciphering algorithm **216** and decrypted by the module **101** with the eUICC **107** using a key deciphering algorithm **217**. The key exchange token **506** at a step **508** could comprise parameters for a key derivation algorithm **503**, such as a base point G if elliptic curve cryptography PKI keys are used with MNO public key **502**, MNO private key **501**, eUICC public key **214**, and eUICC private key **215**.

In another exemplary embodiment, key exchange token **506** with a Diffie Hellman key exchange for a key derivation algorithm **503** could comprise a multiplicative group of integers modulo p, where p is prime and g is primitive root mod p. Other possibilities for a key exchange token **506** in a message **508** exist as well without departing from the scope of the present invention, including the use of multiple values and numbers for a key exchange token **506**. The key exchange token **506** transfer between MNO **104** and module **101** in a step **508** can use the second wireless network after the module **101** authenticates with the first key K **203**, and thus the data-link layer for transfer of the key exchange token **506** could be ciphered using the first key K **203** (where a cipher key for the data-link layer is derived from the first key K **203** and a RAND **118** from a first authentication **304**).

A module **101** with an eUICC **107** could then perform a step **505**, which could comprise an eUICC key exchange algorithm **505** as depicted in FIG. **5***c* using (i) the token **506** from a message **508** above, and (ii) the eUICC private key **215** and MNO public key **502**. The output from an eUICC key exchange algorithm **505** can comprise the second key K **204**. In an exemplary embodiment, the second key K **204** output from the eUICC key exchange algorithm **505** is recorded within a memory of module **101** on a temporary basis. After obtaining and reading the second key K **204** from a step **505**, the module **101** can conduct a second authentication **310** with the MNO **104** using the second key K **204**. The second key K **204** can be associated with a second network module identity **209**, which could be recorded in the profile **107***c* and profile **107***d* for the eUICC **107** from a step **403** above. Exemplary details and steps for a second authentication **310** using the second key K **204** are depicted and described in connection with FIG. **3** and FIG. **5***c* above.

After the conclusion of the second authentication **310**, the module **101** could have access to the public Internet through the IP network **111** of the wireless network **102**. After a step **310** and before a subsequent step **601** below, the module **101** could continue using the second key K **204** with the second network identity **209** in many additional repeated steps **310**, such that module **101** could use the second key K **204** for an exemplary period of time such as several days or several months, and other possibilities exist as well for the continued use of a second key K **204** after a step **310** and before a step **601** in FIG. **6**. For example, a module **101** could repeat a step **311** in a second authentication **310** multiple times with the same wireless network **102** using the same number of value for the second key K **204** during a period of time before a step **601**.

At a step **601** in FIG. **6**, a module **101** or a MNO **104** could determine if the use of a new second key K **204** is required or preferred. There could be several reasons that a different second key K **204** may be periodically preferred. Exemplary reasons include (i) the second key K **204** may only be temporarily stored within a volatile memory in CPU **101***b*, such that a power cycle of module **101** or CPU **101***b*

Petitioner Samsung Ex-1004, 0058

could flush the volatile memory, and in this case module **101** and MNO **104** may need to derive a new second key K **204**, (ii) ownership of module **101** may change, and business or legal contracts could stipulate that a previous second key K **204** with the prior owner of module **101** may no longer be valid and thus a new second key K **204** may be required, (iii) a MNO **104** and a module **101** or M2M service provider **102** may prefer to periodically rotate the second key K **204** in order to increase security of a system **500**. For example, a module **101** may have a planned lifetime of more than a decade, and given the speed of change for mobile networking technology, a module **101** may prefer to support the change in a second key K **204** for accessing a wireless network **102** without downloading and installing a new, different profile **107***d*. Other possibilities exists as well for exemplary reasons why a module **101** and/or a MNO **104** could determine that the use of a new, second key K **204** is preferred or required in a step **601** without departing from the scope of the present invention. If a module **101** or MNO **104** determine a value of "no" for a step **601**, then the module **101** could continue periodically performing repeated second authentication **310** steps using the same second key K **204**, as illustrated in FIG. **6**.

As depicted in FIG. **6**, upon determination of a value of "yes" for a step **601**, a module **101** could return to a step **508** and receive another key exchange token **506**. As depicted in FIG. **6**, the module **101** could use a first authentication **304**, which could comprise an authentication with the first key K **203**. A return to the first authentication **304** with the first key K **203** could be omitted in some embodiments, and thus the box for **304** depicted in FIG. **6** is a dashed line.

In this embodiment where module **101** or MNO **104** determine or evaluates that a new second key K **204** is preferred at a step **601**, the module **101** could return to a step **508** by attaching with the wireless network **102** again using the first network module identity **202** and the first key K **203**. For example, if the second key K **204** is not available (such as being flushed from being stored only in a volatile memory, a potential error condition such as a reset of module **101**, or the second key K **204** is no longer preferred to be used), then the module **101** with the eUICC **107** could use data recorded in the profile **107***d* to reconnect with the wireless network **102**. For example, the first key K **203** and the first network identity **202** may be recorded in generally accessible nonvolatile memory, such as, but not limited to, a flash memory **101***w* within module **101** and subsequently the first key K **203** and the first network identity **202** could be used in a step **304** before a return to a step **508**. Or, the module **101** and MNO **104** could continue to use the previous second key K **204** (if available) for a communications link to transfer the key exchange token **506**, and thus the use of a step **304** with the first key K **203** is optional.

Upon return to a step **508** module **101** and MNO **104** could transfer a key exchange token **506** as described in a step **508** in FIG. **6** above. Upon return to a step **508**, the module **101** and MNO **104** could transfer a key exchange token **506** that has a different value or number from a key exchange token **506** transferred earlier (in order to support the derivation of a different second key K **204** than from a previous iteration). Using the new, different value for the key exchange token **506**, the module **101** with the eUICC **107** could derive a new, different second key K **203**. In this manner and by using the steps illustrated in FIG. **6**, a second key K **204** could operate as a key K for "temporary use", and a different second key K **204** for use in a subsequent authentication **310** could be obtained by a repeated use of a step **505** with a new, different key exchange token **506** for module **101** connecting with the same wireless network **102**.

The module **101** and MNO **104** could continue to use the same network module identity (such as a second network module identity **209**) upon a return to steps **508** through **310**, or the MNO **104** could also send the module **101** a new, different network module identity in a message **508** upon a return to steps **508** through **310**. A MNO **104** and a module **101** can repeat the use the steps **508** through **601** depicted and described in this FIG. **6** in order to derive a series over time of second keys K **204** for the module **101** with the eUICC **107**. Each member of the series (comprising a different second key K **204**) could be associated with the second network module identity **209**, and the second network module identity **209** could remain constant or can also change to different numbers or values for use in a step **310**. Supporting a change in the second key K **204** can both increase the flexibility and security of a system **500** and related systems for a user and a mobile network operator **104**.

CONCLUSION

Various exemplary embodiments have been described above. Those skilled in the art will understand, however, that changes and modifications may be made to those examples without departing from the scope of the claims.

What is claimed is:

1. A method comprising:

(a) generating a first message comprising:
  (1) an identity of an embedded universal integrated circuit card (eUICC);
  (2) a nonce; and
  (3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;

(b) sending the first message via a network application to a subscription manager system;

(c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;

(d) storing a subscription manager public key which corresponds to a subscription manager private key;

(e) deriving a profile key using a key exchange algorithm based on at least:
  (i) the second eUICC private key, and
  (ii) the stored subscription manager public key, wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key;

(f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;

(g) receiving the symmetric key;

(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;

(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and

(j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.

Petitioner Samsung Ex-1004, 0059

2. The method of claim **1**, wherein the subscription manager public key is downloaded via the network application.

3. The method of claim **1**, wherein the step of storing the subscription manager public key occurs at the time of manufacture of the embedded universal integrated circuit card.

4. The method of claim **1**, wherein the key exchange algorithm is a Diffie-Hellman key exchange.

5. The method of claim **1**, wherein the key exchange algorithm is an Elliptic Curve Diffie-Hellman key exchange.

6. The method of claim **1**, wherein the encrypted profile is encrypted in a manner so that intermediate nodes on an IP network would not be able to read data within the profile in an unencrypted form.

7. The method of claim **1**, wherein subscription manager system stores the ciphertext and the symmetric key before step (a).

8. The method of claim **1**, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the identity of the embedded universal integrated circuit card included in the first message.

9. The method of claim **1**, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the digital signature included in the first message.

10. The method of claim **1**, wherein the decrypted ciphertext is stored in nonvolatile memory of the embedded universal integrated circuit card.

11. The method of claim **1**, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a machine-to-machine module.

12. The method of claim **11**, wherein the module comprises a module of a type selected from the group consisting of: vending machine, automobile, alarm system, tracking device, monitoring device, security system and remote control device.

13. The method of claim **1**, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a wireless module.

14. The method of claim **13**, wherein the module is configured to communicate using one or more wireless technologies of types selected from the group consisting of: WiFi, WiMax, General Packet Radio Services, Enhanced Data rates for GSM Evolution and 3rd Generation Partnership Project technology.

15. The method of claim **13**, wherein the module comprises a module of a type selected from the group consisting of the following: wireless handset, cellular phone, smartphone, laptop computer, tracking device, computer with a radio, circuit board with a radio, hand-held device, netbook, portable computer, multiprocessor system, microprocessor based consumer electronic, programmable consumer electronic, network personal computer, minicomputer, mainframe computer and smartcard.

16. The method of claim **1**, wherein the embedded universal integrated circuit card is operably connected to a module, wherein the module is a wired module.

17. The method of claim **16**, wherein the module is configured to communicate using one or more wired connections of types selected from the group consisting of: Ethernet, fiber optic connection and Universal Serial Bus connection.

18. The method of claim **16**, wherein the module comprises a module of a type selected from the group consisting of: computer, security camera, security monitoring device and networked controller.

19. The method of claim **1**, wherein the deriving step (c) is performed prior to the generating step (a).

20. The method of claim **1**, wherein the generating step (a) is performed before the deriving step (c).

21. The method of claim **1**, wherein the embedded integrated circuit card is operably connected to a module and a user accesses a user interface of the module to enter authentication information before the module receives the symmetric key.

22. The method of claim **1**, wherein the subscription manager receives the ciphertext from a mobile network operator before the network application sends the first message.

* * * * *

Petitioner Samsung Ex-1004, 0060

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/416,534	01/18/2024	John A. Nix	63121/0226	7559

1912 7590 01/21/2025

AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

EXAMINER
HO, DAO Q

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
01/21/2025	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Petitioner Samsung Ex-1004, 0061

APPLICATION NO.	ISSUE DATE	PATENT NO.
18/416,534	21-Jan-2025	12207094

AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
NEW YORK, NY 10174

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at https://patentcenter.uspto.gov

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit https://www.uspto.gov/electronicgrants

Petitioner Samsung Ex-1004, 0062

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/416,534	01/21/2025	12207094	63121/0226	7559

1912 7590 01/01/2025

AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at https://patentcenter.uspto.gov/. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at https://certifiedcopycenter.uspto.gov/index.html. The Certified Copy Center may be reached at (800)972-6382.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Center (https://patentcenter.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

Petitioner Samsung Ex-1004, 0063

INVENTOR(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional inventors):

John A. Nix, Evanston, IL;

APPLICANT(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional applicants):

Network-1 Technologies, Inc., New York, NY;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Petitioner Samsung Ex-1004, 0064

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

1912 7590 12/03/2024
AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

Keith J. Barkaus	(Typed or printed name)
/Keith J. Barkaus/	(Signature)
December 11, 2024	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/416,534	01/18/2024	John A. Nix	63121/0226	7559

TITLE OF INVENTION: Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	03/03/2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, DAO Q	2432	713-171000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Amster, Rothstein & Ebenstein LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Network-1 Technologies, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): New York, NEW YORK

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☑ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☑ Electronic Payment via the USPTO patent electronic filing system ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 011785

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Keith J. Barkaus/ Date December 11, 2024

Typed or printed name Keith J. Barkaus Registration No. 51,431

PTOL-85 Part B (11/23) Approved for use through 03/31/2026 OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Petitioner Samsung Ex-1004, 0065

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	**12/11/2024 04:49:03 PM Z ET**	**63121/0226**

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	68332247	AUTHORIZED BY	Keith Barkaus
CUSTOMER #	1912	FILING DATE	01/18/2024
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	John A. Nix

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1051	**E2024BAG49388538**	**Victoria GILMORE**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2501	UTILITY ISSUE FEE	480.00	1	480.00
			TOTAL AMOUNT:	**$480.00**

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	**12/11/2024 04:49:03 PM Z ET**	**63121/0226**

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	68332247	FILING DATE	01/18/2024
CUSTOMER #	1912	FIRST NAMED INVENTOR	John A. Nix
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Keith Barkaus

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
226-PTOL-85.pdf	1	Issue Fee Payment (PTO-85B)	127 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
226-PTOL-85.pdf	A3F2E1DEA8B4A46FF744769F3EB26BB481793BA6B1D5798B6DA562003A705FF0AF8A09DCA8BF5962A4A1F6B2DE901D63ED25705A041F4B1E465C45F7251ACA0D

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

1912 7590 12/03/2024

AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

EXAMINER	
HO, DAO Q	
ART UNIT	**PAPER NUMBER**
2432	

DATE MAILED: 12/03/2024

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/416,534	01/18/2024	John A. Nix	63121/0226	7559

TITLE OF INVENTION: Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	03/03/2025

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

Petitioner Samsung Ex-1004, 0070

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

1912 7590 12/03/2024

AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/416,534	01/18/2024	John A. Nix	63121/0226	7559

TITLE OF INVENTION: Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	03/03/2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, DAO Q	2432	713-171000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via the USPTO patent electronic filing system ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Petitioner Samsung Ex-1004, 0071

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/416,534	01/18/2024	John A. Nix	63121/0226	7559

1912 7590 12/03/2024

AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

EXAMINER	
HO, DAO Q	

ART UNIT	PAPER NUMBER
2432	

DATE MAILED: 12/03/2024

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Petitioner Samsung Ex-1004, 0072

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/ owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013).
https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf

Routine uses of the information in this record may include disclosure to:

1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
2) a federal, state, local, or international agency, in response to its request;
3) a contractor of the USPTO having need for the information in order to perform a contract;
4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
9) the Office of Personnel Management (OPM) for personnel research purposes; and
10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Notice of Allowability	Application No. 18/416,534	Applicant(s) Nix, John A.	
	Examiner DAO Q HO	Art Unit 2432	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☐ This communication is responsive to 11/04/2024.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-22 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/DAO Q HO/
Primary Examiner, Art Unit 2432

Petitioner Samsung Ex-1004, 0074

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

Response to Amendment

This is a reply to the application filed on 11/04/2024, in which, claim(s) **1-22** is/are pending.

Terminal Disclaimer

The terminal disclaimer filed on 11/04/2024 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of **Patent # 10,084,768, 10,382, 422 and 11,233,780** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Claim Rejections - 35 U.S.C. § 112:

Applicants' arguments with respect to 112 2nd paragraph with rejection of claim(s) 1-22 has been fully considered and are persuasive. The rejection has been withdrawn in view of the amendment to claim.

Allowable Subject Matter

Claims 1-22 are allowed.

The following is an examiner's statement of reasons for allowance:

This communication warrants No Examiner's Reason for Allowance as it was previously stated in the Non-Final Rejection filed on 9/18/2024, as such the reasons for allowance are in all probability evident from the record and no statement is deemed necessary (see MPEP 1302.14).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAO Q HO whose telephone number is (571)270-5998. The examiner can normally be reached on 7:00am - 5:00pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Nickerson can be reached on (469) 295-9235. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DAO Q HO/
Primary Examiner, Art Unit 2432

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/416,534	Nix, John A.
	Examiner	**Art Unit**
	DAO Q HO	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/17/2024	11/25/2024							
	1	✓	=							
	2	✓	=							
	3	✓	=							
	4	✓	=							
	5	✓	=							
	6	✓	=							
	7	✓	=							
	8	✓	=							
	9	✓	=							
	10	✓	=							
	11	✓	=							
	12	✓	=							
	13	✓	=							
	14	✓	=							
	15	✓	=							
	16	✓	=							
	17	✓	=							
	18	✓	=							
	19	✓	=							
	20	✓	=							
	21	✓	=							
	22	✓	=							

Petitioner Samsung Ex-1004, 0078

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/416,534	Nix, John A.
	Examiner	**Art Unit**
	DAO Q HO	2432

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08	09/17/2024	dh
H04W12/30 OR H04W12/06 OR H04L63/0853 OR H04L63/08	11/25/2024	dh

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
see attached SEARCH history	09/17/2024	dh
inventor and assignee in SEARCH	09/17/2024	dh
NPL: subscription authentication using SIM card with key exchange	09/17/2024	dh
CPC searches with delimiter	09/17/2024	dh
update	11/25/2024	dh

/DAO Q HO/ Primary Examiner, Art Unit 2432	

Petitioner Samsung Ex-1004, 0079

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/416,534	Nix, John A.
	Examiner	Art Unit
	DAO Q HO	2432

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
	general interference and searches of claim (PGPUB, USPAT)	09/17/2024	dh
	update	11/25/2024	dh

/DAO Q HO/ Primary Examiner, Art Unit 2432	

Petitioner Samsung Ex-1004, 0080

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/416,534	Nix, John A.
	Examiner	**Art Unit**
	DAO Q HO	2432

CPC						
Symbol					**Type**	**Version**
H04W	/	12	/	35	F	2021-01-01
H04L	/	9	/	0869	I	2013-01-01
H04L	/	63	/	0428	I	2013-01-01
H04L	/	9	/	0819	I	2013-01-01
H04L	/	9	/	3271	I	2013-01-01
H04W	/	4	/	70	I	2018-02-01
H04L	/	63	/	062	I	2013-01-01
H04L	/	63	/	08	I	2013-01-01
H04W	/	12	/	06	I	2013-01-01
H04B	/	1	/	3816	I	2013-01-01
H04L	/	63	/	0435	I	2013-01-01
H04L	/	63	/	06	I	2013-01-01
H04L	/	63	/	101	I	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 22	
/DAO Q HO/ Primary Examiner, Art Unit 2432 (Primary Examiner)	25 November 2024 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5B

U.S. Patent and Trademark Office — Part of Paper No.: 20241125

Petitioner Samsung Ex-1004, 0081

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/416,534	Nix, John A.
	Examiner	**Art Unit**
	DAO Q HO	2432

INTERNATIONAL CLASSIFICATION					
CLAIMED					
H04W	/	12	/	30	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 22	
/DAO Q HO/ Primary Examiner, Art Unit 2432 (Primary Examiner) 25 November 2024 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5B

Petitioner Samsung Ex-1004, 0082

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/416,534	Nix, John A.
	Examiner	**Art Unit**
	DAO Q HO	2432

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		10		19										
	2		11		20										
	3		12		21										
	4		13		22										
	5		14												
	6		15												
	7		16												
	8		17												
	9		18												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	22	
/DAO Q HO/ Primary Examiner, Art Unit 2432	25 November 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5B

U.S. Patent and Trademark Office Part of Paper No.: 20241125

Petitioner Samsung Ex-1004, 0083

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L2	76	((("NETWORK-1") near3 ("TECHNOLOGIES") near3 ("INC"))).AS,AANM.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2023/03/23 09:25 AM
L3	172	((("NIX") near3 ("John"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:25 AM
L4	268	2 3	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:25 AM
L5	1656	(eUICC WITH profile)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:33 AM
L6	60	4 AND 5	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:33 AM
L7	791	(mobile WITH eUICC WITH profile)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:33 AM
L8	42	4 AND 7	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:33 AM
L10	42	8 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:36 AM
L11	198	((authenticat$4 validat$6) WITH mobile WITH eUICC WITH profile)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 10:03 AM
L12	171	11 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 10:03 AM
L13	240	("10169587" OR "10621352" OR "20010029581" OR "20020018569" OR "20030003895" OR "20030211842" OR "20040162472" OR "20040179684" OR "20040221163" OR "20050008159" OR "20050021875" OR "20050050323" OR "20050058294" OR "20050120202" OR	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 10:11 AM

Petitioner Samsung Ex-1004, 0084

		"20050138353" OR "20050193199" OR "20050246282" OR "20050278787" OR "20060021063" OR "20060056355" OR "20060059344" OR "20060095771" OR "20060129848" OR "20060206710" OR "20060281442" OR "20070101400" OR "20070158439" OR "20070206799" OR "20080016230" OR "20080022089" OR "20080031204" OR "20080044032" OR "20080107083" OR "20080114978" OR "20080130879" OR "20080165698" OR "20080307218" OR "20090028341" OR "20090041110" OR "20090060197" OR "20090077643" OR "20090113203" OR "20090116642" OR "20090125996" OR "20090132806" OR "20090183541" OR "20090191857" OR "20090209232" OR "20090217348" OR "20090268909" OR "20090274306" OR "20090282246" OR "20090313472" OR "20100031042" OR "20100062808" OR "20100093347" OR "20100098253" OR "20100166167" OR "20100195833" OR "20100199334" OR "20100223461" OR "20100275028" OR "20110016321" OR "20110035584" OR "20110035604" OR "20110055553" OR "20110158411" OR "20110167272" OR "20110213959" OR "20110237281" OR "20110268022" OR "20110269422" OR					

Petitioner Samsung Ex-1004, 0085

		"20110269461" OR "20110269472" OR "20110270747" OR "20110291803" OR "20110314287" OR "20120011360" OR "20120011362" OR "20120023336" OR "20120030461" OR "20120033613" OR "20120072732" OR "20120084568" OR "20120087493" OR "20120089568" OR "20120108205" OR "20120117635" OR "20120159153" OR "20120170451" OR "20120190354" OR "20120214444" OR "20120260086" OR "20120260090" OR "20120260095" OR "20120263298" OR "20120278490" OR "20120300932" OR "20120331292" OR "20120331298" OR "20130007442" OR "20130012168" OR "20130028184" OR "20130091556" OR "20130114810" OR "20130117824" OR "20130122864" OR "20130149996" OR "20130157673" OR "20130165073" OR "20130165075" OR "20130166915" OR "20130173747" OR "20130173926" OR "20130179962" OR "20130182586" OR "20130183932" OR "20130212637" OR "20130227646" OR "20130231087" OR "20130283047" OR "20130294602" OR "20130305345" OR "20130322621" OR "20130331063" OR "20130340040" OR "20130344864" OR "20140003604" OR "20140040628" OR "20140049653" OR					

Petitioner Samsung Ex-1004, 0086

		"20140053241" OR "20140073375" OR "20140082358" OR "20140082359" OR "20140082538" OR "20140082539" OR "20140087790" OR "20140101444" OR "20140108801" OR "20140115335" OR "20140120874" OR "20140122878" OR "20140140507" OR "20140140509" OR "20140143534" OR "20140143826" OR "20140161113" OR "20140165155" OR "20140192976" OR "20140219447" OR "20140219448" OR "20140235210" OR "20140237101" OR "20140244994" OR "20140273913" OR "20140281483" OR "20140287725" OR "20140308991" OR "20140329502" OR "20140337937" OR "20140351403" OR "20140357229" OR "20150012743" OR "20150017910" OR "20150071139" OR "20150089214" OR "20150092590" OR "20150095514" OR "20150095648" OR "20150106616" OR "20150113275" OR "20150121066" OR "20150121495" OR "20150143125" OR "20150163056" OR "20150215126" OR "20150222604" OR "20150222619" OR "20150281964" OR "20150350881" OR "20160014112" OR "20160057725" OR "20160088096" OR "20160127132" OR "20160149903" OR "20160294829" OR "20170206532" OR "20190313246" OR				

Petitioner Samsung Ex-1004, 0087

		"20190332774" OR "20190356482" OR "20200162247" OR "20200162269" OR "20200226258" OR "20200280436" OR "20210126801" OR "20210184842" OR "20210194681" OR "20210211279" OR "20210218560" OR "5216715" OR "5642420" OR "5664017" OR "5852665" OR "5995625" OR "6038322" OR "6256733" OR "6721886" OR "6804357" OR "6842628" OR "7921292" OR "7957532" OR "8127142" OR "8352739" OR "8434139" OR "8452017" OR "8522013" OR "8526606" OR "8555067" OR "8577337" OR "8590028" OR "8782774" OR "8843179" OR "8924715" OR "8948386" OR "8965366" OR "9002018" OR "9020479" OR "9253643" OR "9270653" OR "9332129" OR "9408012" OR "9572016" OR "9596078" OR "9628981" OR "9674690" OR "9698981" OR "9794775" OR "9800993" OR "9807605" OR "9923724").pn.					
L14	5	11 AND 13	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 10:12 AM
L15	128	((elliptic NEAR curve) WITH (diffie NEAR hellman) WITH derive	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:51 AM

Petitioner Samsung Ex-1004, 0088

		WITH key)					
L16	13	13 AND 15	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:52 AM
L17	19	11 AND 15	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:52 AM
L18	3813	((elliptic NEAR curve) WITH (diffie NEAR hellman) WITH key)	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:52 AM
L19	27	11 AND 18	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:53 AM
L20	366	(authenticat$4 WITH network$2 WITH plaintext$2)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:32 PM
L21	19	11 AND 20	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:32 PM
L22	19	21 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:32 PM
L23	248	18 AND (mobile WITH (sim eUICC))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:34 PM
L24	100	23 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:34 PM
L25	9	13 AND 23	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:34 PM
L26	42	((UICC near3 profile) WITH subscriber)	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2023/10/12 02:31 PM
L27	21	26 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 02:31 PM
L30	12	26 AND (decrypt$4 WITH key)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 02:32 PM
L31	7	30 AND (profile WITH key WITH ident$6)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 03:04 PM
L32	1600	(decrypt$4 WITH profile WITH key)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 03:48 PM
L33	51	(decrypt$4 WITH (first near2 (part$2 portion)) WITH profile WITH key)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 03:48 PM
L34	21	33 AND (mobile WITH (sim eUICC))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 03:49 PM
L35	1	13 AND 34	(US-PGPUB; USPAT;	OR	ON	ON	2023/10/12

Petitioner Samsung Ex-1004, 0089

			USOCR; EPO; JPO; DERWENT)				05:14 PM
L36	240	("10169587" OR "10621352" OR "20010029581" OR "20020018569" OR "20030003895" OR "20030211842" OR "20040162472" OR "20040179684" OR "20040221163" OR "20050008159" OR "20050021875" OR "20050050323" OR "20050058294" OR "20050120202" OR "20050138353" OR "20050193199" OR "20050246282" OR "20050278787" OR "20060021063" OR "20060056355" OR "20060059344" OR "20060095771" OR "20060129848" OR "20060206710" OR "20060281442" OR "20070101400" OR "20070158439" OR "20070206799" OR "20080016230" OR "20080022089" OR "20080031204" OR "20080044032" OR "20080107083" OR "20080114978" OR "20080130879" OR "20080165698" OR "20080307218" OR "20090028341" OR "20090041110" OR "20090060197" OR "20090077643" OR "20090113203" OR "20090116642" OR "20090125996" OR "20090132806" OR "20090183541" OR "20090191857" OR "20090209232" OR "20090217348" OR "20090268909" OR "20090274306" OR "20090282246" OR "20090313472" OR "20100031042" OR "20100062808" OR	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:24 PM

Petitioner Samsung Ex-1004, 0090

		"20100093347" OR "20100098253" OR "20100166167" OR "20100195833" OR "20100199334" OR "20100223461" OR "20100275028" OR "20110016321" OR "20110035584" OR "20110035604" OR "20110055553" OR "20110158411" OR "20110167272" OR "20110213959" OR "20110237281" OR "20110268022" OR "20110269422" OR "20110269461" OR "20110269472" OR "20110270747" OR "20110291803" OR "20110314287" OR "20120011360" OR "20120011362" OR "20120023336" OR "20120030461" OR "20120033613" OR "20120072732" OR "20120084568" OR "20120087493" OR "20120089568" OR "20120108205" OR "20120117635" OR "20120159153" OR "20120170451" OR "20120190354" OR "20120214444" OR "20120260086" OR "20120260090" OR "20120260095" OR "20120263298" OR "20120278490" OR "20120300932" OR "20120331292" OR "20120331298" OR "20130007442" OR "20130012168" OR "20130028184" OR "20130091556" OR "20130114810" OR "20130117824" OR "20130122864" OR "20130149996" OR "20130157673" OR "20130165073" OR "20130165075" OR "20130166915" OR "20130173747" OR				

Petitioner Samsung Ex-1004, 0091

		"20130173926" OR "20130179962" OR "20130182586" OR "20130183932" OR "20130212637" OR "20130227646" OR "20130231087" OR "20130283047" OR "20130294602" OR "20130305345" OR "20130322621" OR "20130331063" OR "20130340040" OR "20130344864" OR "20140003604" OR "20140040628" OR "20140049653" OR "20140053241" OR "20140073375" OR "20140082358" OR "20140082359" OR "20140082538" OR "20140082539" OR "20140087790" OR "20140101444" OR "20140108801" OR "20140115335" OR "20140120874" OR "20140122878" OR "20140140507" OR "20140140509" OR "20140143534" OR "20140143826" OR "20140161113" OR "20140165155" OR "20140192976" OR "20140219447" OR "20140219448" OR "20140235210" OR "20140237101" OR "20140244994" OR "20140273913" OR "20140281483" OR "20140287725" OR "20140308991" OR "20140329502" OR "20140337937" OR "20140351403" OR "20140357229" OR "20150012743" OR "20150017910" OR "20150071139" OR "20150089214" OR "20150092590" OR "20150095514" OR "20150095648" OR "20150106616" OR "20150113275" OR					

Petitioner Samsung Ex-1004, 0092

		"20150121066" OR "20150121495" OR "20150143125" OR "20150163056" OR "20150215126" OR "20150222604" OR "20150222619" OR "20150281964" OR "20150350881" OR "20160014112" OR "20160057725" OR "20160088096" OR "20160127132" OR "20160149903" OR "20160294829" OR "20170206532" OR "20190313246" OR "20190332774" OR "20190356482" OR "20200162247" OR "20200162269" OR "20200226258" OR "20200280436" OR "20210126801" OR "20210184842" OR "20210194681" OR "20210211279" OR "20210218560" OR "5216715" OR "5642420" OR "5664017" OR "5852665" OR "5995625" OR "6038322" OR "6256733" OR "6721886" OR "6804357" OR "6842628" OR "7921292" OR "7957532" OR "8127142" OR "8352739" OR "8434139" OR "8452017" OR "8522013" OR "8526606" OR "8555067" OR "8577337" OR "8590028" OR "8782774" OR "8843179" OR "8924715" OR "8948386" OR "8965366" OR "9002018" OR "9020479" OR "9253643" OR "9270653" OR					

Petitioner Samsung Ex-1004, 0093

		"9332129" OR "9408012" OR "9572016" OR "9596078" OR "9628981" OR "9674690" OR "9698981" OR "9794775" OR "9800993" OR "9807605" OR "9923724").pn.					
L38	2	((eUICC near3 key) WITH subscrib$4 WITH (diffie near2 hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:26 PM
L39	29	32 AND 36	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:26 PM
L40	0	(((universal NEAR integrat$4 NEAR circuit NEAR card) near3 key) WITH subscrib$4 WITH (diffie near2 hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:27 PM
L41	0	(((univer$6 near2 integrat$4 near2 circuit$2 NEAR card) near3 key) WITH subscrib$4 WITH (diffie near2 hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:28 PM
L42	3	((UICC near3 key) WITH subscrib$4 WITH (diffie near2 hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:28 PM
L43	3	"20180084415"	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:29 PM
L44	0	((eUICC near3 key) WITH subscrib$4 WITH decrypt$4 WITH ciphertext$2)	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/25 11:22 PM
L45	24	((eUICC near3 key) WITH decrypt$4 WITH ciphertext$2)	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/25 11:23 PM
L46	220	36 AND ((H04W12/30 OR H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/11/25 11:39 PM
L47	2	36 AND (eUICC WITH (key$2 NEAR exchang$4))	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/25 11:39 PM
L48	42	18 AND (eUICC WITH (key$2 NEAR exchang$4))	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/25 11:40 PM
L49	43	48 AND ((H04W12/30 OR H04W12/35 OR H04W12/06 OR H04L63/0853 OR	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/11/25 11:40 PM

Petitioner Samsung Ex-1004, 0094

		H04L63/08).cpc.)					
L50	36	(eUICC WITH (key$2 NEAR exchang$4) WITH (privat$4 public))	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/25 11:41 PM
L51	31	(((univer$6 near2 integrat$4 near2 circuit$2 NEAR card) near3 key) WITH subscrib$4)	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/25 11:43 PM
L52	27	51 AND ((H04W12/30 OR H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/11/25 11:44 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	19	((authenticat$4 validat$6) WITH mobile WITH eUICC WITH profile).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 10:04 AM
N2	38	((elliptic NEAR curve) WITH (diffie NEAR hellman) WITH derive WITH key).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:52 AM
N3	0	N1 AND N2	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 01:33 PM
N4	3	((UICC near3 key) WITH subscrib$4 WITH (diffie near2 hellman)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:45 PM
N5	21	(eUICC WITH (key$2 NEAR exchang$4) WITH (privat$4 public)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/25 11:41 PM
N6	9	(((univer$6 near2 integrat$4 near2 circuit$2 NEAR card) near3 key) WITH subscrib$4).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/25 11:44 PM
N7	0	N5 AND N6	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/25 11:44 PM

Bibliographic Data

Application No: 18/416,534

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☐ No ☐ Met After Allowance

Verified and Acknowledged: /DAO Q HO/ (Examiner's Signature) (Initials)

Title: Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
01/18/2024	713	2432	63121/0226
RULE			

APPLICANTS

Network-1 Technologies, Inc., New York, NY, UNITED STATES

INVENTORS

John A. Nix, Evanston, IL, UNITED STATES

CONTINUING DATA

This application is a CON of 17547990 12/10/2021 PAT 11916893

17547990 is a CON of 16453682 06/26/2019 PAT 11233780

16453682 is a CIP of 16110804 08/23/2018 PAT 10382422

16110804 is a CON of 15928848 03/22/2018 PAT 10084768

15928848 is a CON of 14751119 06/25/2015 PAT 9961060

14751119 is a CON of 14099329 12/06/2013 PAT 9100175

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

02/01/2024

** **SMALL ENTITY** **

STATE OR COUNTRY

UNITED STATES

ADDRESS

AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174
UNITED STATES

FILING FEE RECEIVED

$912

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Network-1 Technologies, Inc.	Confirmation No.: 7559
Title:	EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION	
Appl. No.:	18/416,534	
Filing Date:	January 18, 2024	
Examiner:	HO, Dao Q.	
Art Unit:	2432	
Docket No.:	63121/0226	
Customer No.:	01912	

RESPONSE TO NON-FINAL OFFICE ACTION DATED SEPTEMBER 18, 2024

VIA Patent Center

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a response to the Non-Final Office Action dated September 18, 2024. A response to the Office Action is due on December 18, 2024 such that the present Response is being timely filed. Applicant respectfully requests reconsideration of the outstanding claim rejections in view of the remarks set forth herein, where:

Amendments to the Claims begin on page **2** of this paper.

Remarks begin on page **6** of this paper.

Petitioner Samsung Ex-1004, 0098

IN THE CLAIMS

What is claimed is:

1. (Currently Amended) A method comprising:

(a) generating a first message comprising:

(1) an identity of an embedded universal integrated circuit card (eUICC);

(2) a nonce; and

(3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;

(b) sending the first message via a network application to a subscription manager system;

(c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;

(d) storing a subscription manager public key which corresponds to a subscription manager private key;

(e) deriving a profile key using a key exchange algorithm based on at least:

(i) the second eUICC private key, and

(ii) the stored subscription manager public key, wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key;

(f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;

(g) receiving the symmetric key;

(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;

(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and

(j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.

2. (Original) The method of claim 1, wherein the subscription manager public key is downloaded via the network application.

Petitioner Samsung Ex-1004, 0099

3. (Original) The method of claim 1, wherein the step of storing the subscription manager public key occurs at the time of manufacture of the embedded universal integrated circuit card.

4. (Original) The method of claim 1, wherein the key exchange algorithm is a Diffie-Hellman key exchange.

5. (Original) The method of claim 1, wherein the key exchange algorithm is an Elliptic Curve Diffie-Hellman key exchange.

6. (Original) The method of claim 1, wherein the encrypted profile is encrypted in a manner so that intermediate nodes on an IP network would not be able to read data within the profile in an unencrypted form.

7. (Original) The method of claim 1, wherein subscription manager system stores the ciphertext and the symmetric key before step (a).

8. (Original) The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the identity of the embedded universal integrated circuit card included in the first message.

9. (Original) The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the digital signature included in the first message.

10. (Original) The method of claim 1, wherein the decrypted ciphertext is stored in nonvolatile memory of the embedded universal integrated circuit card.

11. (Original) The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a machine-to-machine module.

Petitioner Samsung Ex-1004, 0100

12. (Original) The method of claim 11, wherein the module comprises a module of a type selected from the group consisting of: vending machine, automobile, alarm system, tracking device, monitoring device, security system and remote control device.

13. (Original) The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a wireless module.

14. (Original) The method of claim 13, wherein the module is configured to communicate using one or more wireless technologies of types selected from the group consisting of: WiFi, WiMax, General Packet Radio Services, Enhanced Data rates for GSM Evolution and 3rd Generation Partnership Project technology.

15. (Original) The method of claim 13, wherein the module comprises a module of a type selected from the group consisting of the following: wireless handset, cellular phone, smartphone, laptop computer, tracking device, computer with a radio, circuit board with a radio, hand-held device, netbook, portable computer, multiprocessor system, microprocessor based consumer electronic, programmable consumer electronic, network personal computer, minicomputer, mainframe computer and smartcard.

16. (Original) The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module, wherein the module is a wired module.

17. (Original) The method of claim 16, wherein the module is configured to communicate using one or more wired connections of types selected from the group consisting of: Ethernet, fiber optic connection and Universal Serial Bus connection.

18. (Original) The method of claim 16, wherein the module comprises a module of a type selected from the group consisting of: computer, security camera, security monitoring device and networked controller.

Petitioner Samsung Ex-1004, 0101

19. (Original) The method of claim 1, wherein the deriving step (c) is performed prior to the generating step (a).

20. (Original) The method of claim 1, wherein the generating step (a) is performed before the deriving step (c).

21. (Original) The method of claim 1, wherein the embedded integrated circuit card is operably connected to a module and a user accesses a user interface of the module to enter authentication information before the module receives the symmetric key.

22. (Original) The method of claim 1, wherein the subscription manager receives the ciphertext from a mobile network operator before the network application sends the first message.

Petitioner Samsung Ex-1004, 0102

REMARKS

This responds to the Office Action dated September 18, 2024. Claims 1-22 are pending with claim 1 being in independent form. Claim 1 has been amended to address minor informalities. Applicant submits that no new matter is added by this amendment. In view of the below remarks, Applicant respectfully asserts that claims 1-22 are in condition for allowance.

In the event that the Examiner disagrees, Applicant respectfully requests that the Examiner contact Applicant's undersigned attorney by telephone prior to issuing another Office Action.

I. Claim rejections under 35 U.S.C. 112(b)

Claim 1 is rejected under 35 U.S.C. 112(b) because the term "an eUICC" is allegedly not properly defined. Office Action, pg. 3. This rejection is respectfully traversed.

Applicant notes that the term "an eUICC" is not used in claim 1. Claim 1 does, however recite "an embedded universal integrated circuit card" which is believed to be self-explanatory. That said, Applicant has amended claim 1 to note that "eUICC" refers to an embedded universal integrated circuit card.

Applicant respectfully requests reconsideration and withdrawal of the rejection of the claims under Section 112.

II. Double Patenting

Claims 1-22 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as allegedly being unpatentable over the claims of U.S. Patent No. 10,084,768, U.S. Patent No. 10,382,422 and U.S. Patent No. 11,233,780. Office Action, pgs. 4.

While Applicant does not necessarily agree with the Examiner's double patenting rejection, in an effort to advance prosecution of the present application, Applicant submits herewith a terminal disclaimer with respect to U.S. Patent No. 10,084,768, U.S. Patent No. 10,382,422 and U.S. Patent No. 11,233,780 to overcome this rejection.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the non-statutory double patenting rejection of claims 1-22.

Petitioner Samsung Ex-1004, 0103

Since there are no other rejections in the Office Action, Applicant respectfully submits that claims 1-22 are allowable over the cited art and are in condition for allowance.

Applicant respectfully submits that the foregoing constitutes a bona fide response to all issues raised in the Office Action and requests that the application be prepared for issuance in due course. Should any questions arise in connection with this response, the Office is invited to contact the undersigned at the number provided below.

III. Reference to Related Patents and Co-Pending Applications

The below chart provides information regarding related issued patents and co-pending applications filed by the present Applicant:

Petitioner Samsung Ex-1004, 0104

Serial No.	Attorney Docket No.	Filing Date	Status
18/435,042	63121/0230	2024-02-07	Pending – Ready for Examination
18/587,462	63121/0229	2024-02-26	Pending – Ready for Examination
18/433,683	63121/0228	2024-02-06	Pending – Ready for Examination
18/438,147	63121/0227	2024-02-09	Pending – Undergoing Preexam Processing
18/416,534	**63121/0226**	**204-01-18**	**Present Application**
18/433,664	63121/0225	2024-02-06	Pending – Ready for Examination
18/229,907	63121/0224	2023-08-03	Pending – Response to Final OA Filed 2024-03-28
18/111,669	63121/0222	2023-02-20	Non-Final OA mailed 2023-10-02
17/647,812	63121/0213	2022-01-13	USP 11,606,204
17/547,990	63121/0212	2021-12-10	USP 11,736,283
17/304,922	63121/0209	2021-06-28	USP 11,736,283
17/249,242	63121/0202	2021-02-24	Response to Non-Final OA filed 2023-11-13
16/879,325	63121/0198	2020-05-20	USP 11,082,218
16/843,107	63121/0197	2020-04-08	USP 11,283,603
16/721,153	63121/0195	2019-12-19	USP 11,539,681
16/593,561	63121/0190	2019-10-04	USP 11,258,595
16/453,682	63121/0184	2019-06-26	USP 11,233,780
16/271,455	63121/0181	2019-02-08	USP 10,594,679
16/271,428	63121/0180	2019-02-08	USP 10,523,432
16/201,401	63121/0179	2018-11-27	USP 10,700,856
16/200,118	63121/0178	2018-11-26	USP 10,498,530
16/110,804	63121/0168	2018-08-23	USP 10,382,422
16/036,506	63121/0167	2018-07-16	USP 10,530,575
15/983,957	63121/0163	2018-05-18	USP 10,177,911
15/973,012	63121/0162	2018-05-07	USP 10,250,386
15/972,914	63121/0161	2018-05-07	USP 10,652,017
15/928,848	63121/0160	2018-03-22	USP 10,084,768
15/010,905	63121/0157	2016-01-29	USP 9,641,327
15/680,758	63121/0147	2017-08-18	USP 10,187,206
15/162,292	63121/0146	2016-05-23	USP 10,362,012
14/751,119	63121/0145	2015-06-25	USP 9,961,060
15/457,700	63121/0144	2017-03-13	USP 9,998,281
15/583,968	63121/0143	2017-05-01	USP 10,057,059
15/043,293	63121/0142	2016-02-12	USP 9,998,280
15/642,088	63121/0141	2017-07-05	USP 10,003,461

Petitioner Samsung Ex-1004, 0105

15/130,146	63121/0140	2016-04-15	USP 9,742,562
15/162,302	63121/0139	2016-05-23	USP 9,698,981
14/789,255	63121/0138	2015-07-01	USP 9,596,078
14/139,419	63121/0137	2013-12-23	USP 9,351,162
14/136,711	63121/0136	2013-12-20	USP 9,300,473
14/099,329	63121/0135	2013-12-06	USP 9,100,175
14/084,141	63121/0134	2013-11-19	USP 9,319,223
14/064,618	63121/0133	2013-10-28	USP 9,118,464
14/055,606	63121/0132	2013-10-16	USP 9,276,740
14/039,401	63121/0131	2013-09-27	USP 9,288,059
14/023,181	63121/0130	2013-09-10	USP 9,350,550
AU 2019246774	63121-0199	2019-10-08	AU2019246774A1 Issued 2021-09-23
GB 1608573	63121-0151	2014-10-27	Published on 2016-08-03
GB 2100530	63121-0201	2014-10-27	Published on 2021-05-12
CA 2,965,119	63121-0152	2014-10-27	Published on 2015-05-07
HK 17101082.8	63121-0153	2014-10-27	Published on 2017-10-20
EU 14868381.6	63121-0154	2014-12-04	Published on 2017-01-04
CA 2,969,829	63121-0155	2014-12-04	Published on 2015-06-11
HK 17106540.3	63121-0156	2014-12-04	Published on 2018-01-19

The Examiner is invited to review the prosecution history of each of these applications, including the cited references of record and related office actions, as the Examiner deems appropriate.

* * * * *

Petitioner Samsung Ex-1004, 0106

No fee is believed to be necessary in conjunction with the filing of the present response, however, if any additional fee is required, including any fee to preserve the pendency of the subject application, authorization is hereby given to charge the amount of any such fee to Deposit Account No. 01-1785. Overpayments may also be credited to Deposit Account No. 01-1785.

Respectfully submitted,

AMSTER, ROTHSTEIN & EBENSTEIN LLP
Attorneys for Applicant
405 Lexington Avenue
New York, NY 10174
(212) 336-8000

Dated: November 4, 2024

By: /Keith J. Barkaus/
Keith J. Barkaus
Reg. No. 51,431

4895-4071-0632v.1

Petitioner Samsung Ex-1004, 0107

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	**11/04/2024 08:15:51 PM Z ET**	**63121/0226**

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	67836797	FILING DATE	01/18/2024
CUSTOMER #	1912	FIRST NAMED INVENTOR	John A. Nix
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Keith Barkaus

Documents

TOTAL DOCUMENTS: 3

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
1-ResponsetoNFOA.pdf		10	-	161 KB
1-ResponsetoNFOA-A....pdf	(1-1)	1	Amendment/Request for Reconsideration-After Non-Final Rejection	123 KB
1-ResponsetoNFOA-CLM.pdf	(2-6)	5	Claims	146 KB
1-ResponsetoNFOA-REM.pdf	(7-10)	4	Applicant Arguments/Remarks Made in an Amendment	146 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

1-ResponsetoNFOA.pdf	8E77D01497F42A807E904184835E0E8C3934423F149258C234E36B63E2FBE2F50D6FD4BA00E399B8739663ECE8666AD7F946B98A683E8A8C251AA2C0AC60D7A3
1-ResponsetoNFOA-A....pdf	7652A500B9E070A5A842AABDFA66F5A449104A08160033D8405621DA75E275158F6D014F00604FDD1804E50B151847875BD39DFD961FE77B3DD8019CC8A16649
1-ResponsetoNFOA-CLM.pdf	F2D06046135AB7D3D5961C96BE6C1CB5773236F2EB02340FA42AA9359B498F6F24543AB5F88513F1E240EAE15B389C1C8559FC4E9861EE4D0DE2F74BCBE29812
1-ResponsetoNFOA-REM.pdf	F5AE0083568C3500F70F22802D5EDE0AF93390CAC394EE8259559EF1B1F05A6968D14BBB32FBF2D58B40BA51C00FC2F27AB639127DD27DF4AEA820E7B5F39BDF

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Network-1 Technologies, Inc.	Confirmation No.: 7559
Title:	EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION	
Appl. No.:	18/416,534	
Filing Date:	January 18, 2024	
Examiner:	HO, Dao Q.	
Art Unit:	2432	
Docket No.:	63121/0226	
Customer No.:	01912	

RESPONSE TO NON-FINAL OFFICE ACTION DATED SEPTEMBER 18, 2024

VIA Patent Center

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a response to the Non-Final Office Action dated September 18, 2024. A response to the Office Action is due on December 18, 2024 such that the present Response is being timely filed. Applicant respectfully requests reconsideration of the outstanding claim rejections in view of the remarks set forth herein, where:

Amendments to the Claims begin on page **2** of this paper.

Remarks begin on page **6** of this paper.

Petitioner Samsung Ex-1004, 0110

IN THE CLAIMS

What is claimed is:

1. (Currently Amended) A method comprising:

(a) generating a first message comprising:

(1) an identity of an embedded universal integrated circuit card (eUICC);

(2) a nonce; and

(3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;

(b) sending the first message via a network application to a subscription manager system;

(c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;

(d) storing a subscription manager public key which corresponds to a subscription manager private key;

(e) deriving a profile key using a key exchange algorithm based on at least:

(i) the second eUICC private key, and

(ii) the stored subscription manager public key, wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key;

(f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;

(g) receiving the symmetric key;

(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;

(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and

(j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.

2. (Original) The method of claim 1, wherein the subscription manager public key is downloaded via the network application.

Petitioner Samsung Ex-1004, 0111

3. (Original) The method of claim 1, wherein the step of storing the subscription manager public key occurs at the time of manufacture of the embedded universal integrated circuit card.

4. (Original) The method of claim 1, wherein the key exchange algorithm is a Diffie-Hellman key exchange.

5. (Original) The method of claim 1, wherein the key exchange algorithm is an Elliptic Curve Diffie-Hellman key exchange.

6. (Original) The method of claim 1, wherein the encrypted profile is encrypted in a manner so that intermediate nodes on an IP network would not be able to read data within the profile in an unencrypted form.

7. (Original) The method of claim 1, wherein subscription manager system stores the ciphertext and the symmetric key before step (a).

8. (Original) The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the identity of the embedded universal integrated circuit card included in the first message.

9. (Original) The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the digital signature included in the first message.

10. (Original) The method of claim 1, wherein the decrypted ciphertext is stored in nonvolatile memory of the embedded universal integrated circuit card.

11. (Original) The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a machine-to-machine module.

Petitioner Samsung Ex-1004, 0112

12. (Original) The method of claim 11, wherein the module comprises a module of a type selected from the group consisting of: vending machine, automobile, alarm system, tracking device, monitoring device, security system and remote control device.

13. (Original) The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a wireless module.

14. (Original) The method of claim 13, wherein the module is configured to communicate using one or more wireless technologies of types selected from the group consisting of: WiFi, WiMax, General Packet Radio Services, Enhanced Data rates for GSM Evolution and 3rd Generation Partnership Project technology.

15. (Original) The method of claim 13, wherein the module comprises a module of a type selected from the group consisting of the following: wireless handset, cellular phone, smartphone, laptop computer, tracking device, computer with a radio, circuit board with a radio, hand-held device, netbook, portable computer, multiprocessor system, microprocessor based consumer electronic, programmable consumer electronic, network personal computer, minicomputer, mainframe computer and smartcard.

16. (Original) The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module, wherein the module is a wired module.

17. (Original) The method of claim 16, wherein the module is configured to communicate using one or more wired connections of types selected from the group consisting of: Ethernet, fiber optic connection and Universal Serial Bus connection.

18. (Original) The method of claim 16, wherein the module comprises a module of a type selected from the group consisting of: computer, security camera, security monitoring device and networked controller.

Petitioner Samsung Ex-1004, 0113

19. (Original) The method of claim 1, wherein the deriving step (c) is performed prior to the generating step (a).

20. (Original) The method of claim 1, wherein the generating step (a) is performed before the deriving step (c).

21. (Original) The method of claim 1, wherein the embedded integrated circuit card is operably connected to a module and a user accesses a user interface of the module to enter authentication information before the module receives the symmetric key.

22. (Original) The method of claim 1, wherein the subscription manager receives the ciphertext from a mobile network operator before the network application sends the first message.

Petitioner Samsung Ex-1004, 0114

REMARKS

This responds to the Office Action dated September 18, 2024. Claims 1-22 are pending with claim 1 being in independent form. Claim 1 has been amended to address minor informalities. Applicant submits that no new matter is added by this amendment. In view of the below remarks, Applicant respectfully asserts that claims 1-22 are in condition for allowance.

In the event that the Examiner disagrees, Applicant respectfully requests that the Examiner contact Applicant's undersigned attorney by telephone prior to issuing another Office Action.

I. Claim rejections under 35 U.S.C. 112(b)

Claim 1 is rejected under 35 U.S.C. 112(b) because the term "an eUICC" is allegedly not properly defined. Office Action, pg. 3. This rejection is respectfully traversed.

Applicant notes that the term "an eUICC" is not used in claim 1. Claim 1 does, however recite "an embedded universal integrated circuit card" which is believed to be self-explanatory. That said, Applicant has amended claim 1 to note that "eUICC" refers to an embedded universal integrated circuit card.

Applicant respectfully requests reconsideration and withdrawal of the rejection of the claims under Section 112.

II. Double Patenting

Claims 1-22 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as allegedly being unpatentable over the claims of U.S. Patent No. 10,084,768, U.S. Patent No. 10,382,422 and U.S. Patent No. 11,233,780. Office Action, pgs. 4.

While Applicant does not necessarily agree with the Examiner's double patenting rejection, in an effort to advance prosecution of the present application, Applicant submits herewith a terminal disclaimer with respect to U.S. Patent No. 10,084,768, U.S. Patent No. 10,382,422 and U.S. Patent No. 11,233,780 to overcome this rejection.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the non-statutory double patenting rejection of claims 1-22.

Petitioner Samsung Ex-1004, 0115

REMARKS

This responds to the Office Action dated September 18, 2024. Claims 1-22 are pending with claim 1 being in independent form. Claim 1 has been amended to address minor informalities. Applicant submits that no new matter is added by this amendment. In view of the below remarks, Applicant respectfully asserts that claims 1-22 are in condition for allowance.

In the event that the Examiner disagrees, Applicant respectfully requests that the Examiner contact Applicant's undersigned attorney by telephone prior to issuing another Office Action.

I. Claim rejections under 35 U.S.C. 112(b)

Claim 1 is rejected under 35 U.S.C. 112(b) because the term "an eUICC" is allegedly not properly defined. Office Action, pg. 3. This rejection is respectfully traversed.

Applicant notes that the term "an eUICC" is not used in claim 1. Claim 1 does, however recite "an embedded universal integrated circuit card" which is believed to be self-explanatory. That said, Applicant has amended claim 1 to note that "eUICC" refers to an embedded universal integrated circuit card.

Applicant respectfully requests reconsideration and withdrawal of the rejection of the claims under Section 112.

II. Double Patenting

Claims 1-22 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as allegedly being unpatentable over the claims of U.S. Patent No. 10,084,768, U.S. Patent No. 10,382,422 and U.S. Patent No. 11,233,780. Office Action, pgs. 4.

While Applicant does not necessarily agree with the Examiner's double patenting rejection, in an effort to advance prosecution of the present application, Applicant submits herewith a terminal disclaimer with respect to U.S. Patent No. 10,084,768, U.S. Patent No. 10,382,422 and U.S. Patent No. 11,233,780 to overcome this rejection.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the non-statutory double patenting rejection of claims 1-22.

Petitioner Samsung Ex-1004, 0116

Since there are no other rejections in the Office Action, Applicant respectfully submits that claims 1-22 are allowable over the cited art and are in condition for allowance.

Applicant respectfully submits that the foregoing constitutes a bona fide response to all issues raised in the Office Action and requests that the application be prepared for issuance in due course. Should any questions arise in connection with this response, the Office is invited to contact the undersigned at the number provided below.

III. Reference to Related Patents and Co-Pending Applications

The below chart provides information regarding related issued patents and co-pending applications filed by the present Applicant:

Petitioner Samsung Ex-1004, 0117

Serial No.	Attorney Docket No.	Filing Date	Status
18/435,042	63121/0230	2024-02-07	Pending – Ready for Examination
18/587,462	63121/0229	2024-02-26	Pending – Ready for Examination
18/433,683	63121/0228	2024-02-06	Pending – Ready for Examination
18/438,147	63121/0227	2024-02-09	Pending – Undergoing Preexam Processing
18/416,534	**63121/0226**	**204-01-18**	**Present Application**
18/433,664	63121/0225	2024-02-06	Pending – Ready for Examination
18/229,907	63121/0224	2023-08-03	Pending – Response to Final OA Filed 2024-03-28
18/111,669	63121/0222	2023-02-20	Non-Final OA mailed 2023-10-02
17/647,812	63121/0213	2022-01-13	USP 11,606,204
17/547,990	63121/0212	2021-12-10	USP 11,736,283
17/304,922	63121/0209	2021-06-28	USP 11,736,283
17/249,242	63121/0202	2021-02-24	Response to Non-Final OA filed 2023-11-13
16/879,325	63121/0198	2020-05-20	USP 11,082,218
16/843,107	63121/0197	2020-04-08	USP 11,283,603
16/721,153	63121/0195	2019-12-19	USP 11,539,681
16/593,561	63121/0190	2019-10-04	USP 11,258,595
16/453,682	63121/0184	2019-06-26	USP 11,233,780
16/271,455	63121/0181	2019-02-08	USP 10,594,679
16/271,428	63121/0180	2019-02-08	USP 10,523,432
16/201,401	63121/0179	2018-11-27	USP 10,700,856
16/200,118	63121/0178	2018-11-26	USP 10,498,530
16/110,804	63121/0168	2018-08-23	USP 10,382,422
16/036,506	63121/0167	2018-07-16	USP 10,530,575
15/983,957	63121/0163	2018-05-18	USP 10,177,911
15/973,012	63121/0162	2018-05-07	USP 10,250,386
15/972,914	63121/0161	2018-05-07	USP 10,652,017
15/928,848	63121/0160	2018-03-22	USP 10,084,768
15/010,905	63121/0157	2016-01-29	USP 9,641,327
15/680,758	63121/0147	2017-08-18	USP 10,187,206
15/162,292	63121/0146	2016-05-23	USP 10,362,012
14/751,119	63121/0145	2015-06-25	USP 9,961,060
15/457,700	63121/0144	2017-03-13	USP 9,998,281
15/583,968	63121/0143	2017-05-01	USP 10,057,059
15/043,293	63121/0142	2016-02-12	USP 9,998,280
15/642,088	63121/0141	2017-07-05	USP 10,003,461

Petitioner Samsung Ex-1004, 0118

15/130,146	63121/0140	2016-04-15	USP 9,742,562
15/162,302	63121/0139	2016-05-23	USP 9,698,981
14/789,255	63121/0138	2015-07-01	USP 9,596,078
14/139,419	63121/0137	2013-12-23	USP 9,351,162
14/136,711	63121/0136	2013-12-20	USP 9,300,473
14/099,329	63121/0135	2013-12-06	USP 9,100,175
14/084,141	63121/0134	2013-11-19	USP 9,319,223
14/064,618	63121/0133	2013-10-28	USP 9,118,464
14/055,606	63121/0132	2013-10-16	USP 9,276,740
14/039,401	63121/0131	2013-09-27	USP 9,288,059
14/023,181	63121/0130	2013-09-10	USP 9,350,550
AU 2019246774	63121-0199	2019-10-08	AU2019246774A1 Issued 2021-09-23
GB 1608573	63121-0151	2014-10-27	Published on 2016-08-03
GB 2100530	63121-0201	2014-10-27	Published on 2021-05-12
CA 2,965,119	63121-0152	2014-10-27	Published on 2015-05-07
HK 17101082.8	63121-0153	2014-10-27	Published on 2017-10-20
EU 14868381.6	63121-0154	2014-12-04	Published on 2017-01-04
CA 2,969,829	63121-0155	2014-12-04	Published on 2015-06-11
HK 17106540.3	63121-0156	2014-12-04	Published on 2018-01-19

The Examiner is invited to review the prosecution history of each of these applications, including the cited references of record and related office actions, as the Examiner deems appropriate.

* * * * *

Petitioner Samsung Ex-1004, 0119

No fee is believed to be necessary in conjunction with the filing of the present response, however, if any additional fee is required, including any fee to preserve the pendency of the subject application, authorization is hereby given to charge the amount of any such fee to Deposit Account No. 01-1785. Overpayments may also be credited to Deposit Account No. 01-1785.

Respectfully submitted,

AMSTER, ROTHSTEIN & EBENSTEIN LLP
Attorneys for Applicant
405 Lexington Avenue
New York, NY 10174
(212) 336-8000

Dated: November 4, 2024

By: /Keith J. Barkaus/
Keith J. Barkaus
Reg. No. 51,431

Petitioner Samsung Ex-1004, 0120

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	**11/04/2024 06:27:21 PM Z ET**	**63121/0226**

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	67828722	AUTHORIZED BY	Keith Barkaus
CUSTOMER #	1912	FILING DATE	01/18/2024
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	John A. Nix

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1077	**E2024A4I29569912**	**Keith Barkaus**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2814	STATUTORY DISCLAIMER, INCLUDING TERMINAL DISCLAIMER	170.00	1	170.00
			TOTAL AMOUNT:	**$170.00**

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C.

371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

APPROVAL LETTER

APPLICATION #	FILING DATE	APPLICANT/PATENT UNDER REEXAMINATION
18/416,534	01/18/2024	John Nix

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Electronic terminal disclaimer filed on 11/04/2024

☑ Approved

This patent is subject to a Terminal Disclaimer

Approved / Disapproved by: Electronic Terminal Disclaimer automatically approved

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	**11/04/2024 06:27:21 PM Z ET**	**63121/0226**

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	67828722	FILING DATE	01/18/2024
CUSTOMER #	1912	FIRST NAMED INVENTOR	John A. Nix
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Keith Barkaus

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
petition-request.pdf	3	Terminal Disclaimer-Filed (Electronic)	45 KB
grantLetter.pdf	1	Terminal Disclaimer-Electronic-Approved	18 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
petition-request.pdf	3B0D34A82C7A5FCEFCA78B8F77D37200A48C0620F7217DC2160803059D733E25D4610F427502FD3927A1B094ABF24D38F0CEFD1B46E43B732B0A5F0E934B5149
grantLetter.pdf	6BB5199CDCD59AED8B416BE966D976209835E24DE19E0AED

4A0672DEE980A04FD26DB44E5DCCB3B1557871DC5F49FB32
710961CD33860D025C5C166EF6657F37

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A PRIOR PATENT

APPLICATION #	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET #
18416534	01/18/2024	John Nix	63121/0226

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

- ☑ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action
- ☑ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent interest
Network-1 Technologies, Inc.	100%
Total	**100%**

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

Application #	Filing Date

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.
In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

Patent #
10084768
10382422
11233780

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.
In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Terminal disclaimer fee under 37 CFR 1.20(d) included with Electronic Terminal Disclaimer request.

Applicant claims the following entity status:
Small

I hereby declare that all statements made herein of my own knowledge are true and that all statemnts made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I certify, in accordance with 37 CFR 1.4(d)(4) that I am: An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Signature	Name	Registration #
/Keith J Barkaus/	Keith Barkaus	51431

* Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this certification. See MPEP 324.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 18/416,534	Filing Date 01/18/2024	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $ 192 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	11/04/2024	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 22	Minus	** 22	= 0		x $40 =	0
	Independent (37 CFR 1.16(h))	* 1	Minus	*** 3	= 0		x $ 192 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/DORIS M KING/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/416,534	01/18/2024	John A. Nix	63121/0226	7559

1912 7590 09/18/2024

AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

EXAMINER	
HO, DAO Q	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
09/18/2024	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Petitioner Samsung Ex-1004, 0130

Office Action Summary	Application No. 18/416,534	Applicant(s) Nix, John A.	
	Examiner DAO Q HO	Art Unit 2432	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 1/18/2024.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-22 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-22 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 1/18/2024 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

This is a reply to the application filed on 1/18/2024, in which, claim(s) 1-22 are pending.

When making claim amendments, the applicant is encouraged to consider the references in their entireties, including those portions that have not been cited by the examiner and their equivalents as they may most broadly and appropriately apply to any particular anticipated claim amendments.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 4/9/2024 [12], has been reviewed. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Specification

The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Drawings

The drawings filed on 4/9/2024 is/are accepted by The Examiner.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-22 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor (or for applications subject to pre-AIA 35 U.S.C. 112, the applicant), regards as the invention.

The claims reciting "an eUICC" without properly defining what it represents.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*,

140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-22 are rejected on the ground of nonstatutory double patenting over claims 1-10 of U.S. Patent No. 10,084,768, claims 1-18 of U.S. Patent No. 10,382,422 and claims 1-22 of U.S. Patent No. 11,233,780. since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows:

Although the claims at issue are not identical, they are not patentably distinct from each other as claimed requires the details of a subcombination as separately claimed the inventions are not patentably distinct. For instance, the current application is a method claim which is anticipated by the parent patent No. 11,233,780, which is a device claim with steps that anticipated the method steps of the current application.

Allowable Subject Matter

Claim(s) 1-22 would be allowable if rewritten to overcome the rejection(s) set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

The following is an examiner's statement of reasons for allowance:

Independent Claim(s) 1 and their respective dependent claims are allowable over prior arts since the prior art of record (such as Rajadurai et al. (US 2013/0012168 - IDS), Park (US 2014/0219447 - IDS)) teach as follows:

The detailed manner in which PKI keys are utilized for both authentication and key derivation in the claimed invention are not contemplated by Rajadurai or Rajadurai when combined with the other cited references. For example, there is no description in Rajadurai for user equipment to create a digital signature using a PKI key, and the word "signature" (or equivalent for a digital signature) is not present in the Rajadurai publication. The claimed invention includes multiple PKI key pairs and their use for securing a system for an eUICC, while Rajadurai's only description of a private key is "a private key infrastructure (PKI) (including an UE certificate, and a root certificate)" for equipment. The claimed invention

includes detailed steps for deriving a profile key, including the use of PKI keys and algorithms to utilize, while the description in Rajadurai for deriving a subscription key (e.g. profile key) is limited to the user equipment "derives the subscription key using the decrypted operator shared key and the random number."

Particularly, with respect to independent claim 1, the Rajadurai reference does not contemplate recording "a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key", as recited in claim 1.

Further, with respect to independent claim 1, Rajadurai does not suggest an eUICC "deriving, by the eUICC, a profile key using a key exchange algorithm based on at least:

(i) the second eUICC private key, and

(ii) the recorded subscription manager public key,

wherein the profile key can also be derived at the subscription manager system based at least on:

(iii) the second eUICC public key, and

(iv) the subscription manager private key;" as recited in independent claim 1. In contrast to the above recited limitations, the description of key derivation for user equipment in the Rajadurai specification is limited to (i) paragraph 0024 where he states: "the user equipment 102A derives security keys and an operator shared key using the security keys upon successful verification of the authentication token", and (ii) paragraph 0028 where he states: "the user equipment 102A derives the subscription key using the operator shared key and the random number". The derivation of the subscription key in Rajadurai does not contemplate or suggest the key exchange recited independent claim 1. First, the security keys in the Rajadurai reference are

described as a shared secrets and not PKI-based keys, which are necessary for the recited key exchange. Also, there is no suggestion in Rajadurai of the eUICC receiving a server public key for input into a key exchange. Likewise, there is no suggestion of using a server public key and the eUICC private key to derive the profile key using a key exchange algorithm.

The Park reference discloses a method wherein an MNO receives a secret key allocated to a corresponding embedded UICC (eUICC) through SM-SR (secure routing) in an environment where SM is divided and implemented as SM-SR and SM-DP (data preparation). Park discloses fundamentally different technology for an eUICC, since keys and related information are communicated over secure channels that utilize asymmetric encryption, as opposed to the mutual derivation of encryption keys in the claimed invention. There are no teachings within Park for deriving keys, and consequently the ciphering keys for profile encryption/decryption are transmitted between endpoints for Park, whereas ciphering keys for profile encryption/decryption can be derived in the claimed invention. Further, Park does not suggest how an eUICC can authenticate a network or server, which can be an important step for securing a system with an eUICC.

With respect to independent claim 1, Park does not contemplate "(a) generating, by the embedded universal integrated circuit card, a first message comprising:

(1) an identity for the embedded universal integrated circuit card;

(2) a nonce; and

(3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key; (b) providing, by the by the embedded universal integrated circuit card to the network application." There are only two sentences in the Park reference where the eUICC generates a digital signature. In both paragraph

0107 and paragraph 0129, Park teaches "At this time, the eUICC may make an electronic signature using the public key of the SM-DP for checking a certificate." These teachings of Park do not suggest the recited limitation of claim 1. Park does not suggest using the eUICC private key for the first digital signature, and specifically states using the public key of the SM-DP.

In addition with respect to independent claim 1, Park teaches one level of encryption of a profile is accomplished via asymmetric ciphering, which is different than the limitations recited by claim 1. Specifically, the claim 1 recites

"(d) storing a subscription manager public key which corresponds to a subscription manager private key;

(e) deriving a profile key using a key exchange algorithm based on at least:

(i) the second eUICC private key, and

(ii) the recorded subscription manager public key,

wherein the profile key can also be derived at the subscription manager system based at least on:

(iii) the second eUICC public key, and

(iv) the subscription manager private key." There is no use of the words "key exchange", "derivation", or "derive" within Park, so there is no suggestion that a key for encrypting or decrypting a profile can be derived. In contrast, Park specifically teaches the different technology of an eUICC performing asymmetric decryption. Regarding decryption of a profile, in paragraph 0107 Park states: "Since the eUICC already knows the eUICC management key, the eUICC may completely decode the profile to be used for a provisioning by performing a second decoding using the private key corresponding to its public key after the first decoding." Park's contemplation of using asymmetric ciphering is further confirmed in paragraph 0104,

where the ciphering steps by the MNO are described: "The MNO which has obtained the public key (the encryption key) of the corresponding eUICC". The use of a public key to encrypt is associated with asymmetric ciphering. In contrast with the claimed invention, the profile is decrypted with a mutually derived key. There is no suggestion in Park for either (i) how an encryption key can be mutually derived, or (ii) the PKI keys that could be input into a key exchange algorithm.

For the above reasons, it would not have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the teachings of Rajadurai and Park with the other cited prior art to arrive at the claimed invention.

Internet Communications

Applicant is encouraged to submit a written authorization for Internet communications (PTO/SB/439, http:ljwww.uspto.gov/sites/default/files/documents/sb0439.pdf) in the instant patent application to authorize the examiner to communicate with the applicant via email. The authorization will allow the examiner to better practice compact prosecution. The written authorization can be submitted via one of the following methods *only*: (1) Central Fax which can be found in the Conclusion section of this Office action; (2) regular postal mail; (3) EFS WEB; or (4) the service window on the Alexandria campus. EFS web is the recommended way to submit the form since this allows the form to be entered into the file wrapper within the same day (system dependent). Written authorization submitted via other methods, such as *direct* fax to the examiner or email, will not be accepted. *See* MPEP § 502.03.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAO Q HO whose telephone number is (571)270-5998. The examiner can normally be reached on 7:00am - 5:00pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Nickerson can be reached on (469) 295-9235. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DAO Q HO/
Primary Examiner, Art Unit 2432

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/416,534	Nix, John A.
	Examiner	**Art Unit**
	DAO Q HO	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/17/2024								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								

Petitioner Samsung Ex-1004, 0141

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/416,534	Nix, John A.
	Examiner	Art Unit
	DAO Q HO	2432

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08	09/17/2024	dh

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
see attached SEARCH history	09/17/2024	dh
inventor and assignee in SEARCH	09/17/2024	dh
NPL: subscription authentication using SIM card with key exchange	09/17/2024	dh
CPC searches with delimiter	09/17/2024	dh

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
	general interference and searches of claim (PGPUB, USPAT)	09/17/2024	dh

/DAO Q HO/ Primary Examiner, Art Unit 2432	

Petitioner Samsung Ex-1004, 0142

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L2	76	((("NETWORK-1") near3 ("TECHNOLOGIES") near3 ("INC"))).AS,AANM.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2023/03/23 09:25 AM
L3	172	((("NIX") near3 ("John"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:25 AM
L4	268	2 3	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:25 AM
L5	1656	(eUICC WITH profile)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:33 AM
L6	60	4 AND 5	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:33 AM
L7	791	(mobile WITH eUICC WITH profile)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:33 AM
L8	42	4 AND 7	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:33 AM
L10	42	8 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 09:36 AM
L11	198	((authenticat$4 validat$6) WITH mobile WITH eUICC WITH profile)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 10:03 AM
L12	171	11 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 10:03 AM
L13	240	("10169587" OR "10621352" OR "20010029581" OR "20020018569" OR "20030003895" OR "20030211842" OR "20040162472" OR "20040179684" OR "20040221163" OR "20050008159" OR "20050021875" OR "20050050323" OR "20050058294" OR "20050120202" OR	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 10:11 AM

Petitioner Samsung Ex-1004, 0143

		"20050138353" OR "20050193199" OR "20050246282" OR "20050278787" OR "20060021063" OR "20060056355" OR "20060059344" OR "20060095771" OR "20060129848" OR "20060206710" OR "20060281442" OR "20070101400" OR "20070158439" OR "20070206799" OR "20080016230" OR "20080022089" OR "20080031204" OR "20080044032" OR "20080107083" OR "20080114978" OR "20080130879" OR "20080165698" OR "20080307218" OR "20090028341" OR "20090041110" OR "20090060197" OR "20090077643" OR "20090113203" OR "20090116642" OR "20090125996" OR "20090132806" OR "20090183541" OR "20090191857" OR "20090209232" OR "20090217348" OR "20090268909" OR "20090274306" OR "20090282246" OR "20090313472" OR "20100031042" OR "20100062808" OR "20100093347" OR "20100098253" OR "20100166167" OR "20100195833" OR "20100199334" OR "20100223461" OR "20100275028" OR "20110016321" OR "20110035584" OR "20110035604" OR "20110055553" OR "20110158411" OR "20110167272" OR "20110213959" OR "20110237281" OR "20110268022" OR "20110269422" OR					

Petitioner Samsung Ex-1004, 0144

		"20110269461" OR "20110269472" OR "20110270747" OR "20110291803" OR "20110314287" OR "20120011360" OR "20120011362" OR "20120023336" OR "20120030461" OR "20120033613" OR "20120072732" OR "20120084568" OR "20120087493" OR "20120089568" OR "20120108205" OR "20120117635" OR "20120159153" OR "20120170451" OR "20120190354" OR "20120214444" OR "20120260086" OR "20120260090" OR "20120260095" OR "20120263298" OR "20120278490" OR "20120300932" OR "20120331292" OR "20120331298" OR "20130007442" OR "20130012168" OR "20130028184" OR "20130091556" OR "20130114810" OR "20130117824" OR "20130122864" OR "20130149996" OR "20130157673" OR "20130165073" OR "20130165075" OR "20130166915" OR "20130173747" OR "20130173926" OR "20130179962" OR "20130182586" OR "20130183932" OR "20130212637" OR "20130227646" OR "20130231087" OR "20130283047" OR "20130294602" OR "20130305345" OR "20130322621" OR "20130331063" OR "20130340040" OR "20130344864" OR "20140003604" OR "20140040628" OR "20140049653" OR					

Petitioner Samsung Ex-1004, 0145

		"20140053241" OR "20140073375" OR "20140082358" OR "20140082359" OR "20140082538" OR "20140082539" OR "20140087790" OR "20140101444" OR "20140108801" OR "20140115335" OR "20140120874" OR "20140122878" OR "20140140507" OR "20140140509" OR "20140143534" OR "20140143826" OR "20140161113" OR "20140165155" OR "20140192976" OR "20140219447" OR "20140219448" OR "20140235210" OR "20140237101" OR "20140244994" OR "20140273913" OR "20140281483" OR "20140287725" OR "20140308991" OR "20140329502" OR "20140337937" OR "20140351403" OR "20140357229" OR "20150012743" OR "20150017910" OR "20150071139" OR "20150089214" OR "20150092590" OR "20150095514" OR "20150095648" OR "20150106616" OR "20150113275" OR "20150121066" OR "20150121495" OR "20150143125" OR "20150163056" OR "20150215126" OR "20150222604" OR "20150222619" OR "20150281964" OR "20150350881" OR "20160014112" OR "20160057725" OR "20160088096" OR "20160127132" OR "20160149903" OR "20160294829" OR "20170206532" OR "20190313246" OR				

Petitioner Samsung Ex-1004, 0146

		"20190332774" OR "20190356482" OR "20200162247" OR "20200162269" OR "20200226258" OR "20200280436" OR "20210126801" OR "20210184842" OR "20210194681" OR "20210211279" OR "20210218560" OR "5216715" OR "5642420" OR "5664017" OR "5852665" OR "5995625" OR "6038322" OR "6256733" OR "6721886" OR "6804357" OR "6842628" OR "7921292" OR "7957532" OR "8127142" OR "8352739" OR "8434139" OR "8452017" OR "8522013" OR "8526606" OR "8555067" OR "8577337" OR "8590028" OR "8782774" OR "8843179" OR "8924715" OR "8948386" OR "8965366" OR "9002018" OR "9020479" OR "9253643" OR "9270653" OR "9332129" OR "9408012" OR "9572016" OR "9596078" OR "9628981" OR "9674690" OR "9698981" OR "9794775" OR "9800993" OR "9807605" OR "9923724").pn.					
L14	5	11 AND 13	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 10:12 AM
L15	128	((elliptic NEAR curve) WITH (diffie NEAR hellman) WITH derive	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:51 AM

Petitioner Samsung Ex-1004, 0147

		WITH key)					
L16	13	13 AND 15	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:52 AM
L17	19	11 AND 15	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:52 AM
L18	3813	((elliptic NEAR curve) WITH (diffie NEAR hellman) WITH key)	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:52 AM
L19	27	11 AND 18	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:53 AM
L20	366	(authenticat$4 WITH network$2 WITH plaintext$2)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:32 PM
L21	19	11 AND 20	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:32 PM
L22	19	21 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:32 PM
L23	248	18 AND (mobile WITH (sim eUICC))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:34 PM
L24	100	23 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:34 PM
L25	9	13 AND 23	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/03/23 01:34 PM
L26	42	((UICC near3 profile) WITH subscriber)	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2023/10/12 02:31 PM
L27	21	26 AND ((H04W12/35 OR H04W12/06 OR H04L63/0853 OR H04L63/08).cpc.)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 02:31 PM
L30	12	26 AND (decrypt$4 WITH key)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 02:32 PM
L31	7	30 AND (profile WITH key WITH ident$6)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 03:04 PM
L32	1600	(decrypt$4 WITH profile WITH key)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 03:48 PM
L33	51	(decrypt$4 WITH (first near2 (part$2 portion)) WITH profile WITH key)	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 03:48 PM
L34	21	33 AND (mobile WITH (sim eUICC))	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/10/12 03:49 PM
L35	1	13 AND 34	(US-PGPUB; USPAT;	OR	ON	ON	2023/10/12

Petitioner Samsung Ex-1004, 0148

			USOCR; EPO; JPO; DERWENT)				05:14 PM
L36	240	("10169587" OR "10621352" OR "20010029581" OR "20020018569" OR "20030003895" OR "20030211842" OR "20040162472" OR "20040179684" OR "20040221163" OR "20050008159" OR "20050021875" OR "20050050323" OR "20050058294" OR "20050120202" OR "20050138353" OR "20050193199" OR "20050246282" OR "20050278787" OR "20060021063" OR "20060056355" OR "20060059344" OR "20060095771" OR "20060129848" OR "20060206710" OR "20060281442" OR "20070101400" OR "20070158439" OR "20070206799" OR "20080016230" OR "20080022089" OR "20080031204" OR "20080044032" OR "20080107083" OR "20080114978" OR "20080130879" OR "20080165698" OR "20080307218" OR "20090028341" OR "20090041110" OR "20090060197" OR "20090077643" OR "20090113203" OR "20090116642" OR "20090125996" OR "20090132806" OR "20090183541" OR "20090191857" OR "20090209232" OR "20090217348" OR "20090268909" OR "20090274306" OR "20090282246" OR "20090313472" OR "20100031042" OR "20100062808" OR	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:24 PM

Petitioner Samsung Ex-1004, 0149

		"20100093347" OR "20100098253" OR "20100166167" OR "20100195833" OR "20100199334" OR "20100223461" OR "20100275028" OR "20110016321" OR "20110035584" OR "20110035604" OR "20110055553" OR "20110158411" OR "20110167272" OR "20110213959" OR "20110237281" OR "20110268022" OR "20110269422" OR "20110269461" OR "20110269472" OR "20110270747" OR "20110291803" OR "20110314287" OR "20120011360" OR "20120011362" OR "20120023336" OR "20120030461" OR "20120033613" OR "20120072732" OR "20120084568" OR "20120087493" OR "20120089568" OR "20120108205" OR "20120117635" OR "20120159153" OR "20120170451" OR "20120190354" OR "20120214444" OR "20120260086" OR "20120260090" OR "20120260095" OR "20120263298" OR "20120278490" OR "20120300932" OR "20120331292" OR "20120331298" OR "20130007442" OR "20130012168" OR "20130028184" OR "20130091556" OR "20130114810" OR "20130117824" OR "20130122864" OR "20130149996" OR "20130157673" OR "20130165073" OR "20130165075" OR "20130166915" OR "20130173747" OR				

Petitioner Samsung Ex-1004, 0150

		"20130173926" OR "20130179962" OR "20130182586" OR "20130183932" OR "20130212637" OR "20130227646" OR "20130231087" OR "20130283047" OR "20130294602" OR "20130305345" OR "20130322621" OR "20130331063" OR "20130340040" OR "20130344864" OR "20140003604" OR "20140040628" OR "20140049653" OR "20140053241" OR "20140073375" OR "20140082358" OR "20140082359" OR "20140082538" OR "20140082539" OR "20140087790" OR "20140101444" OR "20140108801" OR "20140115335" OR "20140120874" OR "20140122878" OR "20140140507" OR "20140140509" OR "20140143534" OR "20140143826" OR "20140161113" OR "20140165155" OR "20140192976" OR "20140219447" OR "20140219448" OR "20140235210" OR "20140237101" OR "20140244994" OR "20140273913" OR "20140281483" OR "20140287725" OR "20140308991" OR "20140329502" OR "20140337937" OR "20140351403" OR "20140357229" OR "20150012743" OR "20150017910" OR "20150071139" OR "20150089214" OR "20150092590" OR "20150095514" OR "20150095648" OR "20150106616" OR "20150113275" OR				

Petitioner Samsung Ex-1004, 0151

		"20150121066" OR "20150121495" OR "20150143125" OR "20150163056" OR "20150215126" OR "20150222604" OR "20150222619" OR "20150281964" OR "20150350881" OR "20160014112" OR "20160057725" OR "20160088096" OR "20160127132" OR "20160149903" OR "20160294829" OR "20170206532" OR "20190313246" OR "20190332774" OR "20190356482" OR "20200162247" OR "20200162269" OR "20200226258" OR "20200280436" OR "20210126801" OR "20210184842" OR "20210194681" OR "20210211279" OR "20210218560" OR "5216715" OR "5642420" OR "5664017" OR "5852665" OR "5995625" OR "6038322" OR "6256733" OR "6721886" OR "6804357" OR "6842628" OR "7921292" OR "7957532" OR "8127142" OR "8352739" OR "8434139" OR "8452017" OR "8522013" OR "8526606" OR "8555067" OR "8577337" OR "8590028" OR "8782774" OR "8843179" OR "8924715" OR "8948386" OR "8965366" OR "9002018" OR "9020479" OR "9253643" OR "9270653" OR				

Petitioner Samsung Ex-1004, 0152

		"9332129" OR "9408012" OR "9572016" OR "9596078" OR "9628981" OR "9674690" OR "9698981" OR "9794775" OR "9800993" OR "9807605" OR "9923724").pn.					
L38	2	((eUICC near3 key) WITH subscrib$4 WITH (diffie near2 hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:26 PM
L39	29	32 AND 36	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:26 PM
L40	0	(((universal NEAR integrat$4 NEAR circuit NEAR card) near3 key) WITH subscrib$4 WITH (diffie near2 hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:27 PM
L41	0	(((univer$6 near2 integrat$4 near2 circuit$2 NEAR card) near3 key) WITH subscrib$4 WITH (diffie near2 hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:28 PM
L42	3	((UICC near3 key) WITH subscrib$4 WITH (diffie near2 hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:28 PM
L43	3	"20180084415"	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:29 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	19	((authenticat$4 validat$6) WITH mobile WITH eUICC WITH profile).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 10:04 AM
N2	38	((elliptic NEAR curve) WITH (diffie NEAR hellman) WITH derive WITH key).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 11:52 AM
N3	0	N1 AND N2	(US-PGPUB; USPAT)	OR	ON	ON	2023/03/23 01:33 PM
N4	3	((UICC near3 key) WITH subscrib$4 WITH (diffie near2 hellman)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/09/17 08:45 PM

Petitioner Samsung Ex-1004, 0153

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060206710	A1	2006-09-14	Gehrmann	
	2	20060281442	A1	2006-12-14	Lee et al.	
	3	20070206799	A1	2007-09-06	Wingert et al.	
	4	20080016230	A1	2008-01-17	Hollmanns et al.	
	5	20080022089	A1	2008-01-24	Leedom	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	6	20080114978	A1	2008-05-15	Lehtoviorta et al.	
	7	20080165698	A1	2008-07-10	Dalsgard et al.	
	8	20090116642	A1	2009-05-07	Yang et al.	
	9	20090028341	A1	2009-01-29	Hamachi	
	10	20090077643	A1	2009-03-19	Schmidt et al.	
	11	20090125996	A1	2009-05-14	Guccione et al.	
	12	20090132806	A1	2009-05-21	Blommaert et al.	
	13	20090191857	A1	2009-07-30	Horn et al.	
	14	20090209232	A1	2009-08-20	Cha et al.	
	15	20090268909	A1	2009-10-29	Girao et al.	
	16	20090282246	A1	2009-11-12	Gunther	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	17	20090313472	A1	2009-12-17	Guccione et al.	
	18	20100166167	A1	2010-07-01	Karimi-Cherkandi et al.	
	19	20100031042	A1	2010-02-04	Di Crescenzo et al.	
	20	20100062808	A1	2010-03-11	Cha et al.	
	21	20100098253	A1	2010-04-22	Delerablee	
	22	20100275028	A1	2010-10-28	Takashima	
	23	20110016321	A1	2011-01-20	Sundaram et al.	
	24	20110055553	A1	2011-03-03	Lee et al.	
	25	20110237281	A1	2011-09-20	Busropan et al.	
	26	20110291803	A1	2011-12-01	Bajic et al.	
	27	20110314287	A1	2011-12-22	Escott et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	28	20120011360	A1	2012-01-12	Engels et al.	
	29	20120023336	A1	2012-01-26	Natarajan	
	30	20120072732	A1	2012-03-22	Canard et al.	
	31	20120089568	A1	2012-04-12	Manley et al.	
	32	20120108205	A1	2012-05-03	Schell et al.	
	33	20120117635	A1	2012-05-10	Schell et al.	
	34	20120159153	A1	2012-06-21	Shim et al.	
	35	20120260086	A1	2012-10-11	Haggerty et al.	
	36	20120260090	A1	2012-10-11	Hauck et al.	
	37	20120260095	A1	2012-10-11	Von Hauck et al.	
	38	20120278490	A1	2012-11-01	Sennett et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	39	20120300932	A1	2012-11-29	Cambridge et al.	
	40	20120331292	A1	2012-12-27	Haggerty et al.	
	41	20130091556	A1	2013-04-11	Horn et al.	
	42	20130114810	A1	2013-05-09	Kobayashi et al.	
	43	20130117824	A1	2013-05-09	Naslund et al.	
	44	20130149996	A1	2013-06-13	King et al.	
	45	20130166915	A1	2013-06-27	desai et al.	
	46	20130173747	A1	2013-07-04	Kim et al.	
	47	20130212637	A1	2013-08-15	Guccione et al.	
	48	20130227646	A1	2013-08-29	Haggerty et al.	
	49	20130305345	A1	2013-11-14	Bugenhagen	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	50	20130322621	A1	2013-12-05	Yoon et al.	
	51	20130331063	A1	2013-12-12	Cormier et al.	
	52	20140003604	A1	2014-01-02	Campagna et al.	
	53	20140053241	A1	2014-02-20	Norman et al.	
	54	20140073375	A1	2014-03-13	Li et al.	
	55	20140082358	A1	2014-03-20	Nakhjiri et al.	
	56	20140082359	A1	2014-03-20	Nakhjiri et al.	
	57	20140087790	A1	2014-03-27	Babbage et al.	
	58	20140101444	A1	2014-04-10	Lee et al.	
	59	20140108801	A1	2014-04-17	McBride et al.	
	60	20140140507	A1	2014-05-22	Park et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DAO Q HO/	Date Considered	09/17/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
	2					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20130149996	A1	2013-06-13	King et al.	
	2	20130166915	A1	2013-06-27	Desai et al.	
	3	20130173747	A1	2013-07-04	Kim et al.	
	4	20130212637	A1	2013-08-15	Guccione et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	5	20130227646	A1	2013-08-29	Haggerty et al.	
	6	20130305345	A1	2013-11-14	Bugenhagen	
	7	20130322621	A1	2013-12-05	Yoon et al.	
	8	20130331063	A1	2013-12-12	Cormier et al.	
	9	20140003604	A1	2014-01-02	Campagna et al.	
	10	20140053241	A1	2014-02-20	Norman et al.	
	11	20140073375	A1	2014-03-13	Li et al.	
	12	20140082538	A1	2014-03-20	Nakhjiri et al.	
	13	20140082539	A1	2014-03-20	Nakhjiri et al.	
	14	20140087790	A1	2014-03-27	Babbage et al.	
	15	20140101444	A1	2014-04-10	Lee et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	16	20140108801	A1	2014-04-17	McBride et al.	
	17	20140140507	A1	2014-05-22	Park et al.	
	18	20140143826	A1	2014-05-22	Sharp et al.	
	19	20140161113	A1	2014-06-12	Cui et al.	
	20	20140165155	A1	2014-06-12	Zhang	
	21	20140192976	A1	2014-07-10	Yoon et al.	
	22	20140219447	A1	2014-08-07	Park et al.	
	23	20140219448	A1	2014-08-07	Froels et al.	
	24	20140244994	A1	2014-08-28	Yu	
	25	20140273913	A1	2014-09-18	Michel et al.	
	26	20140287725	A1	2014-09-25	Lee	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	27	20140337937	A1	2014-11-13	Truskovsky et al.	
	28	20140351403	A1	2014-11-27	Lin et al.	
	29	20150012743	A1	2015-01-08	Holtmanns et al.	
	30	20150017910	A1	2015-01-15	Li et al.	
	31	20150071139	A1	2015-03-12	Nix	
	32	20150092590	A1	2015-04-02	Zhu et al.	
	33	20150095514	A1	2015-04-02	Yu	
	34	20150095648	A1	2015-04-02	Nix	
	35	20150113275	A1	2015-04-23	Kim et al.	
	36	20150121495	A1	2015-04-30	Gao et al.	
	37	20130231087	A1	2013-09-05	O'Leary	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	38	20130165073	A1	2013-06-27	Madsen	
	39	20130007442	A1	2013-01-03	Yinian Mao et al.	
	40	20120170451	A1	2012-07-05	Harish Viswanathan et al.	
	41	20120084568	A1	2012-04-05	Bellcet Sarikaya et al.	
	42	20120030461	A1	2012-02-02	William Daniel Willey et al.	
	43	20080307218	A1	2008-12-11	Oleg Logvinov	
	44	20110035584	A1	2011-02-10	Meyerstein et al.	
	45	20090060197	A1	2009-03-05	Taylor et al.	
	46	20150089214	A1	2015-03-26	Dupre	
	47	20140122878	A1	2014-05-01	Cho et al.	
	48	20140115335	A1	2014-04-24	Jorden et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	49	20130173926	A1	2013-07-04	Morese et al.	
	50	20130012168	A1	2013-01-10	Rajadurai et al.	
	51	20120331298	A1	2012-12-27	Xu et al.	
	52	20120190354	A1	2012-07-26	Merrien et al.	
	53	20040221163	A1	2004-11-04	Jorgensen et al.	
	54	20090113203	A1	2009-04-30	Tsuge et al.	
	55	20150163056	A1	2015-06-11	Nix	
	56	20090217348	A1	2009-08-27	Salmela et al.	
	57	20080130879	A1	2008-06-05	Heinonen et al.	
	58	20130122864	A1	2013-05-16	Haggerty et al.	
	59	20150071139	A1	2015-03-12	Nix	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	60	20150095648	A1	2015-04-02	Nix	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DAO Q HO/	Date Considered	09/17/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Network-1 Technologies, Inc.	Confirmation No.: 7559
Title:	EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION	
Appl. No.:	18/416,534	
Filing Date:	January 18, 2024	
Examiner:	TBD	
Art Unit:	TBD	
Docket No.:	63121/0226	
Customer No.:	01912	

INFORMATION DISCLOSURE STATEMENT LETTER
UNDER 37 CFR § 1.56

Via Patent Center
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure under 37 C.F.R. §1.56, Applicant would like to direct the Examiner's attention to the references that are listed on the attached forms PTO/SB/08A. In addition to any copies of Foreign Patent Documents and Non-Patent Literature Documents submitted herewith, Applicant refers the Examiner to the references previously submitted to or cited by the Patent Office during prosecution of U.S. Patent Application No. 17/547,990, filed December 10, 2021, now U.S. Patent No. 11,916,893, U.S. Patent Application No. 16/453,682 filed June 26, 2019, now U.S. Patent No. 11,233,780, U.S. Patent Application No. 16/110,804, filed August 23, 2018, U.S. Patent Application No. 15/928,848 filed March 22, 2018, now U.S. Patent No. 10,084,768, U.S. Patent Application No. 14/751,119 filed June 25, 2015, now U.S. Patent No. 9,961,060 and U.S. Patent Application No. 14/099,329 filed December 6, 2013, now U.S. Patent No. 9,100,175, from which the subject application claims priority under 35 U.S.C. §120. Accordingly, pursuant to 37 C.F.R. § 1.98(d), copies of

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Petitioner Samsung Ex-1004, 0172

previously cited or submitted references and Non-Patent Literature Documents are not included with this Information Disclosure Statement.

Reference to Related Patents and Co-Pending Applications

The below chart provides information regarding related issued patents and co-pending applications filed by the present Applicant:

Serial No.	Attorney Docket No.	Filing Date	Status
18/435,042	63121/0230	2024-02-07	Pending – Ready for Examination
18/587,462	63121/0229	2024-02-26	Pending – Ready for Examination
18/433,683	63121/0228	2024-02-06	Pending – Ready for Examination
18/438,147	63121/0227	2024-02-09	Pending – Undergoing Preexam Processing
18/416,534	**63121/0226**	**204-01-18**	**Present Application**
18/433,664	63121/0225	2024-02-06	Pending – Ready for Examination
18/229,907	63121/0224	2023-08-03	Pending – Response to Final OA Filed 2024-03-28
18/111,669	63121/0222	2023-02-20	Non-Final OA mailed 2023-10-02
17/647,812	63121/0213	2022-01-13	USP 11,606,204
17/547,990	63121/0212	2021-12-10	USP 11,736,283
17/304,922	63121/0209	2021-06-28	USP 11,736,283
17/249,242	63121/0202	2021-02-24	Response to Non-Final OA filed 2023-11-13
16/879,325	63121/0198	2020-05-20	USP 11,082,218
16/843,107	63121/0197	2020-04-08	USP 11,283,603
16/721,153	63121/0195	2019-12-19	USP 11,539,681
16/593,561	63121/0190	2019-10-04	USP 11,258,595
16/453,682	63121/0184	2019-06-26	USP 11,233,780
16/271,455	63121/0181	2019-02-08	USP 10,594,679
16/271,428	63121/0180	2019-02-08	USP 10,523,432
16/201,401	63121/0179	2018-11-27	USP 10,700,856
16/200,118	63121/0178	2018-11-26	USP 10,498,530
16/110,804	63121/0168	2018-08-23	USP 10,382,422
16/036,506	63121/0167	2018-07-16	USP 10,530,575
15/983,957	63121/0163	2018-05-18	USP 10,177,911
15/973,012	63121/0162	2018-05-07	USP 10,250,386

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Petitioner Samsung Ex-1004, 0173

15/972,914	63121/0161	2018-05-07	USP 10,652,017
15/928,848	63121/0160	2018-03-22	USP 10,084,768
15/010,905	63121/0157	2016-01-29	USP 9,641,327
15/680,758	63121/0147	2017-08-18	USP 10,187,206
15/162,292	63121/0146	2016-05-23	USP 10,362,012
14/751,119	63121/0145	2015-06-25	USP 9,961,060
15/457,700	63121/0144	2017-03-13	USP 9,998,281
15/583,968	63121/0143	2017-05-01	USP 10,057,059
15/043,293	63121/0142	2016-02-12	USP 9,998,280
15/642,088	63121/0141	2017-07-05	USP 10,003,461
15/130,146	63121/0140	2016-04-15	USP 9,742,562
15/162,302	63121/0139	2016-05-23	USP 9,698,981
14/789,255	63121/0138	2015-07-01	USP 9,596,078
14/139,419	63121/0137	2013-12-23	USP 9,351,162
14/136,711	63121/0136	2013-12-20	USP 9,300,473
14/099,329	63121/0135	2013-12-06	USP 9,100,175
14/084,141	63121/0134	2013-11-19	USP 9,319,223
14/064,618	63121/0133	2013-10-28	USP 9,118,464
14/055,606	63121/0132	2013-10-16	USP 9,276,740
14/039,401	63121/0131	2013-09-27	USP 9,288,059
14/023,181	63121/0130	2013-09-10	USP 9,350,550
AU 2019246774	63121-0199	2019-10-08	AU2019246774A1 Issued 2021-09-23
GB 1608573	63121-0151	2014-10-27	Published on 2016-08-03
GB 2100530	63121-0201	2014-10-27	Published on 2021-05-12
CA 2,965,119	63121-0152	2014-10-27	Published on 2015-05-07
HK 17101082.8	63121-0153	2014-10-27	Published on 2017-10-20
EU 14868381.6	63121-0154	2014-12-04	Published on 2017-01-04
CA 2,969,829	63121-0155	2014-12-04	Published on 2015-06-11
HK 17106540.3	63121-0156	2014-12-04	Published on 2018-01-19

4854-6578-3220v.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Petitioner Samsung Ex-1004, 0174

The Examiner is invited to review the prosecution history of each of these applications, including the cited references of record and related office actions, as the Examiner deems appropriate.

* * * * *

This Information Disclosure Statement is being filed within three months of the filing date and before the mailing date of a first Office Action on the merits in the present application. No certification or fee is required. Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered. Please charge any fee deficiency or credit any overpayment to Deposit Account No. 01-1785, under Docket No. 63121/0226.

Respectfully submitted,

AMSTER, ROTHSTEIN & EBENSTEIN LLP
Attorneys for Applicant
405 Lexington Avenue
New York, NY 10174
(212) 336-8000

Dated: April 9, 2024

By: /Keith J. Barkaus/
Keith J. Barkaus
Reg. No. 51,431

/DAO Q HO/

09/17/2024

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Petitioner Samsung Ex-1004, 0175

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20150106616	A1	2015-04-16	Nix	
	2	20150121066	A1	2015-04-30	Nix	
	3	20150143125	A1	2015-05-21	Nix	
	4	20040162472	A1	2004-08-19	Berson et al.	
	5	20150215126	A1	2015-07-30	Ashdown	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	6	20160294829	A1	2016-10-06	Angus	
	7	20120108205	A1	2012-05-03	Schell et al.	
	8	20130012168	A1	2013-01-10	Rajadurai et al.	
	9	20140219447	A1	2014-08-07	Park et al.	
	10	20140161113	A1	2014-06-12	Cui et al.	
	11	20150113275	A1	2015-04-23	Kim et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	10-2013-0026352	KR	A	2013-03-13			☐
	2	10-2013-0026958	KR	A	2013-03-14			☐
	3	EP 1981 224	EP		2008-10-15			☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	4	2013027085	WO	A1	2013-02-28			☐
	5	2013066077	WO	A1	2013-05-10			☐
	6	2775853	CA	A1	2012-12-01			☐
	7	2011138238	WO	A1	2011-11-10			☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report for PCT/US2014/068544 dated February 13, 2015.	☐
	2	T. Pornin, Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm ECDSA), Internet Engineering Task Force RFC 6979, August 2013, pp.I-79.	☐
	3	GSMA, Fast Dormancy Best Practices Version 1.0,27 July 2011, TS.18, pp. 1-23.	☐
	4	N. CHU et al, EXALTED: Expanding LTE for Devices, European Commission for Information Society and Media, 31 October 2012, pp. 1-141.	☐
	5	J. HUANG et al, A Close Examination of Performance and Power Characteristics of 4G LTE Networks, Mobisys' 12, 25-29 June 2012, pp. 1-14.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	6	F. QIAN et al, TOP: Tail Optimization Protocol for Cellular Resource Allocation, 18th IEEE International Conference on Network Protocols (ICNP), 2010, 5-8 Oct. 2010, pp. 285-298.	☐
	7	ETSI, Machine-to-Machine communications (M2M), mia, dla, and mid interfaces, TS 102.921 v1.1.1, Feb 2012, pp. 1-538.	☐
	8	C. DOWNEY, Migrating Legacy M2M Systems to the Cloud, http://www.ecnmag.com/articles/2013/02/migrating-legacy-m2m-systems-cloud, Feb 2013, pp. 1-2.	☐
	9	A. Wander et al, Energy Analysis of Public-Key Cryptography on Small Wireless Devices, Sun Microsystems Laboratories, pp.1-16.	☐
	10	V. Martinez et al, A Survey of the Elliptic Curve Integrated Encryption Scheme, Journal of Computer Science and Engineering, Volume 2, August 2010, pp.7-13.	☐
	11	ETSI, UMTS;LTE; SIM/USIM Internal and External Interworking Aspects, TR 131900 v.10.0.0, May 2011, pp.1-41.	☐
	12	International Search Report and Written Opinion for PCT/US2014/062435 mailed February 6, 2015.	☐
	13	Wikipedia, RSA (algorithm), http://en.wikipedia.org/wiki/RSA_(algorithm), 9 Sept. 2013, pp. 1-12.	☐
	14	Wikipedia, Elliptic Curve Cryptography, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography, 9 Sept. 2013, pp. 1-8 .	☐
	15	L. LARZON, The Lightweight User Datagram Protocol (UDP-Lite), Internet Engineering Task Force RFC 3828, July 2004, pp. 1-12.	☐
	16	Wikipedia, Digital Signature, http://en.wikipedia.orglwiki/Digital_signature, 9 Sept. 2013, pp. 1-10.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	17	D. Cooper, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force RFC 5280, pp. 1-133.	☐
	18	J. Jonsson et al, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Internet Engineering Task Force RFC 3447, February 2003, pp.1-72.	☐
	19	D. McGrew et al, Fundamental Elliptic Curve Cryptography Algorithms, Internet Engineering Task Force RFC 6090, February 2011, pp. 1-34.	☐
	20	Wikipedia, Elliptic Curve Diffie-Hellman, http://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman, 24 Sept. 2013, pp. 1-2.	☐
	21	ETSI, Smart Cards; Embedded UICC; Requirements Specification, TS 103 383 v12.1.0, June 2013, pp. 1-20.	☐
	22	3GPP, 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture, 3GPP TS 33.401 V12.9.0 (2013-09) pp. 1-75.	☐
	23	3GPP, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3, 3GPP TS 24.301 v12.2.0, Sept. 2013 pp. 1-6, 63-100.	☐
	24	ETSI, Smart Cards; UICC-Terminal Interfaces; Physical and Logical Characteristics, TS 102 221 v11.0.0, June 2012, pp. 1-181.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DAO Q HO/	Date Considered	09/17/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120033613	A1	2012-02-09	Lin et al.	
	2	20130028184	A1	2013-01-31	Lee et al.	
	3	20130182586	A1	2013-07-18	Paladugu et al.	
	4	20020018569	A1	2002-02-14	Panjwani et al.	
	5	20030003895	A1	2003-01-02	Wallentin et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	6	20030211842	A1	2003-11-13	Kempf et al.	
	7	20040179684	A1	2004-09-16	Appenzeller et al.	
	8	20050008159	A1	2005-01-13	Grilli et al.	
	9	20050021875	A1	2005-01-27	Bouthemy et al.	
	10	20050120202	A1	2005-06-02	Cuellar et al.	
	11	20050138353	A1	2005-06-23	Spies et al.	
	12	20050193199	A1	2005-09-01	Asokan et al.	
	13	20050246282	A1	2005-11-03	Naslund et al.	
	14	20050278787	A1	2005-12-15	Naslund et al.	
	15	20060021063	A1	2006-01-26	Hori	
	16	20060056355	A1	2006-03-16	Love et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	17	20060059344	A1	2006-03-16	Mononen	
	18	20060206710	A1	2006-09-14	Gehrmann	
	19	20060281442	A1	2006-12-14	Lee et al.	
	20	20070206799	A1	2007-09-06	Wingert et al.	
	21	20080016230	A1	2008-01-17	Holtmanns et al.	
	22	20080022089	A1	2008-01-24	Leedom	
	23	20080114978	A1	2008-05-15	Lehtovirta et al.	
	24	20080165698	A1	2008-07-10	Dalsgaard et al.	
	25	20090116642	A1	2009-05-07	Yang et al.	
	26	20090028341	A1	2009-01-29	Hamachi	
	27	20090077643	A1	2009-03-19	Schmidt et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	28	20090125996	A1	2009-05-14	Guccione et al.	
	29	20090132806	A1	2009-05-21	Blommaert et al.	
	30	20090191857	A1	2009-07-30	Horn et al.	
	31	20090209232	A1	2009-08-20	Cha et al.	
	32	20090268909	A1	2009-10-29	Girao et al.	
	33	20090282246	A1	2009-11-12	Gunther	
	34	20090313472	A1	2009-12-17	Guccione et al.	
	35	20100166167	A1	2010-07-01	Karimi-Cherkandi et al.	
	36	20100031042	A1	2010-02-04	Di Crescenzo et al.	
	37	20100062808	A1	2010-03-11	Cha et al.	
	38	20100098253	A1	2010-04-22	Delerablee	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	39	20100275028	A1	2010-10-28	Takashima	
	40	20110016321	A1	2011-01-20	Sundaram et al.	
	41	20110055553	A1	2011-03-03	Lee et al.	
	42	20110237281	A1	2011-09-29	Busropan et al.	
	43	20110291803	A1	2011-12-01	Bajic et al.	
	44	20110314287	A1	2011-12-22	Escott et al.	
	45	20120011360	A1	2012-01-12	Engels et al.	
	46	20120023336	A1	2012-01-26	Natarajan	
	47	20120072732	A1	2012-03-22	Canard et al.	
	48	20120089568	A1	2012-04-12	Manley et al.	
	49	20120108205	A1	2012-05-03	Schell et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	50	20120117635	A1	2012-05-10	Schell et al.	
	51	20120159153	A1	2012-06-21	Shim et al.	
	52	20120260086	A1	2012-10-11	Haggerty et al.	
	53	20120260090	A1	2012-10-11	Hauck et al.	
	54	20120260095	A1	2012-10-11	Von Hauck et al.	
	55	20120278490	A1	2012-11-01	Sennett et al.	
	56	20120300932	A1	2012-11-29	Cambridge et al.	
	57	20120331292	A1	2012-12-27	Haggerty et al.	
	58	20130091556	A1	2013-04-11	Horn et al.	
	59	20130114810	A1	2013-05-09	Kobayashi et al.	
	60	20130117824	A1	2013-05-09	Naslund et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DAO Q HO/	Date Considered	09/17/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8127142	B2	2012-02-28	Cuppett	
	2	8522013	B2	2013-08-27	Zhang et al.	
	3	8843179	B2	2014-09-23	Li et al.	
	4	9408012	B2	2016-08-02	Li et al.	
	5	8924715	B2	2014-12-30	Schell et al.	
	6	9698981	B2	2017-07-04	Nix	
	7	9596078	B2	2017-03-14	Nix	
	8	8434139	B1	2013-04-30	Ortiz, Jr.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	9	8965366	B1	2015-02-24	Somayajula et al.	
	10	9020479	B1	2015-04-28	Somayajula et al.	
	11	9253643	B2	2016-02-02	Pattar et al.	
	12	6038322		2000-03-14	Harkins	
	13	7921292	B1	2011-04-05	Pauker et al.	
	14	8526606	B2	2013-09-03	Muthaiah	
	15	8555067	B2	2013-10-08	Schell et al.	
	16	8590028	B2	2013-11-19	Saxena et al.	
	17	8782774	B1	2014-07-15	Pahl et al.	
	18	8948386	B2	2015-02-03	Campagna et al.	
	19	9002018	B2	2015-04-07	Wilkins et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	20	9253643	B2	2016-02-02	Pattar et al.	
	21	8434139	B1	2013-04-30	Ortiz, Jr.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140281483	A1	2014-09-18	Vigliaturo et al.	
	2	20130179962	A1	2013-07-11	Arial et al.	
	3	20080031204	A1	2008-02-07	Sood	
	4	20090041110	A1	2009-02-12	Malladi	
	5	20090282246	A1	2009-11-12	Gunther	
	6	20090274306	A1	2009-11-05	Nolte	
	7	20140140509	A1	2014-05-22	Chastain et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	8	20140143534	A1	2014-05-22	Chastain et al.	
	9	20140237101	A1	2014-08-21	Park	
	10	20140235210	A1	2014-08-21	Park et al.	
	11	20060095771	A1	2006-05-04	Appenzeller et al.	
	12	20100223461	A1	2010-09-02	Drader et al.	
	13	20100199334	A1	2010-08-05	Ehrensvard et al.	
	14	20140040628	A1	2014-02-06	Fort et al.	
	15	20070101400	A1	2007-05-03	Freeman et al.	
	16	20160014112	A1	2016-01-14	Gunning et al.	
	17	20150222619	A1	2015-08-06	Hughes et al.	
	18	20010029581	A1	2001-10-11	Knauft	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	19	20140049653	A1	2014-02-20	Leonard et al.	
	20	20120214444	A1	2012-08-23	McBride et al.	
	21	20050050323	A1	2005-03-03	Mizrah	
	22	20090183541	A1	2009-07-23	Sadighi et al.	
	23	20100195833	A1	2010-08-05	Priestley et al.	
	24	20150222604	A1	2015-08-06	Ylonen	
	25	20110268022	A1	2011-11-03	Xu	
	26	20140357229	A1	2014-12-04	Lee et al.	
	27	20110167272	A1	2011-07-07	Kolesnikov	
	28	20160127132	A1	2016-05-05	Lee et al.	
	29	20170206532	A1	2017-07-20	Choi	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	30	20160294829	A1	2016-10-06	Angus	
	31	20150215126	A1	2015-07-30	Ashdown	
	32	20040162472	A1	2004-08-19	Berson et al.	
	33	20110269422	A1	2011-11-03	Xu et al.	
	34	20110269461	A1	2011-11-03	Xu et al.	
	35	20110269472	A1	2011-11-03	Xu et al.	
	36	20110270747	A1	2011-11-03	Xu	
	37	20130294602	A1	2013-11-07	Huxham et al.	
	38	20130340040	A1	2013-12-19	Park et al.	
	39	20140308991	A1	2014-10-16	Lee et al.	
	40	20140329502	A1	2014-10-06	Lee et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	41	20150281964	A1	2015-10-01	Seo et al.	
	42	20070158439	A1	2007-07-12	Conner et al.	
	43	20130183932	A1	2013-07-18	Lemilainen et al.	
	44	20120033613	A1	2012-02-09	Lin et al.	
	45	20130028184	A1	2013-01-31	Lee et al.	
	46	20130182586	A1	2013-07-18	Paladugu et al.	
	47	20020018569	A1	2002-02-14	Panjwani et al.	
	48	20030003895	A1	2003-01-02	Wallentin et al.	
	49	20030211842	A1	2003-11-13	Kempf et al.	
	50	20040179684	A1	2004-09-16	Appenzeller et al.	
	51	20050008159	A1	2005-01-13	Grilli et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	52	20050021875	A1	2005-01-27	Bouthemy et al.	
	53	20050120202	A1	2005-06-02	Cuellar et al.	
	54	20050138353	A1	2005-06-23	Spies et al.	
	55	20050193199	A1	2005-09-01	Asokan et al.	
	56	20050246282	A1	2005-11-03	Naslund et al.	
	57	20050278787	A1	2005-12-15	Naslund et al.	
	58	20060021063	A1	2006-01-26	Hori	
	59	20060056355	A1	2006-03-16	Love et al.	
	60	20060059344	A1	2006-03-16	Mononen	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Cakulev et al., "An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange," August 2012, op. 1-32.	☐
	2	Gollmann, "Authentication - Myths and Misconceptions," Progress in Computer Science and Applied Logic, Vol. 20, 2001, pp. 203-225.	☐
	3	Tin et al., "Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach," Information Security Research Centre, Queensland University of Technology, Australia, 2003, pp. 166-179.	☐
	4	Hegland et al., "A Framework for Authentication in NBD Tactical Ad Hoc Networks," IEEE Communications Magazine, October 2011, pp. 64-71.	☐
	5	Nicholson et al., "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, Vol. 5, No.II, November 2006, pp.1489-1502.	☐
	6	Schwaiger et al., "Smart Card Security for Fieldbus Systems," 2003, pp. 398-406.	☐
	7	CSMG, Reprogrammable SIMs: Technology, Evolution and Implications, 25 SEP 2012, pp. 1-95.	☐
	8	GlobalPlatform Inc., GlobalPlatform Card Specification, Version 2.2.1, JAN 2011, pp. 1-303.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	9	GlobalPlatform Inc., GlobalPlatform Card Security Upgrade for Card Content Management, Card Specification v 2.2. - Amendment E, Version 1.0, NOV 2011, pp. 1-35.	☐
	10	GSM Association, Embedded SIM Task Force Requirements and Use Cases, Version 1.0, 21 FEB 2011, pp. 1-38.	☐
	11	Kirk H.M. Wong et al., A Dynamic User Authentication Scheme for Wireless Sensor Networks, Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 1-8.	☐
	12	Pierre E. ABI-CHAR, et al., A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications, The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007), pp. 1-6.	☐
	13	Jun Shao, et al., An Improved Deniable Authentication Protocol, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, People's Republic of China, pp. 1-3.	☐
	14	Chris Foresman, Embedded SIM could cause carrier conflict for Apple, November 19, 2010, pp. 1-2.	☐
	15	Embedded UICC Remote Provisioning Discussion, Source: Rogers Wireless, 3GPP/SA3-LI#46, Quebec City, Canada, July 17-19, 2012, p. 1-39.	☐
	16	GSMA LAUNCHES EMBEDDED SIM INITIATIVE TO SUPPORT THE CONNECTED FUTURE, November 18, 2010, p. 1-4.	☐
	17	Chang-Seop Park, On Certificate-Based Security Protocols for Wireless Mobile Communication Systems, Dankook University, IEEE Network September/October 1997, pp. 50-55.	☐
	18	M. Prasad, et al., Secure Authentication Key Agreement Protocol for Long Term Evolution - Advanced, Research Scholar, Associate Professor, Department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry, India, Elsevier, 2012, pp. 158-162.	☐
	19	Eun-Jun Yoon, et al., Secure Deniable Authentication Protocol Based on ElGamal Cryptography, 2008 International Conference on Information Security and Assurance, pp. 36-39.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	20	PIETRE-CAMBACEDES et al., Cryptographic key management for SCADA systems - issues and perspectives, 2008 International Conference on Information Security and Assurance, IEEE, pp. 156-161.	☐
	21	BENDER et al., Evolution of SIM provisioning towards a flexible MCIM provisioning in M2M vertical industries, 16th International Conference on Intelligence in Next Generation Networks, IEEE, 2012, pp. 57-64.	☐
	22	PARK et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 International Conference on Availability, Reliability and Security, IEEE, 2013, pp. 297-303.	☐
	23	Appenzeller et al., Identity-Based Encryption Architecture and Supporting Data Structures RFC 5408, 2009, pp. 1-30.	☐
	24	Baugher et al., Group Key Management Architecture, RFC Draft, 2001, pp. 1-20.	☐
	25	Ben Saied, Yosra; Olivereau, Alexis; Laurent, Maryline; "A Distributed Approach for Secure M2M Communications", 5th International Conference on New Technologies, Mobility and Security (NTMS), 7-10 May 2012, pgs. 1-7.	☐
	26	Boyen et al., Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles), 2006.	☐
	27	Boyen et al., Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BBI Cryptosystems, RFC 5091, 2007, pp. 1-63.	☐
	28	Harney et al., Group Key Management Protocol (GKMP) Architecture, 1994, pp. 1-19.	☐
	29	Kiltz et al., CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption, 2008.	☐
	30	Krylov, What is Kerberos Authtentication?, 2003, pp. 1-4.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	31	Martin, Introduction to Identity-Based Encryption, ISBN-13 978-1-59693-238-8, 2008.	☐
	32	Merrian-Webster, Network, 2014.	☐
	33	Park et al., A New Practical Identity-Based Encryption System, 2003, pp_ 1-27.	☐
	34	Park et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 IEEE, pp_ 297-303.	☐
	35	Shih, Jie-Ren; Hu, Yongbo; Hsiao, Ming-Chun; Chen, Ming-Shing; Shen, Wen-Chng; Yang, Bo-Yin; Wu, An-Yeu; Cheng, Chen-Mou; "Securing M2M with Post-Quantum Public-Key Cryptography", IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 7 March 2013, pgs_ 106-116.	☐
	36	Voltage Security, The Identity-Based Encryption Advantage, 2015.	☐
	37	Yang et al., Identity-Based Key Agreement and Encryption for Wireless Sensor Networks, IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No. 5B, May 2006, pp_ 182-189.	☐
	38	Youngblood, An Introduction to Identity-based Cryptography, 2005.	☐
	39	Zhu et al., Public Key Cryptography for Initial Authentication in Kerberos (PPKINIT), RFC 4556, 2006, pp_ 1-42.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DAO Q HO/	Date Considered	09/17/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140143826	A1	2014-05-22	Sharp et al.	
	2	20140161113	A1	2014-06-12	Cui et al.	
	3	20140165155	A1	2014-06-12	Zhang	
	4	20140192976	A1	2014-07-10	Yoon et al.	
	5	20140219447	A1	2014-08-07	Park et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	6	20140219448	A1	2014-08-07	Froels et al.	
	7	20140244994	A1	2014-08-28	Yu	
	8	20140273913	A1	2014-09-18	Michel et al.	
	9	20140287725	A1	2014-09-25	Lee	
	10	20140337937	A1	2014-11-13	Truskovsky et al.	
	11	20140351403	A1	2014-11-27	Lein et al.	
	12	20150012743	A1	2015-01-08	Holtmanns et al.	
	13	20150017910	A1	2015-01-15	Li et al.	
	14	20150071139	A1	2015-03-12	Nix	
	15	20150092590	A1	2015-04-02	Zhu et al.	
	16	20150095514	A1	2015-04-02	Yu	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	17	20150095648	A1	2015-04-02	Nix	
	18	20150113275	A1	2015-04-23	Kim et al.	
	19	20150121495	A1	2015-04-03	Gao et al.	
	20	20130231087	A1	2013-09-05	O'Leary	
	21	20130165073	A1	2013-06-27	Madsen	
	22	20130007442	A1	2013-01-03	Mao et aL	
	23	20120170451	A1	2012-07-05	Viswanathan et aL	
	24	20120084568	A1	2012-08-05	Sarikaya et al.	
	25	20120030461	A1	2012-02-02	Willey et al.	
	26	20080307218	A1	2008-12-11	Logvinov	
	27	20110035584	A1	2011-02-10	Meyerstein et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	28	20090060197	A1	2009-03-05	Taylor et al.	
	29	20150089214	A1	2015-03-26	Dupre	
	30	20140122878	A1	2014-05-01	Cho et al.	
	31	20140115335	A1	2014-04-24	Jorden et al.	
	32	20130173926	A1	2013-07-04	Morese et al.	
	33	20130012168	A1	2013-01-10	Rajadurai et al.	
	34	20120331298	A1	2012-12-27	Xu et al.	
	35	20120190354	A1	2012-07-26	Merrien et al.	
	36	20040221163	A1	2004-11-04	Jorgensen et al.	
	37	20090113203	A1	2009-04-30	Tsuge et al.	
	38	20150163056	A1	2015-06-11	Nix	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	39	20090217348	A1	2009-08-27	Salmela et al.	
	40	20080130879	A1	2008-06-05	Heinonen et al.	
	41	20130122864	A1	2013-05-16	Haggerty et al.	
	42	20150071139	A1	2015-03-12	Nix	
	43	20150095648	A1	2015-04-02	Nix	
	44	20150106616	A1	2015-04-16	Nix	
	45	20150121066	A1	2015-04-30	Nix	
	46	20150143125	A1	2015-05-21	Nix	
	47	20040162472	A1	2004-08-19	Berson et al.	
	48	20150215126	A1	2015-07-30	Ashdown	
	49	20160294829	A1	2016-10-06	Angus	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	50	20110269422	A1	2011-11-03	Xu et al.	
	51	20110269461	A1	2011-11-03	Xu et al.	
	52	20110269472	A1	2011-11-03	Xu et al.	
	53	20110270747	A1	2011-11-03	Xu et al.	
	54	20130294602	A1	2013-11-07	Huxham et al.	
	55	20130340040	A1	2013-12-19	Park et al.	
	56	20140308991	A1	2014-10-16	Lee et al.	
	57	20140329502	A1	2014-11-06	Lee et al.	
	58	20150281964	A1	2015-10-01	Seo et al.	
	59	20070158439	A1	2007-07-12	Conner et al.	
	60	20130183932	A1	2013-07-18	Lemilainen et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DAO Q HO/	Date Considered	09/17/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10169587	B1	2019-01-01	Nix	
	2	10621352	B2	2020-04-14	NIx	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060021063	A1	2006-01-26	Hori	
	2	20100093347	A1	2010-04-15	Hahn et al.	
	3	20110158411	A1	2011-06-30	Medvinsky et al.	
	4	20210126801	A1	2021-04-29	Nix	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	5	20200280436	A1	2020-09-03	Nix	
	6	20210218560	A1	2021-07-15	Nix	
	7	20210184842	A1	2021-06-17	Nix	
	8	20210194681	A1	2021-06-24	Nix	
	9	20190356482	A1	2019-11-21	Nix	
	10	20200226258	A1	2020-07-16	Nix	
	11	20190313246	A1	2019-10-10	Nix	
	12	20210211279	A1	2021-07-08	Nix	
	13	20200162269	A1	2020-05-21	Nix	
	14	20200162247	A1	2020-05-21	Nix	
	15	20190332774	A1	2019-10-31	Nix	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2518976	GB	A	2015-04-08	Vodafone IP Licensing Ltd		☐
	2	2021007235	WO	A1	2021-01-14	Nix		☐
	3	2021007235	WO	A1	2021-01-14	Nix		☐
	4	2021087221	WO	A1	2021-05-06	Nix		☐
	5	2020223319	WO	A1	2020-11-05	Nix		☐
	6	2020006162	WO	A1	2020-01-02	Nix		☐
	7	2019246206	WO	A1	2019-12-26	Nix		☐
	8	2019222319	WO	A1	2019-11-21	Nix		☐
	9	2019209598	WO	A1	2019-10-31	Nix		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	10	2019178312	WO	A1	2019-09-19	Nix		☐
	11	2020123959	WO	A1	2020-06-18	Nix		☐
	12	2020061023	WO	A1	2020-03-26	Nix		☐
	13	3110641	CA	A1	2019-10-31	Nix		☐
	14	3110468	CA	A1	2019-11-21	Nix		☐
	15	19803936	DE	A1	1999-08-05	Osram GmbH Siemens AG		☐
	16	3766222	EP	A1	2021-01-20	Nix		☐
	17	20130026351	KR	A	2013-03-13	SAMSUNG ELECTRONICS CO LTD	English Abstract	☒
	18	2013/048084	WO	A2	2013-04-04	SAMSUNG ELECTRONICS CO LTD	English Abstract	☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	1	Search Report issued in UK Application No. GB2108534.5 dated July 7, 2021.	☐
	2	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000)	☐
	3	TLS 1.3 Wish List Presentation, IETF 87 (Eric Rescorla), dated August 1, 2013.	☐
	4	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182424.8 dated October 12, 2021.	☐
	5	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182451.1 dated October 12, 2021.	☐
	6	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182432.1 dated October 12, 2021.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DAO Q HO/	Date Considered	09/17/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9807605	B2	2017-10-31	Gao et al.	
	2	8577337	B2	2013-11-05	O'Leary	
	3	9800993	B2	2013-11-05	Lee et al.	
	4	9794775	B2	2017-10-17	Huber et al.	
	5	9674690	B2	2017-06-06	Lee et al.	
	6	9628981	B2	2017-04-18	Park et al.	
	7	9572016	B2	2017-02-14	Cormier et al.	
	8	9332129	B2	2016-05-03	Li et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	9	9270653	B2	2016-02-23	Maria	
	10	6804357	B1	2004-10-12	Ikonen et al.	
	11	9923724	B2	2018-03-20	Lee et al.	
	12	6842628	B1	2005-01-11	Arnold et al.	
	13	8352739	B2	2013-01-08	Park et al.	
	14	6721886	B1	2004-04-13	Uskela	
	15	5995625	A	1999-11-30	Sudia et al.	
	16	5852665	A	1998-12-22	Gressel et al.	
	17	5664017	A	1997-09-02	Gressel et al.	
	18	5642420	A	1997-06-24	Kuroda et al.	
	19	5216715	A	1993-06-01	Markwitz	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	20	6256733	B1	2001-07-03	Thakkar et al.	
	21	9020479	B1	2015-04-28	Somayajula et al.	
	22	8965366	B1	2015-02-24	Somayajula et al.	
	23	8452017	B2	2013-05-28	Sherkin	
	24	7957532	B2	2011-06-07	Chen et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20110213959	A1	2011-09-01	Bodi et al.	
	2	20130344864	A1	2013-12-26	Park et al.	
	3	20140082359	A1	2014-03-20	Nakhjiri et al.	
	4	20140120874	A1	2014-05-01	Kang et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	5	20140329502	A1	2014-11-06	Lee et al.	
	6	20150350881	A1	2015-12-03	Weiss et al.	
	7	20130283047	A1	2013-10-24	Merrien et al.	
	8	20120263298	A1	2012-10-18	Suh et al.	
	9	20080044032	A1	2008-02-21	Lou et al.	
	10	20050058294	A1	2005-03-17	Chen et al.	
	11	20160088096	A1	2016-03-24	Quiriconi et al.	
	12	20120190354	A1	2012-07-23	Merrien et al.	
	13	20110035604	A1	2011-02-10	Habraken	
	14	20140237101	A1	2014-08-21	Park	
	15	20140235210	A1	2014-08-21	Park et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	16	20140219447	A1	2014-08-07	Park et al.	
	17	20140140507	A1	2014-05-22	Park et al.	
	18	20140082358	A1	2014-03-20	Nakhjiri et al.	
	19	20150281964	A1	2015-10-01	Seo et al.	
	20	20150121495	A1	2015-04-30	Gao et al.	
	21	20140308991	A1	2014-10-16	LEE et al.	
	22	20130340040	A1	2013-12-19	Park et al.	
	23	20130122864	A1	2013-05-16	Haggerty et al.	
	24	20110270747	A1	2011-11-03	Xu	
	25	20160057725	A1	2016-02-25	Suh	
	26	20160149903	A1	2016-05-26	Suh	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

	27	20130157673	A1	2013-06-20	Brusilovsky	
	28	20110268022	A1	2011-11-03	Xu	
	29	20160127132	A1	2016-05-05	Lee et al.	
	30	20140357229	A1	2014-12-04	Lee et al.	
	31	20130227646	A1	2013-08-29	Haggerty et al.	
	32	20130012168	A1	2013-01-10	Rajadurai et al.	
	33	20130294602	A1	2013-11-07	Huxham et al.	
	34	20140003604	A1	2014-01-02	Campagna et al.	
	35	20110269461	A1	2011-11-03	Xu et al.	
	36	20110269472	A1	2011-11-03	Xu et al.	
	37	20110269422	A1	2011-11-03	Xu et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	38	20120011362	A1	2012-01-12	Lambert	
	39	20060129848	A1	2006-06-15	Paksoy et al.	
	40	20120087493	A1	2012-04-12	Chidambaram et al.	
	41	20080107083	A1	2008-05-08	Shirota et al.	
	42	20130165075	A1	2013-06-27	Rishy-Maharaj et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000)	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

EXAMINER SIGNATURE			
Examiner Signature	/DAO Q HO/	Date Considered	09/17/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
18/416,534	01/18/2024	John A. Nix	63121/0226

CONFIRMATION NO. 7559

1912
AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

PUBLICATION NOTICE



Date Mailed: 07/25/2024

Title: Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Publication No.US-2024-0250938-A1
Publication Date:07/25/2024

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be viewed using the USPTO's publicly available Searchable Databases via the Patent Public Search tool at www.uspto.gov. The direct link to access the Patent Public Search tool is currently https://ppubs.uspto.gov/pubwebapp/static/pages/ppubsbasic.html.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through Patent Center, the USPTO's electronic patent application filing and management system. The direct link to access this status information is currently https://patentcenter.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of Patent Center.

Further assistance in electronically accessing the publication, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Petitioner Samsung Ex-1004, 0233

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/416,534	01/18/2024	John A. Nix	63121/0226	7559

1912 7590 05/01/2024

AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

EXAMINER
CENTRAL, DOCKET

ART UNIT	PAPER NUMBER
OPAP	

MAIL DATE	DELIVERY MODE
05/01/2024	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Petitioner Samsung Ex-1004, 0234

Notice of Potential Erroneous Release of Patent Application Titles

On February 5, 2024, the United States Patent and Trademark Office (USPTO), replaced the Electronic Patent Assignment System (EPAS) and Electronic Trademark Assignment System (ETAS) with Assignment Center.

Between February 5, 2024 and March 29, 2024, the USPTO, unintentionally, through a computer programming error, permitted bibliographic information to be viewed by unauthorized individuals with access to registered Assignment Center accounts. This bibliographic information was limited to the application number (the two-digit series code plus the six-digit serial number) and title of the invention.

You are receiving this notification because your application's patent title may have been viewed during that time frame by individual(s) who lacked permission to do so. The software error was first reproduced by USPTO on March 28, 2024, and was corrected on March 29, 2024. Only application numbers and titles were disclosed; it is important to note that your specification and claims were not part of the information made available and were not accessed.

Any improper access of the application information between the dates of February 5, 2024 and March 29, 2024, is not considered a publication of such applications under 35 U.S.C. 122(b). No rights in United States patents are threatened by the access to unpublished applications. It is extremely unlikely that the title could disclose the invention in a way that would constitute patent-defeating prior art in any jurisdiction. To the extent any issue is raised, the USPTO will assist applicants by confirming that the disclosure was erroneous and inadvertent.

We're committed to data security and are taking enhanced steps to prevent incidents such as this from happening in the future. The USPTO sincerely regrets this error and is instituting more testing controls, both manual and automated testing, to prevent similar processing errors in the future.

Inquiries regarding this matter may be directed to Mark Polutta, Senior Legal Advisor, at (571) 272-7709 or Andrew Stclair, Legal Advisor, at (571) 270-0238, both of the Office of Patent Legal Administration or via email addressed to Patent.Practice@uspto.gov.



Henry "Jamie" Holcombe
Chief Information Officer
US Patent and Trademark Office
Office +1 (571) 272-9400

Dated: April 27th, 2024

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR/ PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
18/416,534	01/18/2024	Nix, John A.	63121/0226

	EXAMINER	
AMSTER, ROTHSTEIN & EBENSTEIN LLP 405 LEXINGTON AVENUE FLOOR 48 NEW YORK, NY 10174	--	
	ART UNIT	PAPER
	--	20240427-fJaor1

DATE MAILED: 27 April 2024

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

PTO-90C (Rev.04-03)

Notice of Potential Erroneous Release of Patent Application Titles

On February 5, 2024, the United States Patent and Trademark Office (USPTO), replaced the Electronic Patent Assignment System (EPAS) and Electronic Trademark Assignment System (ETAS) with Assignment Center.

Between February 5, 2024 and March 29, 2024, the USPTO, unintentionally, through a computer programming error, permitted bibliographic information to be viewed by unauthorized individuals with access to registered Assignment Center accounts. This bibliographic information was limited to the application number (the two-digit series code plus the six-digit serial number) and title of the invention.

You are receiving this notification because your application's patent title may have been viewed during that time frame by individual(s) who lacked permission to do so. The software error was first reproduced by USPTO on March 28, 2024, and was corrected on March 29, 2024. Only application numbers and titles were disclosed; it is important to note that your specification and claims were not part of the information made available and were not accessed.

Any improper access of the application information between the dates of February 5, 2024 and March 29, 2024, is not considered a publication of such applications under 35 U.S.C. 122(b). No rights in United States patents are threatened by the access to unpublished applications. It is extremely unlikely that the title could disclose the invention in a way that would constitute patent-defeating prior art in any jurisdiction. To the extent any issue is raised, the USPTO will assist applicants by confirming that the disclosure was erroneous and inadvertent.

We're committed to data security and are taking enhanced steps to prevent incidents such as this from happening in the future. The USPTO sincerely regrets this error and is instituting more testing controls, both manual and automated testing, to prevent similar processing errors in the future.

Inquiries regarding this matter may be directed to Mark Polutta, Senior Legal Advisor, at (571) 272-7709 or Andrew Stclair, Legal Advisor, at (571) 270-0238, both of the Office of Patent Legal Administration or via email addressed to Patent.Practice@uspto.gov.



Henry "Jamie" Holcombe
Chief Information Officer
US Patent and Trademark Office
Office +1 (571) 272-9400

Dated: April 27th, 2024

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	**04/09/2024 05:23:57 PM Z ET**	**63121/0226**

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	65027573	FILING DATE	01/18/2024
CUSTOMER #	1912	FIRST NAMED INVENTOR	John A. Nix
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Keith Barkaus

Documents

TOTAL DOCUMENTS: 9

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
1-Transmittal Letter.pdf	4	Transmittal Letter	131 KB
2-IDS1.pdf	15	Information Disclosure Statement (IDS) Form (SB08)	1015 KB
3-IDS2.pdf	9	Information Disclosure Statement (IDS) Form (SB08)	1012 KB
4-IDS3.pdf	9	Information Disclosure Statement (IDS) Form (SB08)	1012 KB
5-IDS4.pdf	9	Information Disclosure Statement (IDS) Form (SB08)	985 KB

6-IDS5.pdf	9	Information Disclosure Statement (IDS) Form (SB08)	985 KB
7-IDS6.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	986 KB
8-IDS7.pdf	10	Information Disclosure Statement (IDS) Form (SB08)	1012 KB
9-IDS8.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1012 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
1-Transmittal Letter.pdf	FD616C871B1D7C8D8728153CCB3002C6CBF8C3C1EA1196A9E287703627D1A367D96B29B23627374F15277EBBAC593EDD476A2473754BD821BA5F3739B50804C5
2-IDS1.pdf	331590615F9C14DED03D3341E1EFAFFC0F35C0FEBA8096BBC907E58ED1A4594151E2350E8AD51FB39BD8F29BB8B4205B1DF61C77B5FB15C2AB3690D0223CDAFD
3-IDS2.pdf	4A05DB8213AA751E0E57987F6EBD53854231D5CABB007D49E5E67A31B8386A0A952978360A6D04145EFD69EB27F355C8A97F499BAA2FD8E908CF5150CA76F3C9
4-IDS3.pdf	D376A5589F1215CD410C74E21CC3BE88A96C5796E9443EB6665DFABEAB4AF0938CAC5D8384FE21312F0B0619230D7F2F880C7CBD1AC4B9756BCF146014FAAF46
5-IDS4.pdf	6D88EE1C2BE0CF3CC62C940A459683489618E894835436721E8EB4901233F8775F051ECB1D89179E1512FE1DA9F0FE77B96E958EB6D0E2247DE9B218764A8912
6-IDS5.pdf	411837068DADBC910BF3D6C5F287693DD359420D41442ADAD051DB24BEEF4F1C5052E407767B4BDA2DEC7AD7A874C0250

	48FC96857E0B5C18DA3898A8C6376D7
7-IDS6.pdf	0725518556E26192C079D017AAD6D65784AB005CBE73C60F57A41D79D3CB8B9EBE2B43714F011FFE7F23982D00AB615851D8F25E5DCCF05A52DC9EF56924F5EF
8-IDS7.pdf	0DABCB3600A8485A357EF80A84C7D6317DAB3E42910759EDABA8932F17E012545FD59FCAA3C713BF159EFB8C749936C66164B121BA8650C334296E1F4884F844
9-IDS8.pdf	97AB836C6C9BA0692C7F637A033771203B3A34B9F1D3FC7F556DF7FECBE225215B88602AC1FBC87B7047938FD350044405C2FCB40BECD11571AF117CFAFD3183

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140143826	A1	2014-05-22	Sharp et al.	
	2	20140161113	A1	2014-06-12	Cui et al.	
	3	20140165155	A1	2014-06-12	Zhang	
	4	20140192976	A1	2014-07-10	Yoon et al.	
	5	20140219447	A1	2014-08-07	Park et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	6	20140219448	A1	2014-08-07	Froels et al.	
	7	20140244994	A1	2014-08-28	Yu	
	8	20140273913	A1	2014-09-18	Michel et al.	
	9	20140287725	A1	2014-09-25	Lee	
	10	20140337937	A1	2014-11-13	Truskovsky et al.	
	11	20140351403	A1	2014-11-27	Lein et al.	
	12	20150012743	A1	2015-01-08	Holtmanns et al.	
	13	20150017910	A1	2015-01-15	Li et al.	
	14	20150071139	A1	2015-03-12	Nix	
	15	20150092590	A1	2015-04-02	Zhu et al.	
	16	20150095514	A1	2015-04-02	Yu	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	17	20150095648	A1	2015-04-02	Nix	
	18	20150113275	A1	2015-04-23	Kim et al.	
	19	20150121495	A1	2015-04-03	Gao et al.	
	20	20130231087	A1	2013-09-05	O'Leary	
	21	20130165073	A1	2013-06-27	Madsen	
	22	20130007442	A1	2013-01-03	Mao et aL	
	23	20120170451	A1	2012-07-05	Viswanathan et aL	
	24	20120084568	A1	2012-08-05	Sarikaya et al.	
	25	20120030461	A1	2012-02-02	Willey et al.	
	26	20080307218	A1	2008-12-11	Logvinov	
	27	20110035584	A1	2011-02-10	Meyerstein et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	28	20090060197	A1	2009-03-05	Taylor et al.	
	29	20150089214	A1	2015-03-26	Dupre	
	30	20140122878	A1	2014-05-01	Cho et al.	
	31	20140115335	A1	2014-04-24	Jorden et al.	
	32	20130173926	A1	2013-07-04	Morese et al.	
	33	20130012168	A1	2013-01-10	Rajadurai et al.	
	34	20120331298	A1	2012-12-27	Xu et al.	
	35	20120190354	A1	2012-07-26	Merrien et al.	
	36	20040221163	A1	2004-11-04	Jorgensen et al.	
	37	20090113203	A1	2009-04-30	Tsuge et al.	
	38	20150163056	A1	2015-06-11	Nix	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	39	20090217348	A1	2009-08-27	Salmela et al.	
	40	20080130879	A1	2008-06-05	Heinonen et al.	
	41	20130122864	A1	2013-05-16	Haggerty et al.	
	42	20150071139	A1	2015-03-12	Nix	
	43	20150095648	A1	2015-04-02	Nix	
	44	20150106616	A1	2015-04-16	Nix	
	45	20150121066	A1	2015-04-30	Nix	
	46	20150143125	A1	2015-05-21	Nix	
	47	20040162472	A1	2004-08-19	Berson et al.	
	48	20150215126	A1	2015-07-30	Ashdown	
	49	20160294829	A1	2016-10-06	Angus	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	50	20110269422	A1	2011-11-03	Xu et al.	
	51	20110269461	A1	2011-11-03	Xu et al.	
	52	20110269472	A1	2011-11-03	Xu et al.	
	53	20110270747	A1	2011-11-03	Xu et al.	
	54	20130294602	A1	2013-11-07	Huxham et al.	
	55	20130340040	A1	2013-12-19	Park et al.	
	56	20140308991	A1	2014-10-16	Lee et al.	
	57	20140329502	A1	2014-11-06	Lee et al.	
	58	20150281964	A1	2015-10-01	Seo et al.	
	59	20070158439	A1	2007-07-12	Conner et al.	
	60	20130183932	A1	2013-07-18	Lemilainen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Network-1 Technologies, Inc.	Confirmation No.: 7559
Title:	EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION	
Appl. No.:	18/416,534	
Filing Date:	January 18, 2024	
Examiner:	TBD	
Art Unit:	TBD	
Docket No.:	63121/0226	
Customer No.:	01912	

INFORMATION DISCLOSURE STATEMENT LETTER
UNDER 37 CFR § 1.56

Via Patent Center
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure under 37 C.F.R. §1.56, Applicant would like to direct the Examiner's attention to the references that are listed on the attached forms PTO/SB/08A. In addition to any copies of Foreign Patent Documents and Non-Patent Literature Documents submitted herewith, Applicant refers the Examiner to the references previously submitted to or cited by the Patent Office during prosecution of U.S. Patent Application No. 17/547,990, filed December 10, 2021, now U.S. Patent No. 11,916,893, U.S. Patent Application No. 16/453,682 filed June 26, 2019, now U.S. Patent No. 11,233,780, U.S. Patent Application No. 16/110,804, filed August 23, 2018, U.S. Patent Application No. 15/928,848 filed March 22, 2018, now U.S. Patent No. 10,084,768, U.S. Patent Application No. 14/751,119 filed June 25, 2015, now U.S. Patent No. 9,961,060 and U.S. Patent Application No. 14/099,329 filed December 6, 2013, now U.S. Patent No. 9,100,175, from which the subject application claims priority under 35 U.S.C. §120. Accordingly, pursuant to 37 C.F.R. § 1.98(d), copies of

Petitioner Samsung Ex-1004, 0250

previously cited or submitted references and Non-Patent Literature Documents are not included with this Information Disclosure Statement.

Reference to Related Patents and Co-Pending Applications

The below chart provides information regarding related issued patents and co-pending applications filed by the present Applicant:

Serial No.	Attorney Docket No.	Filing Date	Status
18/435,042	63121/0230	2024-02-07	Pending – Ready for Examination
18/587,462	63121/0229	2024-02-26	Pending – Ready for Examination
18/433,683	63121/0228	2024-02-06	Pending – Ready for Examination
18/438,147	63121/0227	2024-02-09	Pending – Undergoing Preexam Processing
18/416,534	**63121/0226**	**204-01-18**	**Present Application**
18/433,664	63121/0225	2024-02-06	Pending – Ready for Examination
18/229,907	63121/0224	2023-08-03	Pending – Response to Final OA Filed 2024-03-28
18/111,669	63121/0222	2023-02-20	Non-Final OA mailed 2023-10-02
17/647,812	63121/0213	2022-01-13	USP 11,606,204
17/547,990	63121/0212	2021-12-10	USP 11,736,283
17/304,922	63121/0209	2021-06-28	USP 11,736,283
17/249,242	63121/0202	2021-02-24	Response to Non-Final OA filed 2023-11-13
16/879,325	63121/0198	2020-05-20	USP 11,082,218
16/843,107	63121/0197	2020-04-08	USP 11,283,603
16/721,153	63121/0195	2019-12-19	USP 11,539,681
16/593,561	63121/0190	2019-10-04	USP 11,258,595
16/453,682	63121/0184	2019-06-26	USP 11,233,780
16/271,455	63121/0181	2019-02-08	USP 10,594,679
16/271,428	63121/0180	2019-02-08	USP 10,523,432
16/201,401	63121/0179	2018-11-27	USP 10,700,856
16/200,118	63121/0178	2018-11-26	USP 10,498,530
16/110,804	63121/0168	2018-08-23	USP 10,382,422
16/036,506	63121/0167	2018-07-16	USP 10,530,575
15/983,957	63121/0163	2018-05-18	USP 10,177,911
15/973,012	63121/0162	2018-05-07	USP 10,250,386

Petitioner Samsung Ex-1004, 0251

15/972,914	63121/0161	2018-05-07	USP 10,652,017
15/928,848	63121/0160	2018-03-22	USP 10,084,768
15/010,905	63121/0157	2016-01-29	USP 9,641,327
15/680,758	63121/0147	2017-08-18	USP 10,187,206
15/162,292	63121/0146	2016-05-23	USP 10,362,012
14/751,119	63121/0145	2015-06-25	USP 9,961,060
15/457,700	63121/0144	2017-03-13	USP 9,998,281
15/583,968	63121/0143	2017-05-01	USP 10,057,059
15/043,293	63121/0142	2016-02-12	USP 9,998,280
15/642,088	63121/0141	2017-07-05	USP 10,003,461
15/130,146	63121/0140	2016-04-15	USP 9,742,562
15/162,302	63121/0139	2016-05-23	USP 9,698,981
14/789,255	63121/0138	2015-07-01	USP 9,596,078
14/139,419	63121/0137	2013-12-23	USP 9,351,162
14/136,711	63121/0136	2013-12-20	USP 9,300,473
14/099,329	63121/0135	2013-12-06	USP 9,100,175
14/084,141	63121/0134	2013-11-19	USP 9,319,223
14/064,618	63121/0133	2013-10-28	USP 9,118,464
14/055,606	63121/0132	2013-10-16	USP 9,276,740
14/039,401	63121/0131	2013-09-27	USP 9,288,059
14/023,181	63121/0130	2013-09-10	USP 9,350,550
AU 2019246774	63121-0199	2019-10-08	AU2019246774A1 Issued 2021-09-23
GB 1608573	63121-0151	2014-10-27	Published on 2016-08-03
GB 2100530	63121-0201	2014-10-27	Published on 2021-05-12
CA 2,965,119	63121-0152	2014-10-27	Published on 2015-05-07
HK 17101082.8	63121-0153	2014-10-27	Published on 2017-10-20
EU 14868381.6	63121-0154	2014-12-04	Published on 2017-01-04
CA 2,969,829	63121-0155	2014-12-04	Published on 2015-06-11
HK 17106540.3	63121-0156	2014-12-04	Published on 2018-01-19

Petitioner Samsung Ex-1004, 0252

The Examiner is invited to review the prosecution history of each of these applications, including the cited references of record and related office actions, as the Examiner deems appropriate.

* * * * *

This Information Disclosure Statement is being filed within three months of the filing date and before the mailing date of a first Office Action on the merits in the present application. No certification or fee is required. Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered. Please charge any fee deficiency or credit any overpayment to Deposit Account No. 01-1785, under Docket No. 63121/0226.

Respectfully submitted,

AMSTER, ROTHSTEIN & EBENSTEIN LLP
Attorneys for Applicant
405 Lexington Avenue
New York, NY 10174
(212) 336-8000

Dated: April 9, 2024

By: /Keith J. Barkaus/
Keith J. Barkaus
Reg. No. 51,431

Petitioner Samsung Ex-1004, 0253

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060206710	A1	2006-09-14	Gehrmann	
	2	20060281442	A1	2006-12-14	Lee et al.	
	3	20070206799	A1	2007-09-06	Wingert et al.	
	4	20080016230	A1	2008-01-17	Hollmanns et al.	
	5	20080022089	A1	2008-01-24	Leedom	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	6	20080114978	A1	2008-05-15	Lehtoviorta et al.	
	7	20080165698	A1	2008-07-10	Dalsgard et al.	
	8	20090116642	A1	2009-05-07	Yang et al.	
	9	20090028341	A1	2009-01-29	Hamachi	
	10	20090077643	A1	2009-03-19	Schmidt et al.	
	11	20090125996	A1	2009-05-14	Guccione et al.	
	12	20090132806	A1	2009-05-21	Blommaert et al.	
	13	20090191857	A1	2009-07-30	Horn et al.	
	14	20090209232	A1	2009-08-20	Cha et al.	
	15	20090268909	A1	2009-10-29	Girao et al.	
	16	20090282246	A1	2009-11-12	Gunther	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	17	20090313472	A1	2009-12-17	Guccione et al.	
	18	20100166167	A1	2010-07-01	Karimi-Cherkandi et al.	
	19	20100031042	A1	2010-02-04	Di Crescenzo et al.	
	20	20100062808	A1	2010-03-11	Cha et al.	
	21	20100098253	A1	2010-04-22	Delerablee	
	22	20100275028	A1	2010-10-28	Takashima	
	23	20110016321	A1	2011-01-20	Sundaram et al.	
	24	20110055553	A1	2011-03-03	Lee et al.	
	25	20110237281	A1	2011-09-20	Busropan et al.	
	26	20110291803	A1	2011-12-01	Bajic et al.	
	27	20110314287	A1	2011-12-22	Escott et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	28	20120011360	A1	2012-01-12	Engels et al.	
	29	20120023336	A1	2012-01-26	Natarajan	
	30	20120072732	A1	2012-03-22	Canard et al.	
	31	20120089568	A1	2012-04-12	Manley et al.	
	32	20120108205	A1	2012-05-03	Schell et al.	
	33	20120117635	A1	2012-05-10	Schell et al.	
	34	20120159153	A1	2012-06-21	Shim et al.	
	35	20120260086	A1	2012-10-11	Haggerty et al.	
	36	20120260090	A1	2012-10-11	Hauck et al.	
	37	20120260095	A1	2012-10-11	Von Hauck et al.	
	38	20120278490	A1	2012-11-01	Sennett et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	39	20120300932	A1	2012-11-29	Cambridge et al.	
	40	20120331292	A1	2012-12-27	Haggerty et al.	
	41	20130091556	A1	2013-04-11	Horn et al.	
	42	20130114810	A1	2013-05-09	Kobayashi et al.	
	43	20130117824	A1	2013-05-09	Naslund et al.	
	44	20130149996	A1	2013-06-13	King et al.	
	45	20130166915	A1	2013-06-27	desai et al.	
	46	20130173747	A1	2013-07-04	Kim et al.	
	47	20130212637	A1	2013-08-15	Guccione et al.	
	48	20130227646	A1	2013-08-29	Haggerty et al.	
	49	20130305345	A1	2013-11-14	Bugenhagen	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	50	20130322621	A1	2013-12-05	Yoon et al.	
	51	20130331063	A1	2013-12-12	Cormier et al.	
	52	20140003604	A1	2014-01-02	Campagna et al.	
	53	20140053241	A1	2014-02-20	Norman et al.	
	54	20140073375	A1	2014-03-13	Li et al.	
	55	20140082358	A1	2014-03-20	Nakhjiri et al.	
	56	20140082359	A1	2014-03-20	Nakhjiri et al.	
	57	20140087790	A1	2014-03-27	Babbage et al.	
	58	20140101444	A1	2014-04-10	Lee et al.	
	59	20140108801	A1	2014-04-17	McBride et al.	
	60	20140140507	A1	2014-05-22	Park et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
	2					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20130149996	A1	2013-06-13	King et al.	
	2	20130166915	A1	2013-06-27	Desai et al.	
	3	20130173747	A1	2013-07-04	Kim et al.	
	4	20130212637	A1	2013-08-15	Guccione et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	5	20130227646	A1	2013-08-29	Haggerty et al.	
	6	20130305345	A1	2013-11-14	Bugenhagen	
	7	20130322621	A1	2013-12-05	Yoon et al.	
	8	20130331063	A1	2013-12-12	Cormier et al.	
	9	20140003604	A1	2014-01-02	Campagna et al.	
	10	20140053241	A1	2014-02-20	Norman et al.	
	11	20140073375	A1	2014-03-13	Li et al.	
	12	20140082538	A1	2014-03-20	Nakhjiri et al.	
	13	20140082539	A1	2014-03-20	Nakhjiri et al.	
	14	20140087790	A1	2014-03-27	Babbage et al.	
	15	20140101444	A1	2014-04-10	Lee et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	16	20140108801	A1	2014-04-17	McBride et al.	
	17	20140140507	A1	2014-05-22	Park et al.	
	18	20140143826	A1	2014-05-22	Sharp et al.	
	19	20140161113	A1	2014-06-12	Cui et al.	
	20	20140165155	A1	2014-06-12	Zhang	
	21	20140192976	A1	2014-07-10	Yoon et al.	
	22	20140219447	A1	2014-08-07	Park et al.	
	23	20140219448	A1	2014-08-07	Froels et al.	
	24	20140244994	A1	2014-08-28	Yu	
	25	20140273913	A1	2014-09-18	Michel et al.	
	26	20140287725	A1	2014-09-25	Lee	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	27	20140337937	A1	2014-11-13	Truskovsky et al.	
	28	20140351403	A1	2014-11-27	Lin et al.	
	29	20150012743	A1	2015-01-08	Holtmanns et al.	
	30	20150017910	A1	2015-01-15	Li et al.	
	31	20150071139	A1	2015-03-12	Nix	
	32	20150092590	A1	2015-04-02	Zhu et al.	
	33	20150095514	A1	2015-04-02	Yu	
	34	20150095648	A1	2015-04-02	Nix	
	35	20150113275	A1	2015-04-23	Kim et al.	
	36	20150121495	A1	2015-04-30	Gao et al.	
	37	20130231087	A1	2013-09-05	O'Leary	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	38	20130165073	A1	2013-06-27	Madsen	
	39	20130007442	A1	2013-01-03	Yinian Mao et al.	
	40	20120170451	A1	2012-07-05	Harish Viswanathan et al.	
	41	20120084568	A1	2012-04-05	Bellcet Sarikaya et al.	
	42	20120030461	A1	2012-02-02	William Daniel Willey et al.	
	43	20080307218	A1	2008-12-11	Oleg Logvinov	
	44	20110035584	A1	2011-02-10	Meyerstein et al.	
	45	20090060197	A1	2009-03-05	Taylor et al.	
	46	20150089214	A1	2015-03-26	Dupre	
	47	20140122878	A1	2014-05-01	Cho et al.	
	48	20140115335	A1	2014-04-24	Jorden et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	49	20130173926	A1	2013-07-04	Morese et al.	
	50	20130012168	A1	2013-01-10	Rajadurai et al.	
	51	20120331298	A1	2012-12-27	Xu et al.	
	52	20120190354	A1	2012-07-26	Merrien et al.	
	53	20040221163	A1	2004-11-04	Jorgensen et al.	
	54	20090113203	A1	2009-04-30	Tsuge et al.	
	55	20150163056	A1	2015-06-11	Nix	
	56	20090217348	A1	2009-08-27	Salmela et al.	
	57	20080130879	A1	2008-06-05	Heinonen et al.	
	58	20130122864	A1	2013-05-16	Haggerty et al.	
	59	20150071139	A1	2015-03-12	Nix	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	60	20150095648	A1	2015-04-02	Nix	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9807605	B2	2017-10-31	Gao et al.	
	2	8577337	B2	2013-11-05	O'Leary	
	3	9800993	B2	2013-11-05	Lee et al.	
	4	9794775	B2	2017-10-17	Huber et al.	
	5	9674690	B2	2017-06-06	Lee et al.	
	6	9628981	B2	2017-04-18	Park et al.	
	7	9572016	B2	2017-02-14	Cormier et al.	
	8	9332129	B2	2016-05-03	Li et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	9	9270653	B2	2016-02-23	Maria	
	10	6804357	B1	2004-10-12	Ikonen et al.	
	11	9923724	B2	2018-03-20	Lee et al.	
	12	6842628	B1	2005-01-11	Arnold et al.	
	13	8352739	B2	2013-01-08	Park et al.	
	14	6721886	B1	2004-04-13	Uskela	
	15	5995625	A	1999-11-30	Sudia et al.	
	16	5852665	A	1998-12-22	Gressel et al.	
	17	5664017	A	1997-09-02	Gressel et al.	
	18	5642420	A	1997-06-24	Kuroda et al.	
	19	5216715	A	1993-06-01	Markwitz	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	20	6256733	B1	2001-07-03	Thakkar et al.	
	21	9020479	B1	2015-04-28	Somayajula et al.	
	22	8965366	B1	2015-02-24	Somayajula et al.	
	23	8452017	B2	2013-05-28	Sherkin	
	24	7957532	B2	2011-06-07	Chen et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20110213959	A1	2011-09-01	Bodi et al.	
	2	20130344864	A1	2013-12-26	Park et al.	
	3	20140082359	A1	2014-03-20	Nakhjiri et al.	
	4	20140120874	A1	2014-05-01	Kang et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	5	20140329502	A1	2014-11-06	Lee et al.	
	6	20150350881	A1	2015-12-03	Weiss et al.	
	7	20130283047	A1	2013-10-24	Merrien et al.	
	8	20120263298	A1	2012-10-18	Suh et al.	
	9	20080044032	A1	2008-02-21	Lou et al.	
	10	20050058294	A1	2005-03-17	Chen et al.	
	11	20160088096	A1	2016-03-24	Quiriconi et al.	
	12	20120190354	A1	2012-07-23	Merrien et al.	
	13	20110035604	A1	2011-02-10	Habraken	
	14	20140237101	A1	2014-08-21	Park	
	15	20140235210	A1	2014-08-21	Park et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	16	20140219447	A1	2014-08-07	Park et al.	
	17	20140140507	A1	2014-05-22	Park et al.	
	18	20140082358	A1	2014-03-20	Nakhjiri et al.	
	19	20150281964	A1	2015-10-01	Seo et al.	
	20	20150121495	A1	2015-04-30	Gao et al.	
	21	20140308991	A1	2014-10-16	LEE et al.	
	22	20130340040	A1	2013-12-19	Park et al.	
	23	20130122864	A1	2013-05-16	Haggerty et al.	
	24	20110270747	A1	2011-11-03	Xu	
	25	20160057725	A1	2016-02-25	Suh	
	26	20160149903	A1	2016-05-26	Suh	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	27	20130157673	A1	2013-06-20	Brusilovsky	
	28	20110268022	A1	2011-11-03	Xu	
	29	20160127132	A1	2016-05-05	Lee et al.	
	30	20140357229	A1	2014-12-04	Lee et al.	
	31	20130227646	A1	2013-08-29	Haggerty et al.	
	32	20130012168	A1	2013-01-10	Rajadurai et al.	
	33	20130294602	A1	2013-11-07	Huxham et al.	
	34	20140003604	A1	2014-01-02	Campagna et al.	
	35	20110269461	A1	2011-11-03	Xu et al.	
	36	20110269472	A1	2011-11-03	Xu et al.	
	37	20110269422	A1	2011-11-03	Xu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	38	20120011362	A1	2012-01-12	Lambert	
	39	20060129848	A1	2006-06-15	Paksoy et al.	
	40	20120087493	A1	2012-04-12	Chidambaram et al.	
	41	20080107083	A1	2008-05-08	Shirota et al.	
	42	20130165075	A1	2013-06-27	Rishy-Maharaj et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000)	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8127142	B2	2012-02-28	Cuppett	
	2	8522013	B2	2013-08-27	Zhang et al.	
	3	8843179	B2	2014-09-23	Li et al.	
	4	9408012	B2	2016-08-02	Li et al.	
	5	8924715	B2	2014-12-30	Schell et al.	
	6	9698981	B2	2017-07-04	Nix	
	7	9596078	B2	2017-03-14	Nix	
	8	8434139	B1	2013-04-30	Ortiz, Jr.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	9	8965366	B1	2015-02-24	Somayajula et al.	
	10	9020479	B1	2015-04-28	Somayajula et al.	
	11	9253643	B2	2016-02-02	Pattar et al.	
	12	6038322		2000-03-14	Harkins	
	13	7921292	B1	2011-04-05	Pauker et al.	
	14	8526606	B2	2013-09-03	Muthaiah	
	15	8555067	B2	2013-10-08	Schell et al.	
	16	8590028	B2	2013-11-19	Saxena et al.	
	17	8782774	B1	2014-07-15	Pahl et al.	
	18	8948386	B2	2015-02-03	Campagna et al.	
	19	9002018	B2	2015-04-07	Wilkins et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	20	9253643	B2	2016-02-02	Pattar et al.	
	21	8434139	B1	2013-04-30	Ortiz, Jr.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140281483	A1	2014-09-18	Vigliaturo et al.	
	2	20130179962	A1	2013-07-11	Arial et al.	
	3	20080031204	A1	2008-02-07	Sood	
	4	20090041110	A1	2009-02-12	Malladi	
	5	20090282246	A1	2009-11-12	Gunther	
	6	20090274306	A1	2009-11-05	Nolte	
	7	20140140509	A1	2014-05-22	Chastain et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	8	20140143534	A1	2014-05-22	Chastain et al.	
	9	20140237101	A1	2014-08-21	Park	
	10	20140235210	A1	2014-08-21	Park et al.	
	11	20060095771	A1	2006-05-04	Appenzeller et al.	
	12	20100223461	A1	2010-09-02	Drader et al.	
	13	20100199334	A1	2010-08-05	Ehrensvard et al.	
	14	20140040628	A1	2014-02-06	Fort et al.	
	15	20070101400	A1	2007-05-03	Freeman et al.	
	16	20160014112	A1	2016-01-14	Gunning et al.	
	17	20150222619	A1	2015-08-06	Hughes et al.	
	18	20010029581	A1	2001-10-11	Knauft	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	19	20140049653	A1	2014-02-20	Leonard et al.	
	20	20120214444	A1	2012-08-23	McBride et al.	
	21	20050050323	A1	2005-03-03	Mizrah	
	22	20090183541	A1	2009-07-23	Sadighi et al.	
	23	20100195833	A1	2010-08-05	Priestley et al.	
	24	20150222604	A1	2015-08-06	Ylonen	
	25	20110268022	A1	2011-11-03	Xu	
	26	20140357229	A1	2014-12-04	Lee et al.	
	27	20110167272	A1	2011-07-07	Kolesnikov	
	28	20160127132	A1	2016-05-05	Lee et al.	
	29	20170206532	A1	2017-07-20	Choi	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	30	20160294829	A1	2016-10-06	Angus	
	31	20150215126	A1	2015-07-30	Ashdown	
	32	20040162472	A1	2004-08-19	Berson et al.	
	33	20110269422	A1	2011-11-03	Xu et al.	
	34	20110269461	A1	2011-11-03	Xu et al.	
	35	20110269472	A1	2011-11-03	Xu et al.	
	36	20110270747	A1	2011-11-03	Xu	
	37	20130294602	A1	2013-11-07	Huxham et al.	
	38	20130340040	A1	2013-12-19	Park et al.	
	39	20140308991	A1	2014-10-16	Lee et al.	
	40	20140329502	A1	2014-10-06	Lee et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	41	20150281964	A1	2015-10-01	Seo et al.	
	42	20070158439	A1	2007-07-12	Conner et al.	
	43	20130183932	A1	2013-07-18	Lemilainen et al.	
	44	20120033613	A1	2012-02-09	Lin et al.	
	45	20130028184	A1	2013-01-31	Lee et al.	
	46	20130182586	A1	2013-07-18	Paladugu et al.	
	47	20020018569	A1	2002-02-14	Panjwani et al.	
	48	20030003895	A1	2003-01-02	Wallentin et al.	
	49	20030211842	A1	2003-11-13	Kempf et al.	
	50	20040179684	A1	2004-09-16	Appenzeller et al.	
	51	20050008159	A1	2005-01-13	Grilli et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	52	20050021875	A1	2005-01-27	Bouthemy et al.	
	53	20050120202	A1	2005-06-02	Cuellar et al.	
	54	20050138353	A1	2005-06-23	Spies et al.	
	55	20050193199	A1	2005-09-01	Asokan et al.	
	56	20050246282	A1	2005-11-03	Naslund et al.	
	57	20050278787	A1	2005-12-15	Naslund et al.	
	58	20060021063	A1	2006-01-26	Hori	
	59	20060056355	A1	2006-03-16	Love et al.	
	60	20060059344	A1	2006-03-16	Mononen	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Cakulev et al., "An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange," August 2012, op. 1-32.	☐
	2	Gollmann, "Authentication - Myths and Misconceptions," Progress in Computer Science and Applied Logic, Vol. 20, 2001, pp. 203-225.	☐
	3	Tin et al., "Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach," Information Security Research Centre, Queensland University of Technology, Australia, 2003, pp. 166-179.	☐
	4	Hegland et al., "A Framework for Authentication in NBD Tactical Ad Hoc Networks," IEEE Communications Magazine, October 2011, pp. 64-71.	☐
	5	Nicholson et al., "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, Vol. 5, No.II, November 2006, pp.1489-1502.	☐
	6	Schwaiger et al., "Smart Card Security for Fieldbus Systems," 2003, pp. 398-406.	☐
	7	CSMG, Reprogrammable SIMs: Technology, Evolution and Implications, 25 SEP 2012, pp. 1-95.	☐
	8	GlobalPlatform Inc., GlobalPlatform Card Specification, Version 2.2.1, JAN 2011, pp. 1-303.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	9	GlobalPlatform Inc., GlobalPlatform Card Security Upgrade for Card Content Management, Card Specification v 2.2. - Amendment E, Version 1.0, NOV 2011, pp. 1-35.	☐
	10	GSM Association, Embedded SIM Task Force Requirements and Use Cases, Version 1.0, 21 FEB 2011, pp. 1-38.	☐
	11	Kirk H.M. Wong et al., A Dynamic User Authentication Scheme for Wireless Sensor Networks, Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 1-8.	☐
	12	Pierre E. ABI-CHAR, et al., A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications, The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007), pp. 1-6.	☐
	13	Jun Shao, et al., An Improved Deniable Authentication Protocol, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, People's Republic of China, pp. 1-3.	☐
	14	Chris Foresman, Embedded SIM could cause carrier conflict for Apple, November 19, 2010, pp. 1-2.	☐
	15	Embedded UICC Remote Provisioning Discussion, Source: Rogers Wireless, 3GPP/SA3-LI#46, Quebec City, Canada, July 17-19, 2012, p. 1-39.	☐
	16	GSMA LAUNCHES EMBEDDED SIM INITIATIVE TO SUPPORT THE CONNECTED FUTURE, November 18, 2010, p. 1-4.	☐
	17	Chang-Seop Park, On Certificate-Based Security Protocols for Wireless Mobile Communication Systems, Dankook University, IEEE Network September/October 1997, pp. 50-55.	☐
	18	M. Prasad, et al., Secure Authentication Key Agreement Protocol for Long Term Evolution - Advanced, Research Scholar, Associate Professor, Department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry, India, Elsevier, 2012, pp. 158-162.	☐
	19	Eun-Jun Yoon, et al., Secure Deniable Authentication Protocol Based on ElGamal Cryptography, 2008 International Conference on Information Security and Assurance, pp. 36-39.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	20	PIETRE-CAMBACEDES et al., Cryptographic key management for SCADA systems - issues and perspectives, 2008 International Conference on Information Security and Assurance, IEEE, pp. 156-161.	☐
	21	BENDER et al., Evolution of SIM provisioning towards a flexible MCIM provisioning in M2M vertical industries, 16th International Conference on Intelligence in Next Generation Networks, IEEE, 2012, pp. 57-64.	☐
	22	PARK et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 International Conference on Availability, Reliability and Security, IEEE, 2013, pp. 297-303.	☐
	23	Appenzeller et al., Identity-Based Encryption Architecture and Supporting Data Structures RFC 5408, 2009, pp. 1-30.	☐
	24	Baugher et al., Group Key Management Architecture, RFC Draft, 2001, pp. 1-20.	☐
	25	Ben Saied, Yosra; Olivereau, Alexis; Laurent, Maryline; "A Distributed Approach for Secure M2M Communications", 5th International Conference on New Technologies, Mobility and Security (NTMS), 7-10 May 2012, pgs. 1-7.	☐
	26	Boyen et al., Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles), 2006.	☐
	27	Boyen et al., Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BBI Cryptosystems, RFC 5091, 2007, pp. 1-63.	☐
	28	Harney et al., Group Key Management Protocol (GKMP) Architecture, 1994, pp. 1-19.	☐
	29	Kiltz et al., CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption, 2008.	☐
	30	Krylov, What is Kerberos Authtentication?, 2003, pp. 1-4.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	31	Martin, Introduction to Identity-Based Encryption, ISBN-13 978-1-59693-238-8, 2008.	☐
	32	Merrian-Webster, Network, 2014.	☐
	33	Park et al., A New Practical Identity-Based Encryption System, 2003, pp_ 1-27.	☐
	34	Park et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 IEEE, pp_ 297-303.	☐
	35	Shih, Jie-Ren; Hu, Yongbo; Hsiao, Ming-Chun; Chen, Ming-Shing; Shen, Wen-Chng; Yang, Bo-Yin; Wu, An-Yeu; Cheng, Chen-Mou; "Securing M2M with Post-Quantum Public-Key Cryptography", IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 7 March 2013, pgs_ 106-116.	☐
	36	Voltage Security, The Identity-Based Encryption Advantage, 2015.	☐
	37	Yang et al., Identity-Based Key Agreement and Encryption for Wireless Sensor Networks, IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No. 5B, May 2006, pp_ 182-189.	☐
	38	Youngblood, An Introduction to Identity-based Cryptography, 2005.	☐
	39	Zhu et al., Public Key Cryptography for Initial Authentication in Kerberos (PPKINIT), RFC 4556, 2006, pp_ 1-42.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120033613	A1	2012-02-09	Lin et al.	
	2	20130028184	A1	2013-01-31	Lee et al.	
	3	20130182586	A1	2013-07-18	Paladugu et al.	
	4	20020018569	A1	2002-02-14	Panjwani et al.	
	5	20030003895	A1	2003-01-02	Wallentin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	6	20030211842	A1	2003-11-13	Kempf et al.	
	7	20040179684	A1	2004-09-16	Appenzeller et al.	
	8	20050008159	A1	2005-01-13	Grilli et al.	
	9	20050021875	A1	2005-01-27	Bouthemy et al.	
	10	20050120202	A1	2005-06-02	Cuellar et al.	
	11	20050138353	A1	2005-06-23	Spies et al.	
	12	20050193199	A1	2005-09-01	Asokan et al.	
	13	20050246282	A1	2005-11-03	Naslund et al.	
	14	20050278787	A1	2005-12-15	Naslund et al.	
	15	20060021063	A1	2006-01-26	Hori	
	16	20060056355	A1	2006-03-16	Love et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	17	20060059344	A1	2006-03-16	Mononen	
	18	20060206710	A1	2006-09-14	Gehrmann	
	19	20060281442	A1	2006-12-14	Lee et al.	
	20	20070206799	A1	2007-09-06	Wingert et al.	
	21	20080016230	A1	2008-01-17	Holtmanns et al.	
	22	20080022089	A1	2008-01-24	Leedom	
	23	20080114978	A1	2008-05-15	Lehtovirta et al.	
	24	20080165698	A1	2008-07-10	Dalsgaard et al.	
	25	20090116642	A1	2009-05-07	Yang et al.	
	26	20090028341	A1	2009-01-29	Hamachi	
	27	20090077643	A1	2009-03-19	Schmidt et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	28	20090125996	A1	2009-05-14	Guccione et al.	
	29	20090132806	A1	2009-05-21	Blommaert et al.	
	30	20090191857	A1	2009-07-30	Horn et al.	
	31	20090209232	A1	2009-08-20	Cha et al.	
	32	20090268909	A1	2009-10-29	Girao et al.	
	33	20090282246	A1	2009-11-12	Gunther	
	34	20090313472	A1	2009-12-17	Guccione et al.	
	35	20100166167	A1	2010-07-01	Karimi-Cherkandi et al.	
	36	20100031042	A1	2010-02-04	Di Crescenzo et al.	
	37	20100062808	A1	2010-03-11	Cha et al.	
	38	20100098253	A1	2010-04-22	Delerablee	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	39	20100275028	A1	2010-10-28	Takashima	
	40	20110016321	A1	2011-01-20	Sundaram et al.	
	41	20110055553	A1	2011-03-03	Lee et al.	
	42	20110237281	A1	2011-09-29	Busropan et al.	
	43	20110291803	A1	2011-12-01	Bajic et al.	
	44	20110314287	A1	2011-12-22	Escott et al.	
	45	20120011360	A1	2012-01-12	Engels et al.	
	46	20120023336	A1	2012-01-26	Natarajan	
	47	20120072732	A1	2012-03-22	Canard et al.	
	48	20120089568	A1	2012-04-12	Manley et al.	
	49	20120108205	A1	2012-05-03	Schell et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	50	20120117635	A1	2012-05-10	Schell et al.	
	51	20120159153	A1	2012-06-21	Shim et al.	
	52	20120260086	A1	2012-10-11	Haggerty et al.	
	53	20120260090	A1	2012-10-11	Hauck et al.	
	54	20120260095	A1	2012-10-11	Von Hauck et al.	
	55	20120278490	A1	2012-11-01	Sennett et al.	
	56	20120300932	A1	2012-11-29	Cambridge et al.	
	57	20120331292	A1	2012-12-27	Haggerty et al.	
	58	20130091556	A1	2013-04-11	Horn et al.	
	59	20130114810	A1	2013-05-09	Kobayashi et al.	
	60	20130117824	A1	2013-05-09	Naslund et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10169587	B1	2019-01-01	Nix	
	2	10621352	B2	2020-04-14	NIx	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060021063	A1	2006-01-26	Hori	
	2	20100093347	A1	2010-04-15	Hahn et al.	
	3	20110158411	A1	2011-06-30	Medvinsky et al.	
	4	20210126801	A1	2021-04-29	Nix	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	5	20200280436	A1	2020-09-03	Nix	
	6	20210218560	A1	2021-07-15	Nix	
	7	20210184842	A1	2021-06-17	Nix	
	8	20210194681	A1	2021-06-24	Nix	
	9	20190356482	A1	2019-11-21	Nix	
	10	20200226258	A1	2020-07-16	Nix	
	11	20190313246	A1	2019-10-10	Nix	
	12	20210211279	A1	2021-07-08	Nix	
	13	20200162269	A1	2020-05-21	Nix	
	14	20200162247	A1	2020-05-21	Nix	
	15	20190332774	A1	2019-10-31	Nix	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2518976	GB	A	2015-04-08	Vodafone IP Licensing Ltd		☐
	2	2021007235	WO	A1	2021-01-14	Nix		☐
	3	2021007235	WO	A1	2021-01-14	Nix		☐
	4	2021087221	WO	A1	2021-05-06	Nix		☐
	5	2020223319	WO	A1	2020-11-05	Nix		☐
	6	2020006162	WO	A1	2020-01-02	Nix		☐
	7	2019246206	WO	A1	2019-12-26	Nix		☐
	8	2019222319	WO	A1	2019-11-21	Nix		☐
	9	2019209598	WO	A1	2019-10-31	Nix		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	10	2019178312	WO	A1	2019-09-19	Nix		☐
	11	2020123959	WO	A1	2020-06-18	Nix		☐
	12	2020061023	WO	A1	2020-03-26	Nix		☐
	13	3110641	CA	A1	2019-10-31	Nix		☐
	14	3110468	CA	A1	2019-11-21	Nix		☐
	15	19803936	DE	A1	1999-08-05	Osram GmbH Siemens AG		☐
	16	3766222	EP	A1	2021-01-20	Nix		☐
	17	20130026351	KR	A	2013-03-13	SAMSUNG ELECTRONICS CO LTD	English Abstract	☒
	18	2013/048084	WO	A2	2013-04-04	SAMSUNG ELECTRONICS CO LTD	English Abstract	☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	1	Search Report issued in UK Application No. GB2108534.5 dated July 7, 2021.	☐
	2	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000)	☐
	3	TLS 1.3 Wish List Presentation, IETF 87 (Eric Rescorla), dated August 1, 2013.	☐
	4	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182424.8 dated October 12, 2021.	☐
	5	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182451.1 dated October 12, 2021.	☐
	6	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182432.1 dated October 12, 2021.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20150106616	A1	2015-04-16	Nix	
	2	20150121066	A1	2015-04-30	Nix	
	3	20150143125	A1	2015-05-21	Nix	
	4	20040162472	A1	2004-08-19	Berson et al.	
	5	20150215126	A1	2015-07-30	Ashdown	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	6	20160294829	A1	2016-10-06	Angus	
	7	20120108205	A1	2012-05-03	Schell et al.	
	8	20130012168	A1	2013-01-10	Rajadurai et al.	
	9	20140219447	A1	2014-08-07	Park et al.	
	10	20140161113	A1	2014-06-12	Cui et al.	
	11	20150113275	A1	2015-04-23	Kim et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	10-2013-0026352	KR	A	2013-03-13			☐
	2	10-2013-0026958	KR	A	2013-03-14			☐
	3	EP 1981 224	EP		2008-10-15			☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	4	2013027085	WO	A1	2013-02-28			☐
	5	2013066077	WO	A1	2013-05-10			☐
	6	2775853	CA	A1	2012-12-01			☐
	7	2011138238	WO	A1	2011-11-10			☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report for PCT/US2014/068544 dated February 13, 2015.	☐
	2	T. Pornin, Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm ECDSA), Internet Engineering Task Force RFC 6979, August 2013, pp.I-79.	☐
	3	GSMA, Fast Dormancy Best Practices Version 1.0,27 July 2011, TS.18, pp. 1-23.	☐
	4	N. CHU et al, EXALTED: Expanding LTE for Devices, European Commission for Information Society and Media, 31 October 2012, pp. 1-141.	☐
	5	J. HUANG et al, A Close Examination of Performance and Power Characteristics of 4G LTE Networks, Mobisys' 12, 25-29 June 2012, pp. 1-14.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	6	F. QIAN et al, TOP: Tail Optimization Protocol for Cellular Resource Allocation, 18th IEEE International Conference on Network Protocols (ICNP), 2010, 5-8 Oct. 2010, pp. 285-298.	☐
	7	ETSI, Machine-to-Machine communications (M2M), mia, dla, and mid interfaces, TS 102.921 v1.1.1, Feb 2012, pp. 1-538.	☐
	8	C. DOWNEY, Migrating Legacy M2M Systems to the Cloud, http://www.ecnmag.com/articles/2013/02/migrating-legacy-m2m-systems-cloud, Feb 2013, pp. 1-2.	☐
	9	A. Wander et al, Energy Analysis of Public-Key Cryptography on Small Wireless Devices, Sun Microsystems Laboratories, pp.1-16.	☐
	10	V. Martinez et al, A Survey of the Elliptic Curve Integrated Encryption Scheme, Journal of Computer Science and Engineering, Volume 2, August 2010, pp.7-13.	☐
	11	ETSI, UMTS;LTE; SIM/USIM Internal and External Interworking Aspects, TR 131900 v.10.0.0, May 2011, pp.1-41.	☐
	12	International Search Report and Written Opinion for PCT/US2014/062435 mailed February 6, 2015.	☐
	13	Wikipedia, RSA (algorithm), http://en.wikipedia.org/wiki/RSA_(algorithm), 9 Sept. 2013, pp. 1-12.	☐
	14	Wikipedia, Elliptic Curve Cryptography, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography, 9 Sept. 2013, pp. 1-8 .	☐
	15	L. LARZON, The Lightweight User Datagram Protocol (UDP-Lite), Internet Engineering Task Force RFC 3828, July 2004, pp. 1-12.	☐
	16	Wikipedia, Digital Signature, http://en.wikipedia.orglwiki/Digital_signature, 9 Sept. 2013, pp. 1-10.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18416534
	Filing Date	2024-01-18
	First Named Inventor	John A. Nix
	Art Unit	
	Examiner Name	
	Attorney Docket Number	63121/0226

	17	D. Cooper, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force RFC 5280, pp. 1-133.	☐
	18	J. Jonsson et al, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Internet Engineering Task Force RFC 3447, February 2003, pp.1-72.	☐
	19	D. McGrew et al, Fundamental Elliptic Curve Cryptography Algorithms, Internet Engineering Task Force RFC 6090, February 2011, pp. 1-34.	☐
	20	Wikipedia, Elliptic Curve Diffie-Hellman, http://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman, 24 Sept. 2013, pp. 1-2.	☐
	21	ETSI, Smart Cards; Embedded UICC; Requirements Specification, TS 103 383 v12.1.0, June 2013, pp. 1-20.	☐
	22	3GPP, 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture, 3GPP TS 33.401 V12.9.0 (2013-09) pp. 1-75.	☐
	23	3GPP, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3, 3GPP TS 24.301 v12.2.0, Sept. 2013 pp. 1-6, 63-100.	☐
	24	ETSI, Smart Cards; UICC-Terminal Interfaces; Physical and Logical Characteristics, TS 102 221 v11.0.0, June 2012, pp. 1-181.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	18416534
Filing Date	2024-01-18
First Named Inventor	John A. Nix
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith J. Barkaus/	Date (YYYY-MM-DD)	2024-04-09
Name/Print	Keith J. Barkaus	Registration Number	51,431

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
18/416,534	01/18/2024		1072	63121/0226	22	1

CONFIRMATION NO. 7559

UPDATED FILING RECEIPT

1912
AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

OC00000070872137

Date Mailed: 04/09/2024

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

John A. Nix, Evanston, IL;

Applicant(s)

Network-1 Technologies, Inc., New York, NY;

Power of Attorney: The patent practitioners associated with Customer Number 01912

Domestic Priority data as claimed by applicant

This application is a CON of 17/547,990 12/10/2021 PAT 11,916,893
which is a CON of 16/453,682 06/26/2019 PAT 11,233,780
which is a CIP of 16/110,804 08/23/2018 PAT 10,382,422
which is a CON of 15/928,848 03/22/2018 PAT 10,084,768
which is a CON of 14/751,119 06/25/2015 PAT 9,961,060
which is a CON of 14/099,329 12/06/2013 PAT 9,100,175

Foreign Applications for which priority is claimed (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Petitioner Samsung Ex-1004, 0320

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 02/01/2024

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 18/416,534**

Projected Publication Date: 07/18/2024

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

Petitioner Samsung Ex-1004, 0321

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

Petitioner Samsung Ex-1004, 0322

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Petitioner Samsung Ex-1004, 0323

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 18/416,534

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	64		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	280		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	320		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	22 minus 20 =	* 2	x 40 =	80	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x =	0			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			168			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	912		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	**04/05/2024 12:40:39 PM Z ET**	**63121/0226**

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	64981004	FILING DATE	01/18/2024
CUSTOMER #	1912	FIRST NAMED INVENTOR	John A. Nix
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Keith Barkaus

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
1-ResponsetoNTFMP.pdf	2	Applicant Response to Pre-Exam Formalities Notice	95 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
1-ResponsetoNTFMP.pdf	3F713566AF9C56CB13C468EF8BBC72A00C367BA48A44143234 B233CCB79F60B0D5C5053231AE264170296972E68DA96DC07 121780A125E37BE790F3117938C63A

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	04/05/2024 12:40:39 PM Z ET	63121/0226

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	64961004	AUTHORIZED BY	Keith Barkaus
CUSTOMER #	1912	FILING DATE	01/18/2024
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	John A. Nix

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1010	E202445C41236204	Victoria GILMORE

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2054	Non-DOCX Filing Surcharge	160.00	1	160.00
			TOTAL AMOUNT:	$160.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C.

371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Network-1 Technologies, Inc.	Confirmation No.: 7559
Title:	Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication	
Appl. No.:	18/416,534	
Filing Date:	January 18, 2024	
Examiner:	TBD	
Art Unit:	TBD	
Docket No.:	63121/0226	
Customer No.:	01912	

RESPONSE TO NOTICE TO FILE MISSING PARTS

VIA EFS

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is being submitted in reply to the Notice to File Missing Parts issued on February 8, 2024, in connection with the above-identified patent application.

Remarks begin on page **2.**

Petitioner Samsung Ex-1004, 0329

REMARKS

This is a response to the Notice to File Missing Parts dated February 8, 2024 (the "Notice") in connection with the above-referenced application. A response to the Notice is due April 8, 2024 such that the present response is being timely filed.

The Notice states that Applicant is required to pay the non-DOCX fee. In response, Applicant submits herewith the additional fee ($160).

Applicant respectfully submits that the foregoing constitutes a bona fide response to all issues raised in the Notice and requests that the application be taken up for examination in due course. Should any questions arise in connection with this response, the Office is invited to contact the undersigned at the number provided below.

As indicated above, Applicant submits herewith the $160 surcharge. If any additional fees are required in order to preserve the pendency of the subject application, the Director is hereby authorized to charge any such fee to Deposit Account No. 01-1785.

Respectfully submitted,

AMSTER, ROTHSTEIN & EBENSTEIN LLP
Attorneys for Applicant
405 Lexington Avenue
New York, NY 10174
(212) 336-8000

Dated: New York, New York
April 5, 2024

By: /Keith J. Barkaus/
Keith J. Barkaus
Registration No. 51,431

Petitioner Samsung Ex-1004, 0330

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
18/416,534	01/18/2024		912	63121/0226	22	1

CONFIRMATION NO. 7559

FILING RECEIPT

1912
AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

OC00000068001334

Date Mailed: 02/08/2024

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

John A. Nix, Evanston, IL;

Applicant(s)

Network-1 Technologies, Inc., New York, NY;

Power of Attorney: The patent practitioners associated with Customer Number 01912

Domestic Priority data as claimed by applicant

This application is a CON of 17/547,990 12/10/2021
which is a CON of 16/453,682 06/26/2019 PAT 11,233,780
which is a CIP of 16/110,804 08/23/2018 PAT 10,382,422
which is a CON of 15/928,848 03/22/2018 PAT 10,084,768
which is a CON of 14/751,119 06/25/2015 PAT 9,961,060
which is a CON of 14/099,329 12/06/2013 PAT 9,100,175

Foreign Applications for which priority is claimed (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Petitioner Samsung Ex-1004, 0331

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 02/01/2024

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 18/416,534**

Projected Publication Date: To Be Determined - pending completion of Missing Parts.

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

Petitioner Samsung Ex-1004, 0332

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

Petitioner Samsung Ex-1004, 0333

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Petitioner Samsung Ex-1004, 0334

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 18/416,534

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	64		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	280		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	320		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	22 minus 20 =	* 2	x 40 =	80	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x =	0			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			168			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	912		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
18/416,534	01/18/2024	John A. Nix	63121/0226

CONFIRMATION NO. 7559

1912
AMSTER, ROTHSTEIN & EBENSTEIN LLP
405 LEXINGTON AVENUE
FLOOR 48
NEW YORK, NY 10174

FORMALITIES LETTER

OC000000068001336

Date Mailed: 02/08/2024

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

An application number and filing date have been accorded to the above-identified nonprovisional application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The fee set forth in 37 CFR 1.16(u) for submitting documents not in DOCX format has not been received.

  The fee is due because:
  - the specification was not submitted in DOCX format.
  - the claims were not submitted in DOCX format.
  - the abstract was not submitted in DOCX format.

  Note: The fee set forth in 37 CFR 1.16(u) is required if the specification, claims, and/or abstract do not conform to the USPTO requirements for submission in DOCX format. In addition, if applicants submit a PDF version of the specification, claims, and/or abstract that is not generated by the USPTO filing system and also includes a DOCX version of the specification, claims, and/or abstract, then the surcharge is required for the version of the specification, claims, and/or abstract that were submitted in PDF format. However, the fee set forth in 37 CFR 1.16(u) will not be required if applicant submitted an Auxiliary PDF in compliance with the USPTO process for submitting an Auxiliary PDF that was automatically assigned the document code AUX.PDF.

SUMMARY OF FEES DUE:

The fee(s) required (including the fees noted above) are as follows. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $**160** non-DOCX fee.
- $(**0**) previous unapplied payment amount.
- $**160** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Petitioner Samsung Ex-1004, 0336

Replies should be addressed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

REPLY VIA ELECTRONIC FILING

A reply may be submitted via electronic filing only by registered users of the appropriate USPTO patent electronic filing system and must include:

- A separate document having the document description, "**Applicant response to Pre-Exam Formalities Notice**"; and
- the item(s) for which a reply period is set forth above.

For more information about electronic filing, contact the Patent Electronic Business Center (EBC) 1-866-217-9197 or visit https://www.uspto.gov/ebc

NOTE: If the reply is not being submitted electronically, a copy of this notice must be included.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/azahmed/

Petitioner Samsung Ex-1004, 0337

United States Patent and Trademark Office

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

WELCOME TO THE UNITED STATES PATENT AND TRADEMARK OFFICE (USPTO)

*Congratulations on taking the first step to protect your invention. You can now advertise or mark any products covered by this application for your invention as **"Patent Pending"** for as long as this application is pending!*

We are here to help you on the rest of your journey.

New to the process? The Patent Basics page will take you from "What is a patent?" to assistance with the application process.

- **www.uspto.gov/PatentBasics**

Consider cost savings. You might qualify for small entity or micro entity status, which means a discount on most USPTO patent fees.

- **www.uspto.gov/EntityStatus**

Become a registered electronic filer (eFiler). You'll gain access to the full capabilities of Patent Center. As a registered eFiler, you can electronically view your submission, track the progress of your application, and respond to USPTO correspondence.

- **www.uspto.gov/NewPatentFilers**

Learn how to identify which of your creative ideas might be intellectual property assets and how to protect them by using the USPTO Intellectual Property (IP) Identifier.

- **ipidentifier.uspto.gov**

We also provide Pro Se Assistance, support specifically geared for **independent inventors without an attorney or agent.** Follow the link below, call us at 866-767-3848, or email **proseassistancecenter@uspto.gov**.

- **www.uspto.gov/ProSePatents**

Need help near you? We have regional offices across the country, as well as Patent and Trademark Resource Centers in libraries in nearly every state, with specialists standing by to help you at no cost.

- **www.uspto.gov/locations**
- **www.uspto.gov/ptrc**

Contact us:

- **General information:** USPTO Contact Center
  - **www.uspto.gov/help**
- **Patent Center:**
  Patent Electronic Business Center
  - **www.uspto.gov/EBC**
- **Pre or post-examination:** Application Assistance Unit
  - **www.uspto.gov/PatentAssistance**

Want to learn more?

- **Access our free services** all in one spot. Find all of our contact centers, nationwide services, events, education, and training.
  - **www.uspto.gov/FreeServices**
- **Connect with us** on Instagram, LinkedIn, Twitter, Facebook, and YouTube.
- **Hear about resources for startups, inventors, and entrepreneurs,** as well as our initiatives engaging women, the military community, and others. These programs offer helpful tips and tricks on identifying and managing your IP, finding options for funding, and expanding your network to support your business.
  - **www.uspto.gov/startups**
  - **www.uspto.gov/inventors**
  - **www.uspto.gov/initiatives**
- We hope you connect with us by subscribing to receive important notifications by email.
  - **www.uspto.gov/subscribe**

Kathi Vidal

Kathi Vidal
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

Derrick Brent
Deputy Under Secretary of Commerce for Intellectual Property and
Deputy Director of the United States Patent and Trademark Office

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR UNITED STATES PATENT

Title: **An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication**

Inventor: John A. Nix
807 Davis St., Unit 409
Evanston, IL 60201
Citizen of the United States of America

Petitioner Samsung Ex-1004, 0339

CROSS-REFERENCE TO RELATED APPLICATIONS

This is a continuation of U.S. Patent Application No. 17/547,990, filed December 10, 2021 , and entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication", which is a continuation of U.S. Patent Application No. 16/453,682, filed June 26, 2019, entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," which is a continuation of U.S. Patent Application No. 16/110,804, filed August 23, 2018, entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," which is a continuation of U.S. Patent Application No. 15/928,848, filed March 22, 2018, entitled "EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION," which is a continuation of U.S. Patent Application No. 14/751,119, filed June 25, 2015, entitled "An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication", now U.S. Patent No. 9,961,060, which is a continuation of U.S. Patent Application No. 14/099,329, filed December 6, 2013, entitled "An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," now U.S. Patent No. 9,100,175, the contents of all of which are incorporated herein by reference in their entirety.

The subject matter of this application is related to the subject matter of U.S. Patent Application Serial No. 14/084,141, filed November 19, 2013 in the name of John Nix, entitled "Key Derivation for a Module using an Embedded Universal Integrated Circuit Card," now U.S. Patent No. 9,319,223, which is hereby incorporated by reference in its entirety.

Petitioner Samsung Ex-1004, 0340

BACKGROUND

Technical Field

The present methods and systems relate to communications for a module, and more particularly, to methods and systems for using an embedded universal integrated circuit card (eUICC), where the methods and systems also support the authentication of a user associated with the eUICC.

Description of Related Art

The combination of "machine-to-machine" (M2M) communications and using low-cost sensors, Internet connections, and processors is a promising and growing field. Among many potential benefits, M2M technologies allow the remote monitoring and/or control of people, assets, or a location where manual monitoring is not economic, or costs can be significantly reduced by using automated monitoring as opposed to manual techniques. Prominent examples today include vending machines, automobiles, alarm systems, and remote sensors. Fast growing markets for M2M applications today include tracking devices for shipping containers or pallets, health applications such as, but not limited to, the remote monitoring of a person's glucose levels or heartbeat, monitoring of industrial equipment deployed in the field, and security systems. Many M2M applications leverage either wired Internet connections or wireless connections, and both types of connections continue to grow rapidly. M2M applications may also be referred to as "the Internet of things".

M2M communications can provide remote control over actuators that may be connected to a M2M device, such as, but not limited to, turning on or off a power switch, locking or unlocking a door, adjusting a speed of a motor, or similar remote control. A decision to change or adjust an actuator associated with an M2M device can utilize one or a series of sensor measurements. An M2M device may also be referred to as a "wireless module" or also simply a

Petitioner Samsung Ex-1004, 0341

module. As one example, if a building or room is too cold, then temperature can be reported to a central server by an M2M device and the server can instruct the M2M device to turn on a switch that activates heat or adjusts a thermostat. As the costs for computer and networking hardware continue to decline, together with the growing ease of obtaining either wired or wireless Internet access for small form-factor devices, the number of economically favorable applications for M2M communications grows.

Many M2M applications can leverage wireless networking technologies. Wireless technologies such as, but not limited to, wireless local area networks and wireless wide area networks have proliferated around the world over the past 15 years, and usage of these wireless networks is also expected to continue to grow. Wireless local area network (LAN) technologies include WiFi and wireless wide area network (WAN) technologies include 3rd Generation Partnership Project's (3GPP) 3rd Generation (3G) Universal Mobile Telecommunications System (UMTS) and 4th Generation (4G) Long-term Evolution (LTE), LTE Advanced, and the Institute of Electrical and Electronics Engineers' (IEEE) 802.16 standard, also known as WiMax. The use of wireless technologies with M2M communications creates new opportunities for the deployment of M2M modules in locations less suitable for fixed-wire Internet access, but also creates a significant new class of problems that need to be solved.

One class of problems for using M2M modules with traditional wireless networks results from basic design considerations for the wireless networks, where many wireless wide-area networking standards were designed and optimized for mobile phones, including smart phones. A core element of traditional wireless WAN technologies such as 3GPP and ETSI standards over the past 20 years has included the use of a subscriber identity module (SIM) card within 2G networks and a related universal integrated circuit card (UICC) for 3G and 4G networks, including LTE networks. ETSI standards for a physical UICC as of 2013 include ETSI TR 102 216. Traditionally, these cards have been supplied by a mobile network operator (MNO) and contain 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. The parameters could

Petitioner Samsung Ex-1004, 0342

include (i) an identity such as an IMSI, (ii) a set of frequencies for a mobile phone to scan in order to locate a beacon signal from the MNO, (iii) a preferred access list of other MNOs in order to support roaming in locations where the MNI associated with the IMSI is not available, and (iv) many other related parameters as well. The physical media and cards in the form of a UICC can be appropriate or suitable for a mobile phone or mobile handset, where an end user can readily replace or "swap out" the physical card as the mobile phone changes geographical locations or due to other preferences for the subscriber or end-user. Distributors of either mobile handsets or mobile phone service can physically insert or change an appropriate UICC for the mobile phones as well.

However, the rapid growth for "machine-to-machine" applications has created significant challenges to the traditional model of utilizing physical media such as a UICC in order to provide data and parameters for a module's connectivity to a MNO. Exemplary reasons for potential difficulties with physical media such as a UICC in M2M applications include (i) the modules may be installed in remote locations that are difficult or expensive to reach after installation, such as, but not limited to, tracking devices on shipping containers that can move globally, (ii) a manufacturer or service provider may prefer for the module to be hermetically sealed for business or technical reasons, including the physical UICC may not be easily tampered with, and (iii) a module (such as a tracking device on a 40 foot shipping container) may move between several different countries, and the lowest costs for Internet or data connectivity through the wireless WAN may be through utilizing different UICC cards from different operators, but the cost of swapping the UICC card could be prohibitive.

Other needs for changing a preferred network or network credentials without physically changing a UICC exist as well. These needs have been one motivation for the industry, including ETSI and 3GPP standards bodies, to consider an embedded UICC, also known as an "eUICC". With an eUICC, the operation of an UICC can be essentially "virtualized", such that the data and algorithms within a UICC can be processed in software and distributed through electronic media (such as, but not limited to, a file transfer or file download). Exemplary

Petitioner Samsung Ex-1004, 0343

benefits and technical considerations for using an eUICC in M2M applications as of November 2013 is outlined in ETSI TS 103 383 v12.1, entitled “Smart Cards; Embedded UICC; Requirements Specification,” which is herein incorporated by reference in its entirety. Note that this published standard from June 2013, and the standard is primarily in the requirements definition phase, and many of the technical specifications for implementation and operation of an eUICC will be defined in the future.

Although the use of an embedded eUICC can solve many of the issues for distributing and managing physical media such as a UICC, many additional challenges remain. Many open and remaining challenges for a eUICC pertain to securely and electronically transferring a new set of MNO network access credentials (such as an IMSI and network key K) to a module in a secure and efficient manner. A need exists in the art for a module to securely obtain network access credentials. Another need exists in the art for the obtained credentials in a eUICC to be fully compatible with the significant installed and legacy base of networks that use a pre-shared secret key K, where the key K serves as the foundation for authentication and ciphering of data for a mobile phone or user equipment, including modules using conventional technology. A successful solution to these needs for M2M applications in the form of an eUICC can also provide a working solution of the needs for regular mobile phones as well, such that a consumer mobile phone or smartphone could implement and utilize an eUICC in order to eliminate the costs and complexity of dealing with a physical UICC.

A need exists in the art for module and a mobile network operator to securely share a pre-shared secret key K without depending on physical distribution of the key K or electronic distribution of the key K through 3rd parties, even in an encrypted form. A need exists in the art for the decryption of data within an eUICC profile to be under the control of the mobile network operator, because the mobile network operator may not control the distribution or release of profiles from an eUICC subscription manager to a module with an eUICC. As currently contemplated in November of 2013 by eUICC standards discussed above, a pre-shared secret key K and related network access credentials are transmitted to a module from an eUICC

Petitioner Samsung Ex-1004, 0344

subscription manager. The pre-shared secret key K is also known as key K in 4G LTE and related networks and key Ki in 3G networks. The resulting security for the electronically transferred, pre-shared secret key K is no stronger than (i) the encryption on the channel used to transfer key K, and (ii) the security and chain of control for keys used to encrypt the communications channel transferring key K to a module or a mobile phone. A module and mobile network operator (MNO) using an electronically transferred key K for network access credentials is dependent on the communications channel for transferring key K, even though that communications channel may be outside the control of the MNO (such as at a time when key K is transferred using another MNO or a different network). Therefore, a need exists in the art for the MNO to securely and efficiently control the use of an electronically transferred key K within a profile for an eUICC, even though copying and distributing the profile may be outside the control of the MNO.

In addition, over an extended period of time such as several years, a mobile network operator could prefer for the key K to periodically rotate or change for an individual module or mobile phone in order to increase security. The continued and extended use of a single key K for all communications with a module or mobile phone can be a security risk, especially with a large volume of data transferred that could be subject to analysis for cryptographic weaknesses by potential attackers. Additionally, in the future a standard key length for key K may increase from today's current 128 bits to a longer key length such as an exemplary 256 bits. With conventional technology where key K is recorded in physical media such as a UICC, the only feasible way to change key K for a module or mobile phone is to physically distribute a new UICC card, with resulting costs and business complexities. A need exists in the art for a module, including a mobile phone, and a MNO to securely and efficiently support a change in network access credentials, including a key K for the module connecting to the MNO, without requiring a physical replacement of a UICC or equivalent physical media recording a key K.

And other needs exist in the art as well, as the list recited above is not meant to be exhaustive but rather illustrative.

Petitioner Samsung Ex-1004, 0345

SUMMARY

Methods and systems are provided for secure and efficient communication using a module to communicate with a server and a mobile operator network. The module can support "Machine to Machine" (M2M) communications, also known as "the Internet of things". The methods and systems contemplated herein can also support other applications as well, including mobile phone handsets connecting to a wireless network, where the wireless network can be associated with or the radio access portion of a mobile network operator. 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. An objective of the invention is to address the challenges noted above for securing the deployment of modules that can utilize an embedded universal integrated circuit card (eUICC) and/or also PKI algorithms and keys.

The methods and systems contemplated herein can reduce the need for manual intervention with a module in order to automatically and remotely change network access credentials in order for the module to utilize new or different keys in order to connect and authenticate with a wireless network. By using an eUICC, where the eUICC can support both (i) the authentication of a user by the MNO, and (ii) the secure decryption or derivation of the key K under control of the MNO, the value and usefulness of modules can be increased for a user and a mobile operator network. An eUICC can also comprise software and/or firmware components to "virtualize" the operation of a physical UICC, such that (i) the data normally recorded in a physical UICC can be recorded in a file with encryption, and (ii) the steps for using the data in the file can be processed by an eUICC.

In a first embodiment, a mobile network operator can process a set of data for inclusion in a profile for an eUICC. Data within the profile can be equivalent or similar to the data recorded in a physical UICC, including a set of network parameters, a module network identity, and a first key K. The mobile network operator can send the data for a profile to an eUICC

Petitioner Samsung Ex-1004, 0346

subscription manager. A module can include an embedded universal integrated circuit card (eUICC). The eUICC can be processed by an operating system on the module and can be recorded in a nonvolatile memory, such that the eUICC is available after a powered off state. The eUICC can include data such as an eUICC identity, an eUICC profile key, and a symmetric ciphering algorithm. A manufacturer or distributor could record the data for the eUICC before the module is received by a user. The eUICC can communicate in the module with a network application. The network application can communicate with the mobile network operator using a wireless network and a radio within the module. The module can connect with a first network, send the eUICC identity and receive an encrypted profile, and the module can record the encrypted profile in a nonvolatile memory associated with the eUICC. The first network can be a network different than the wireless network for the profile, and the first network could comprise a WiFi network, a LAN connection using a USB interface to the module, or a public land mobile network.

Continuing with this first embodiment, the encrypted profile as received by the module can include a first portion of ciphertext and a second portion of ciphertext. The module using the eUICC can decrypt the first potion of ciphertext using the eUICC profile key and the symmetric ciphering algorithm. The resulting plaintext from the decrypted first portion of ciphertext can include the set of network parameters, the first network module identity, and the first key K. The module using the eUICC can select and activate the profile in order to connect with the wireless network associated with the mobile network operator. The module can conduct a first authentication with the mobile network operator using the first network module identity and the first key K. The module can send an attach request message, including an exemplary radio resource request message with the first network module identity, and the module can receive a random number in the form of a first RAND value.

Continuing with this first embodiment, the module can forward the RAND to the eUICC with the activated profile. The eUICC can input the first RAND and the first key K into a cryptographic algorithm in order to output a response RES value. The eUICC can return the

Petitioner Samsung Ex-1004, 0347

RES value to the module, and the module could forward the RES to the wireless network. The wireless network can compare the received RES with a stored, expected RES (previously calculated using the same first RAND and first key K), and if the two RES values match then the module with the eUICC and profile can be authenticated by the network. The network and the module can take additional steps for the module to have at least limited access to an IP network. With access to the IP network for the module, a user associated with the module can conduct an authentication with the mobile network operator (whereas the mobile network operator may not have control over distribution of the profile with the network access credentials including the first key K up to this point).

Continuing with this first embodiment, the mobile network operator can authenticate or verify a user or M2M service provider associated with the module. The authentication or verification could comprise steps to verify a user, including the user entering information in a web page through the IP connection established with the network in the paragraph above using the first key K. Or the user could place a telephone call to a call center, and the user could verbally confirm identification information or enter DTMF digits. Or, the MNO could authenticate or verify the identity of a user associated with the module by a representative of the MNO visually viewing physical identification of the user such as a drivers license or a passport. If the module is associated with or operated by an M2M service provider, then the MNO could exchange data with the M2M service provider in order to confirm the module with the first key K is authenticated. In either case, where the module is associated with a user or an M2M service provider, the MNO could take steps to authenticate with a second factor, where authentication with the first factor comprised receiving the RES. After successful authentication with the second factor, the MNO can confirm the identity of an entity associated with the module, whereas that identity may not be known before the authentication with the second factor since the distribution of the eUICC profile may be outside the control of the mobile network operator.

Continuing with this first embodiment, after successful authentication with the second factor, the mobile network operator can send a symmetric key to the module. The symmetric key

Petitioner Samsung Ex-1004, 0348

can be encrypted with a key ciphering algorithm. Or, the symmetric key can be (i) plaintext at the application layer, and (ii) encrypted at the data-link layer using the encryption between the module and wireless network after the first authentication above with the first key K. The module can receive the symmetric key (and decrypt the symmetric key if encrypted), and subsequently decrypt the second portion of ciphertext in the eUICC profile. The second portion of ciphertext can include a second network module identity and a second key K. The module can convert the second portion of ciphertext into plaintext using the symmetric ciphering algorithm and the received symmetric key. Note that the decryption of the second portion of ciphertext in the profile without the symmetric key is not feasible, and thus the mobile network operator can retain control over the use of the second key K in the profile for the eUICC, such as not releasing the symmetric key until after a user has successfully completed authentication with the mobile network operator as contemplated in the paragraph above.

After decrypting the second portion of ciphertext, the module with the eUICC can read a plaintext second network module identity and second key K. The second key K can be recorded in a protected, nonvolatile memory. The module can disconnect from the wireless network (where the first session used the first key K), and reconnect with the wireless network using the second network module identity and the second key K. The module with the eUICC can conduct a second authentication using the second key K, including sending the second network module identity, receiving a second RAND value, calculating a second RES value using the second RAND and the second key K, and sending the second RES value. After a successful second authentication, the module can access the IP network and the public Internet through the wireless network, and subsequent authentications with the wireless network can continue to use the second network module identity and the second key K. For embodiments where the module comprises a mobile phone and the user is an individual subscribing to mobile phone services from the mobile network operator, the user can be associated with a telephone number and place/receive phone calls after a successful second authentication.

Petitioner Samsung Ex-1004, 0349

In another embodiment, the eUICC profile key, associated with decrypting the profile from the eUICC subscription manager, may not be recorded in the eUICC before the eUICC sends an eUICC identity to the module, where the module sends the eUICC identity to the eUICC subscription manager through a first network. The eUICC can record an eUICC private key and the eUICC subscription manager could record an eUICC public key. The eUICC subscription manager can (i) encrypt the profile with the eUICC profile key, and then (ii) encrypt the eUICC profile key with an asymmetric ciphering algorithm and the eUICC public key, where the output is an encrypted eUICC profile key. The eUICC can receive the encrypted eUICC profile key from the eUICC subscription manager and decrypt the encrypted eUICC key using the asymmetric ciphering algorithm and the eUICC private key. After reading the plaintext eUICC profile key, the eUICC can decrypt the encrypted profile using the plaintext eUICC profile key, in order to read a plaintext first key K and first network module identity.

In an exemplary embodiment, the first key K is a null value for a profile recorded in the eUICC in a module. The use of a null value or the number zero for a shared secret key K is contemplated in wireless WAN standards and supported by commercial wireless networks in order to support emergency services for a module without a valid UICC. With a null value for the first key K, the MNO and wireless network can provide limited access to the IP network, such that a user of the module with a null or zero value for the first key K could perform steps to authenticate or verify the user with the MNO through the IP network accesses with the first key K as a null value. The data-link layer may not be effectively ciphered due to the use of a null value for the first key K, but the application or transport layer could secure communication from a web browser on the module to a web server for the user to authenticate with the MNO. The secure communication between the web browser and web server can utilize transport layer security (TLS) or similar standards for security at the transport or application layer, even though the data-link or network layer may not be encrypted. After successful authentication via the web browser, the MNO can take steps (discussed in other embodiments) allowing the module with

Petitioner Samsung Ex-1004, 0350

the eUICC to access and use a second key K and a second network module identity for subsequent secured communication between the module and the MNO.

In another embodiment, the second key K can be derived using by both the mobile network operator and the module with the eUICC using a key derivation algorithm. The eUICC could include an eUICC key exchange algorithm and the mobile network operator could include a MNO key exchange algorithm, and the key exchange algorithms can include a key derivation algorithm that accepts input of a token value, a private key, and a public key for the other node. The mobile network operator and the module with the eUICC could communicate the token value used for the key derivation algorithm (including using the connectivity through the wireless network after using the first key K in the profile). The module can record an eUICC private key, and the MNO can have access to the eUICC public key. The key derivation algorithm in the eUICC key exchange algorithm can output a second key K using the token. The MNO can obtain the same value for the second key K. In this manner, both node can derive the same second key K without electronically transferring the second key K, even in encrypted form and thereby increasing the security of a systems with an eUICC.

In an exemplary embodiment can support a module changing a key K used to (i) authenticate with a wireless network and (i) cipher/decipher data with a wireless network. The module can change key K without requiring the manual exchange of a UICC or other physical intervention. The module can use an eUICC profile and change key K while using the same eUICC profile. The module, could also comprise a mobile phone such as, but not limited to, a smart phone. After connecting with a first network, which could comprise a first wireless WAN, wireless LAN, or wired connection, the module can receive a eUICC profile for an eUICC in the module, where the eUICC profile includes a first network module identity and a first key K. The first key K can be a standards-based key K used with wireless networks, and be equivalent to a pre-shared secret key K recorded in physical UICCs for LTE networks.

After authenticating with the wireless network using the first key K, the module and MNO can share a token. The module and MNO can mutually derive a second key K using the

Petitioner Samsung Ex-1004, 0351

token and a key derivation algorithm. The module can disconnect from the wireless network after attaching using the first key K, and then reconnect using the second key K which has now been mutually derived by both the module and the mobile network operator. The module or MNO could determine or evaluate if the use of a new key K is required or preferred, and share a new token for input into the key derivation algorithms to derive a mutually shared new key K. In this manner, a module can change the key K used to authenticate and cipher/decipher data with a wireless network from a first key K to a second key K. This can increase flexibility of the system and reduce costs of physically distributing a new UICC to the module (or electronically sending new eUICC profiles) in order to change a key K.

These as well as other aspects and advantages will become apparent to those of ordinary skill in the art by reading the following detailed description, with reference where appropriate to the accompanying drawings.

Petitioner Samsung Ex-1004, 0352

BRIEF DESCRIPTION OF THE DRAWINGS

Various exemplary embodiments are described herein with reference to the following drawings, wherein like numerals denote like entities.

Figure 1a is a graphical illustration of an exemplary system that includes a module and a mobile network operator, in accordance with exemplary embodiments;

Figure 1b is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments;

Figure 1c is a graphical illustration of components within a module, in accordance with exemplary embodiments;

Figure 1d is a graphical illustration for authenticating with a wireless network using a physical UICC, in accordance with conventional technology;

Figure 1e is a graphical illustration for authenticating with a wireless network using an eUICC, in accordance with exemplary embodiments;

Figure 1f is a graphical illustration of an exemplary system that includes a module, a mobile network operator, and an eUICC in accordance with exemplary embodiments;

Figure 2a is a graphical illustration of an exemplary profile for an eUICC, including encrypted data, decryption steps, and decrypted data for the profile, in accordance with exemplary embodiments;

Figure 2b is a graphical illustration for ciphering and deciphering a profile using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments;

Figure 2c is a graphical illustration for ciphering and deciphering a key K using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments;

Figure 2d is a graphical illustration of a public key and a private key for an eUICC, in accordance with exemplary embodiments;

Petitioner Samsung Ex-1004, 0353

Figure 2e is a graphical illustration for ciphering and deciphering a key for an eUICC using an asymmetric ciphering algorithm using a PKI key pair, in accordance with exemplary embodiments;

Figure 3 is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments;

Figure 4 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments;

Figure 5a is a graphical illustration of a public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments;

Figure 5b is a graphical illustration of deriving a second key K using public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments;

Figure 5c is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments; and,

Figure 6 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments.

Petitioner Samsung Ex-1004, 0354

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS OF THE INVENTION

Figure 1a

Figure 1a is a graphical illustration of an exemplary system that includes a module and a mobile network operator, in accordance with exemplary embodiments. The system 100 includes a module 101 operating within a wireless network 102. System 100 can also include a mobile network operator 104, an IP Network 111, and an eUICC subscription manager 109. Mobile network operator (MNO) 104 can include a server 105. For embodiments where the MNO 104 uses 4G LTE and LTE Advanced networks, server 105 could comprise a home subscriber server (HSS) and/or a mobility management entity (MME). Server 105 could be a server with related functionality as a HSS or MME for a MNO 104 that uses different wireless network standards than those based on 4G LTE. Although not illustrated in Figure 1a, an eUICC subscription manager 109 may also include one or more servers 105, such that a first server 105 could function as an HSS in 4G LTE and LTE Advanced networks and a second server 105 could function as a MME in 4G LTE and LTE Advanced networks.

System 100 is illustrated without specific packet transmissions between module 101 and mobile network operator 104 and eUICC subscription manager 109. Examples of the communications and messages pertaining to the present invention will be illustrated in later Figures. As contemplated herein, machine-to-machine communications may comprise communication between a module 101 and a server 105, such that data can be transferred between the two with minimal manual intervention, although manual intervention can be required to set up system 100 and any occasional manual maintenance required. As contemplated herein, machine-to-machine communications may also be referred to as “the Internet of things” (IoT). Also note that module 101 may comprise a wireless module, such that module 101 can communicate with wireless network 102 using a radio and an antenna. A wireless or a wired configuration for module 101 can be utilized in the present invention.

Petitioner Samsung Ex-1004, 0355

If module 101 operates as a wireless module, module 101 and wireless network 102 can communicate using a base station 103. Module 101 and wireless network 102 can utilize a variety of wireless technologies to communicate, including WiFi, WiMax, a 2nd generation wireless wide area network (WAN) technology such as, but not limited to, General Packet Radio Services (GPRS) or Enhanced Data rates for GSM Evolution (EDGE), 3rd Generation Partnership Project (3GPP) technology such as, but not limited to, 3G, 4G LTE, or 4G LTE Advanced, and other examples exist as well including wireless networks based on WiMAX standards. A wired module 101 can connect to the IP Network 111 via a wired connection such as, but not limited to, an Ethernet, a fiber optic, or a Universal Serial Bus (USB) connection (not shown).

Generally, the communication techniques described herein can be independent of the network technologies utilized at the physical and data-link layers, so long as the underlying network provides access to the IP Network 111 and supports Internet Protocols (IP). The IP Network 111 can be an IPv4 or an IPv6 packet-switched based network that utilizes standards derived from the Internet Engineering Task Force, such as, but not limited to, RFC 786 (User Datagram Protocol), RFC 793 (Transmission Control Protocol), and related protocols. The IP Network 111 can be the public Internet comprising globally routable IP addresses, or a private network that utilizes private IP addresses. IP Network 111 as illustrated in Figure 1a could comprise the globally routable public Internet, or IP Network 111 could also be a private Internet that is (i) not globally routable and (ii) only accessible to authorized modules and servers. As one example of a private IP Network 111, IP Network 111 could use private IP addresses for nodes on the network, and in this case IP Network 107 could be referred to as an intranet or private network. Alternatively, IP Network 111 could be a private network layered on top of the publicly routable Internet via secured and encrypted connections. The specific numbers for IP addresses and port numbers shown in Figure 1a and other figures are illustrative and any valid IP address or port number can be used, including an IPv4 and an IPv6 address. Server 105 within mobile network operator 104 can communicate with the module 101 using IP network 111,

Petitioner Samsung Ex-1004, 0356

where IP network 111 can comprise a private network that utilizes Internet Protocol standards. Module 101 can access the public Internet after authenticating with the server 105 associated with the MNO 104.

When operating in a wireless network configuration, module 101 can access the IP Network 111 via the wireless network 102. In the wireless network configuration, 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. Examples of wireless modules that utilize a wireless WAN such as, but not limited to, 2G and 3G networking technologies include the Motorola® G24-l and Huawei® MC323. Example manufacturers of wireless modules in 2012 include Sierra Wireless® and Telit®. Example leading manufacturers of mobile phones in 2013 include Apple® and Samsung®. In a wired configuration (not shown), module 101 can be a computer, security camera, security monitoring device, networked controller, etc. Module 101 can include a module identity 110, which can comprise a serial number or identity code in order to identify an individual, specific module 101 among a plurality of modules 101. A more detailed depiction of exemplary components of a module 101 is included in Figure 1b and Figure 1c below. Module 101 could also operate as a "smartcard" such that an end user presents module 101 to merchants for payments.

Wireless network 102 may comprise either a wireless local area network (LAN) or a wireless WAN such as a public land mobile network (PLMN). Examples for technologies used in wireless LANs include an 802.11 WLAN, Bluetooth, or Zigbee among other possibilities. Module 101 operating in wireless mode could communicate with a base station 103 of a wireless network 102 using a radio and an antenna. Wireless network 102 could operate as a Mode II device according to FCC Memorandum Opinion and Order (FC-12-36) and related white space regulation documents. If module 101 supports IEEE 802.15.4, then wireless network 102 could be a Zigbee network, an ISA100.11a standards-based network, or a 6LoWPAN network as described by IETF RFC 4944. Other possibilities exist as well for the wireless technology

utilized by a wireless network 102 and module 101, operating in a wireless mode, without departing from the scope of the present invention.

System 100 can include an eUICC subscription manager 109, where an eUICC subscription manager 109 can manage the recording and secure distribution of eUICC profiles 107c to a module 101. Example entities that could operate or control an eUICC subscription manager 109 include a manufacturer of module 101, an M2M service provider that manages the operation of module 101, or possibly a mobile network operator 104 could operate the eUICC subscription manager 109. Other entities could operate as an eUICC subscription manager 109 as well. An exemplary eUICC subscription manager 109 is described in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. An eUICC subscription manager 109 can also use a server 105 and record private keys and public keys for the server/subscription manager operation (including exemplary keys depicted and described in connection with Figure 2d below).

In exemplary embodiments, eUICC subscription manager 109 can use an eUICC profile key 107b to cipher portions of an eUICC profile 107c, such that only module 101 with the same eUICC profile key 107b could reasonably decipher the portions of the eUICC profile 107c. In this manner, the eUICC profile 107c can remain reasonably secured. The eUICC subscription manager 109 can share the eUICC profile key 107b in several different ways, including (i) pre-sharing the eUICC profile key 107b, or (ii) the eUICC subscription manager 109 sending the eUICC profile key 107b to the eUICC 107 using an asymmetric ciphering algorithm 219 as depicted and described in connection with Figure 2e below. An eUICC profile 107c can include an eUICC profile identity 107e in order to identify a profile among a plurality of eUICC profiles 107c. An eUICC subscription manager 109 can include an address 109a. The address 109a could comprise a domain name, such that a domain name system (DNS) or secure DNS (DNSSEC) query could resolve the name into an IP address in order for module 101 to communicate with the eUICC subscription manager 109. Or the address 109a could comprise an

Petitioner Samsung Ex-1004, 0358

Internet Protocol (IP) address, and the address 109a could include or be associated with a port number, such as port number 443 for data that utilizes transport layer security.

An eUICC 107 within module 101 can comprise an embedded universal integrated circuit card (eUICC) 107. An eUICC 107 can provide the equivalent functionality as a physical UICC, where definitions for a physical UICC are included in ETSI TR 102 216 and ETSI TS 102 221 V11.0.0, and other examples for the use of a physical UICC in mobile phones and M2M modules exist as well. An eUICC 107 in Figure 1a can support exemplary requirements for an eUICC outlined in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. In other words, an eUICC 107 can operate as a "virtualized" UICC, such that data operations and input/output to a physical UICC can be provided by an eUICC 107. Exemplary details of a conventional, physical UICC for authenticating a module 101 (which can be "virtualized in an eUICC 107) are depicted and described in connection with Figure 1d below. An eUICC 107 can include an eUICC identity 107a, such that an eUICC subscription manager 109 can select and identify the eUICC 107 among a plurality of eUICCs 107. The eUICC 107 can also record an eUICC profile key 107b and an eUICC profile 107d. Profile 107d can represent a profile that is partially decrypted using the eUICC profile key 107b, as depicted and described in connection with Figure 2a below. Additional exemplary details for the operation of an eUICC 107 within module 101 are also provided in Figure 1b, Figure 1c, Figure 1e, and Figure 1f below.

According to an exemplary embodiment, an eUICC 107 can be recorded and operate within a "eUICC supporting" physical universal integrated circuit card (UICC) 108 within module 101. This "eUICC supporting", physical UICC 108 can include a processing unit, RAM memory, ROM memory, EEPROM memory, a bus, and a physical interface (not shown in Figure 1a, but described in Figure 1b). An exemplary processing unit, RAM memory, ROM memory, EEPROM memory, and bus are depicted and described in connection with Figure 1b below. The physical interface for an UICC 108 is depicted and described in connection with Figure 1d below. The "eUICC supporting" physically UICC 108 can perform all of the functions of an

Petitioner Samsung Ex-1004, 0359

eUICC 107, including (i) receiving and recording profiles 107d, (ii) receiving and recording eUICC profile keys 107b, (iii) recording an eUICC identity 107e, (iv) decrypting an eUICC profile 107c into an eUICC profile 107d as depicted and described in connection with Figure 2a below, (v) recording a set of network parameters 201 (in Figure 2a below) for module 101 to connect with wireless network 102, and (vi) recording keys such as a key K for conducting a message digest authentication with wireless network as depicted and described in Figures 1d, Figure 1e, and Figure 3 below. An "eUICC supporting" physical UICC 108 can include a physical electrical interface of ISO/IEC 7816-3 in order to support existing physical slots for UICCs. The use of an "eUICC supporting" physical UICC 108 is optional, and can be omitted. In this case (where "eUICC supporting" physical UICC 108 is omitted), the eUICC 107 can operate as a program within module 101 as depicted and described in connection with Figure 1b below, and the eUICC 107 would not reside within the "eUICC supporting" physical UICC 108.

The physical form-factor for an "eUICC supporting" UICC 108 could be identical to a UICC, and a difference between the two may not even be apparent upon visual inspection without special markings on the card. The physical form-factor for an "eUICC supporting" UICC 108 could comprise a "micro-SIM" or a "nano-SIM" as defined in ETSI TS 102 221 V11.0.0, which is herein incorporated by reference. When the module 101 detects a "eUICC supporting" UICC 107, the module 101 could send received eUICC profiles 107c to the "eUICC supporting" UICC 107, and also select, deselect, activate, and deactivate the different received eUICC profiles 107d recorded in the "eUICC supporting" UICC 108. When a module 101 detects that a regular UICC (i.e. not an "eUICC supporting " UICC 108) has been loaded into a slot for UICCs within the module, the module 101 could access the UICC in a regular manner implemented by mobile phones and modules for connecting to existing wireless networks in 2013, such as LTE or 3G networks. This use of conventional technology for a physical UICC is depicted and described in connection with Figure 1d below.

A module 101 can be associated with a user 113 or an M2M service provider 115. A user 113 could be a subscriber to mobile phone services provided by the mobile network operator

Petitioner Samsung Ex-1004, 0360

104. In this case, the user could be an individual and the module 101 could comprise a mobile phone with a telephone number, an email client, and a web browser (in addition to other, standard functionality for a mobile phone). The user 113 could periodically charge the module 101 (which can comprise a mobile phone), such as typically at night and carry the module 101 during the day in order to place calls and send/receive data. Thus, the user 113 may typically be physically close to a mobile phone as module 101, but an M2M service provider 115 can be associated with module 101 but may not be physically close to module 101. For embodiments where module 101 is associated with M2M communications, such as including a sensor to collect data regarding a monitored unit, the module 101 can be associated with an M2M service provider 115. In this case, the M2M service provider 115 can be a company or a division or department within a larger company that is associated with a plurality of modules 101 for collecting data using sensors and sending the data to a server similar to server 105. The M2M service provider 115 may operate the server similar to server 105 in order to automatically collect data from the plurality of modules 101. The server for the M2M service provider 115 could communicate with module 101 using the IP network 111 and the wireless network 102 when module 101 is connected to the wireless network 102.

Other configurations besides the one illustrated in Figure 1a are possible as well. In many common commercial relationships for the operation of mobile phone service in the United States in 2013, wireless network 102 could represent a portion of the radio access network used by a mobile network operator 104. MNO 104 could outsource portions of the operation and maintenance of a radio access network, such as a wireless network 102, to 3rd parties. In this configuration, wireless network 102 could represent a network operated by a first company specializing in the operation of radio towers and BTS equipment. This first company could be contracted with the mobile network operator 104 in order to support mobile phone service or data services to modules 101.

In addition, server 105 could reside within wireless network 102 in a data center managed by wireless network 102. Wireless network 102 could also operate as an eUICC subscription

Petitioner Samsung Ex-1004, 0361

manager 109. Although a single module 101, server 105, wireless network 102, and mobile network operator 104 are illustrated in Figure 1a, system 100 could comprise a plurality of each of these elements. Module 101 could also record sensor data pertaining to a monitored unit (not shown). Module 101 could be mobile, such as physically attached to a truck or a pallet, and module 101 could connect to a series of different wireless networks 102 or base stations 103 as module 101 moves geographically. Other configurations are possible as well for the elements illustrated in Figure 1a without departing from the scope of the present invention.

Figure 1b

Figure 1b is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments. Figure 1b is illustrated to include many components that can be common within a module 101, and module 101 may also operate in a wireless configuration in order to connect with a wireless network 102. In a wireless configuration, the physical interface 101a of module 101 may support radio-frequency (RF) communications with networks including a wireless network 102 via standards such as, but not limited to, GSM, UMTS, mobile WiMax, CDMA, LTE, LTE Advanced, and/or other mobile-network technologies. In a wireless configuration, the physical interface 101a may also provide connectivity to local networks such as, but not limited to, 802.11 WLAN, Bluetooth, or Zigbee among other possibilities. In a wireless configuration, module 101 could use a physical interface 101a be connected with both a wireless WAN and wireless LAN simultaneously. In a wired configuration, the physical interface 101a can provide connectivity to a wired network such as, but not limited to, through an Ethernet connection or USB connection. As contemplated herein, a physical interface 101a can include a network interface (such as a radio or an Ethernet port), such that module 101 can use the network interface in order to connect with a network and communicate with the network. A network interface can also comprise a physical interface 101a as contemplated herein.

Petitioner Samsung Ex-1004, 0362

The physical interface 101a can include associated hardware to provide the connections such as, but not limited to, radio-frequency (RF) chipsets, a power amplifier, an antenna, cable connectors, etc., and additional exemplary details regarding these components are described below in Figure 1c. Device driver 101g can communicate with the physical interfaces 101a, providing hardware access to higher-level functions on module 101. Device drivers 101g may also be embedded into hardware or combined with the physical interfaces 101a. Module 101 may preferably include an operating system 101h to manage device drivers 101g and hardware resources within module 101. The operating systems described herein can also manage other resources such as, but not limited to, memory and may support multiple software programs operating on module 101 at the same time.

The operating system 101h can include Internet protocol stacks such as, but not limited to, a User Datagram Protocol (UDP) stack, Transmission Control Protocol (TCP) stack, a domain name system (DNS) stack, etc., and the operating system 101h may include timers and schedulers for managing the access of software to hardware resources. The operating system shown of 101h can be appropriate for a low-power device with limited memory and CPU resources (compared to a server 105). An example operating system 101h for module 101 includes Linux, Android® from Google®, Windows® Mobile, or Open AT® from Sierra Wireless®. Additional example operating systems 101h for module 101 include eCos, uC/OS, LiteOs, and Contiki, and other possibilities exist as well without departing from the scope of the present invention.

A module program 101i may be an application programmed in a language such as, but not limited to, C, C++, Java, and/or Python, and could provide functionality to support regular mobile phone functionality. The module program 101i could include a network application 101x, where network application 101x comprises the user equipment protocol for accessing and communicating with the wireless network 102. For embodiments where module 101 connects with a wireless network 102 comprising an LTE network, the network application 101x can receive, process, and send signals with the wireless network 102 for user equipment messages in

Petitioner Samsung Ex-1004, 0363

ETSI TS 136 331 v.10.7 entitled “LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification”, which is herein incorporated by reference. In other words, network application 101x can comprise software for accessing and communicating with the wireless network 102. Although network application 101x is depicted in Figure 1b as operating as software within RAM memory 101e, the network application 101x could be included in firmware or a processor or application associated with a radio 101z (described in Figure 1c). Exemplary messages sent and received by a network application 101x are also depicted and described in connection with Figure 3 below.

A module program 101i could also include software for M2M applications such as, but not limited to, remote monitoring of sensors and remote activation of actuators. Module program 101i could also include a software routine, subroutine, linked library, or software module, according to one preferred embodiment. As contemplated herein, a module program 101i can include an application operating within a smartphone, such as, but not limited to, an iPhone® or Android®-based smartphone, and in this case module 101 could comprise a smartphone. The application functioning as a module program 101i could be downloaded from an “app store” associated with the smartphone. A set of device drivers 101g could include an eUICC driver 129, such that a network application 101x or other software or firmware within module 101 communicating with the eUICC 107 could send and receive data with the eUICC driver 129. Additional details regarding an exemplary eUICC driver 129 are depicted and described in connection with Figure 1e below.

Many of the logical steps for operation of module 101 or eUICC 107 can be performed in software and hardware by various combinations of physical interface 101a, device driver 101g, operating system 101h, and a module program 101i. As depicted in Figure 1b, module program 101i can include an eUICC 107 and a network application 101x. When module 101 or eUICC 107 is described herein as performing various actions such as acquiring an IP address, connecting to the wireless network, monitoring a port, transmitting a packet, sending a message, receiving a response, or encrypting or signing data, specifying herein that module 101 or eUICC

Petitioner Samsung Ex-1004, 0364

107 performs an action can refer to software, hardware, and/or firmware operating within module 101 illustrated in Figure 1b or Figure 1c performing the action.

Note that module 101 may also optionally include user interface 101j which may include one or more devices for receiving inputs and/or one or more devices for conveying outputs. User interfaces are known in the art and thus user interfaces are not described in detail here. User interface 101j could comprise a touch screen if module 101 operates as a smartphone or mobile phone. For embodiments where module 101 comprises a module for M2M applications and is associated with an M2M service provider 115, then module 101 can optionally omit a user interface 101j, since no local user 113 input may be required for many M2M applications, although a user interface 101j could be included with module 101. For embodiments where module 101 comprises a mobile phone and is associated with a user 113, the user interface 101j could comprise a touch screen on the front of a mobile phone.

Module 101 may be a computing device that includes computer components for the purposes of collecting data from a sensor 101f or triggering an action by an actuator 101y. Module 101 may include a central processing unit (CPU) 101b, a random access memory (RAM) 101e, and a system bus 101d that couples various system components including the random access memory 101e to the processing unit 101b. The system bus 101d may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures including a data bus. Note that the computer components illustrated for the module 101 in Figure 1b may be selected in order to minimize power consumption and thereby maximize battery life, if module 101 includes a battery and is not attached to external power. In addition, the computer components illustrated for the module 101 in Figure 1b may also be selected in order to optimize the system for both long periods of sleep or idle states relative to active communications and also may be optimized for predominantly uplink (i.e. device to network) communications with small packets or messages. The computer components illustrated for the module 101 in Figure 1b may also be general-

Petitioner Samsung Ex-1004, 0365

purpose computing components, and specialized components may not be required in order to utilize many of the embodiments contemplated herein.

Module 101 may include a read-only memory (ROM) 101c which can contain a boot loader program. Although ROM 101c is illustrated as “read-only memory”, ROM 101c could comprise long-term memory storage chipsets or physical units that are designed for writing once and reading many times. As contemplated within the present invention, a read-only address could comprise a ROM 101c memory address or another hardware address for read-only operations accessible via bus 101d. Changing data recorded in a ROM 101c can require a technician have physical access to module 101, such as, but not limited to, removing a cover or part of an enclosure, where the technician can subsequently connect equipment to a circuit board in module 101, including replacing ROM 101c. ROM 101c could also comprise a nonvolatile memory, such that data is stored within ROM 101c even if no electrical power is provided to ROM 101c. Although not illustrated in Figure 1b, but illustrated in Figure 1c below, module 101 could also include a flash memory 101w. Module program 101i, network application 101x, operating system 101h, eUICC 107, or device drivers 101g could be stored in flash memory 101w within module 101 when the module is powered off. These components and/or instructions could be moved from a flash memory 101w (not shown in Figure 1b but shown in Figure 1c) into RAM 101e when the module is powered on by a bootloader program recorded in the ROM 101c. Note that ROM 101c could be optionally omitted or included in a memory unit within CPU 101b (not shown).

Although the exemplary environment described herein employs ROM 101c and RAM 101e, it should be appreciated by those skilled in the art that other types of computer readable media which can store data that is accessible by a module 101, such as, but not limited to, memory cards, subscriber identity module (SIM) cards, local miniaturized hard disks, and the like, may also be used in the exemplary operating environment without departing from the scope of the invention. The memory and associated hardware illustrated in Figure 1b provide nonvolatile storage of computer-executable instructions, data structures, program modules,

Petitioner Samsung Ex-1004, 0366

module program 101i, and other data for computer or module 101. Note the module 101 may include a physical data connection at the physical interface 101a such as, but not limited to, a miniaturized universal serial bus adapter 101v (illustrated in Figure 1c), firewire, optical, or other another port.

The computer executable instructions such as, but not limited to, module program 101i, network application 101x, eUICC 107, operating system 101h, or device driver 101g can be initially loaded into memory such as, but not limited to, ROM 101c or RAM 101e through the physical interface 101a before module 101 is given to an end user, shipped by a manufacturer to a distribution channel, or installed by a technician. In addition, the computer executable instructions such as, but not limited to, module program 101i, network application 101x, operating system 101h or device driver 101g could be transferred wirelessly to module 101. In either case (wired or wireless transfer of computer executable instructions), the computer executable instructions such as module program 101i, network application 101x, operating system 101h, or device driver 101g could be stored remotely on a disk drive, solid state drive, or optical disk (external drives not shown).

A number of program modules may be stored in RAM 101e, ROM 101c, or possibly within CPU 101b, including an operating system 101h, device driver 101g, an http client (not shown), a DNS client, and related software. Further, the module program 101i and/or network application 101x can perform the various actions described in the present invention for the module 101 through instructions the module program 101i and/or network application 101x provide to the CPU 101b. A user may enter commands and information into module 101 through an optional user interface 101j, such as a keypad, keyboard (possibly miniaturized for a mobile phone form-factor), and a pointing device. Pointing devices may include a trackball, an electronic pen, or a touch screen.

The module 101, comprising a computer, may operate in a networked environment using logical connections to one or more remote computers, such as the server 105 illustrated in Figure 1a. Server 105 can also function as a general purpose server to provide files, programs, disk

Petitioner Samsung Ex-1004, 0367

storage, remote memory, and other resources to module 101 usually through a networked connection. Additional remote computers with which module 101 communicates may include another module 101 or mobile device, an M2M node within a capillary network, a personal computer, other servers, a client, a router, a network PC, a peer device, a base station 103, or other common network node. It will be appreciated that the network connections shown throughout the present invention are exemplary and other means of establishing a wireless or wired communications link may be used between mobile devices, computers, servers, corresponding nodes, and similar computers. Although a single module program 101i is depicted in Figure 1b, module 101 could include a plurality of module programs 101i.

The module program 101i, eUICC 107, and network application 101x operating within module 101 illustrated in Figure 1b can provide computer executable instructions to hardware such as CPU 101b through a system bus 101d in order for a module 101 to (i) connect with a wireless network 102, (ii) authenticate with a mobile network operator 104 associated with the wireless network 102, and (iii) send or receive packets with a server 105 or a server associated with an eUICC subscription manager 109. The module program 101i and/or network application 101x can enable the module 101 or eUICC 107 to transmit or send data from the eUICC 107 or module 101. The eUICC 107 or module 101 can send data by recording data in memory such as RAM 101e, where the data can include cryptographic data such as a RAND and RES values, a destination IP:port number, a packet or packet header value, an encryption or ciphering algorithm and key, a digital signature algorithm and key, etc. The data recorded in RAM 101e can be subsequently read by the operating system 101h or the device driver 101g. The operating system 101h or the device driver 101g can write the data to a physical interface 101a using a system bus 101d in order to use a physical interface 101a to send data to the wireless network 102 and IP network 111 using a radio 101z (shown in Figure 1c). Alternatively, the module program 101i and/or network application 101x can write the data directly to the physical interface 101a using the system bus 101d.

The module program 101i, eUICC 107, network application 101x, and/or operating system 101h can include steps to process the data recorded in memory such as, but not limited to, encrypting data, selecting a destination address, or decrypting ciphertext data. The data recorded in memory could also include an eUICC profile 107c or eUICC profile 107d, as described in Figure 1a above and Figure 2a below. The eUICC profiles 107d can include instructions and data for connecting with wireless network 102, including network parameters and network access credentials. The module 101 can use the physical interface 101a such as, but not limited to, a radio to transmit or send the data associated with a profile 107d to a base station 103. For those skilled in the art, other steps are possible as well for a module program 101i or operating system 101h to communicate with a wireless network 102 using data associated with an UICC (where an eUICC 107 records data normally associated with a physical UICC) without departing from the scope of the present invention.

Conversely, in order for module 101, network application 101x, or eUICC 107 to receive a packet or message from MNO 104 or wireless network 102, the physical interface 101a can use a radio to receive data from a base station 103. The received data can include information from MNO 104 and may comprise a datagram, a source IP:port number, a packet or header value, an instruction for module 101, an acknowledgement to a packet that module 101 sent, a digital signature, and/or encrypted data. The received data can also include radio resource control (RRC) messages, and related layer 1 and layer 2 access and control messages for module 101 to access the wireless network 102. The operating system 101h or device driver 101g can use a system bus 101d and CPU 101b to record the received data in memory such as RAM 101e, and the module program 101i or operating system 101h may access the memory in order to process the received data and determine the next step for the module 101 after receiving the data. The steps within this paragraph may also describe the steps a module program 101i, eUICC 107, or network application 101x can perform in order to receive a message from wireless network 102 that includes a RAND value. For those skilled in the art, other steps are possible as well for a module program 101i, network application 101x, module 101, and/or eUICC 107 to receive a

Petitioner Samsung Ex-1004, 0369

message from a mobile network operator 104 or wireless network 102 within the scope of the present invention.

Module program 101i can include an eUICC 107, which can provide the functionality or CPU 101b instructions for module 101 to access data normally within a physical UICC, such as network parameters and network access credentials. An eUICC 107 as illustrated in Figure 1a and Figure 1b can be implemented within module 101 in several different ways, including (i) as depicted in Figure 1b a module program 101i stored in RAM 101e during operation, but also recorded in a nonvolatile memory, such as, but not limited to, either flash memory 101w (described in Figure 1c) or ROM 101c at other times than normal operation (such as during periods of power off), (ii) firmware within CPU 101b or another specialized processing unit within module 101, (iii) an "eUICC supporting" physical UICC 108 within module 101 that contains the eUICC 107, or (iv) a specialized circuit within a surface mount package that is soldered directly onto a circuit board of the module 101, including an 8-lead small outline non-leaded (SON-8) package. For the embodiment where an eUICC 107 comprises a module program 101i, the eUICC 107 could be loaded and installed within nonvolatile memory 101w in module 101 using the steps and procedures described for a module program 101i in Figure 1b. Other possibilities exist as well for the physical implementation of an eUICC 107 within a module 101 without departing from the scope of the present invention. An eUICC 107 may also be referred to as an "electronic UICC", an "electronic SIM" (eSIM), or an "embedded SIM" (also eSIM).

For embodiments where an eUICC 107 can be loaded into a RAM 101e or flash 101w memory, a CPU 101b could designate the RAM 101e or flash 101w memory containing the instructions or data for an eUICC 107 to be a protected memory. When (i) loaded with appropriate data (such as, but not limited to a eUICC profile 107d described in Figure 2a below), and (ii) a profile for a MNO 104 is selected and activated, then an eUICC 107 can provide the equivalent functionality of a physical UICC. The eUICC 107, using an activated eUICC profile 107d, can provide the module 101 with (i) network access credentials 202 and 203, and (ii)

Petitioner Samsung Ex-1004, 0370

network parameters 201 in order to connect with wireless network 102. The eUICC 107, using an activated eUICC profile 107d, can record a first key K 203 (described in Figures 2a and 3 below) and also a first network module identity 202. The eUICC 107 can support standard steps by module 101 for network authentication contemplated in 3GPP TS 33.401 V12.9.0 and related standards, including inputting a RAND value into the eUICC 107 and outputting a RES value.

Moreover, those skilled in the art will appreciate that the present invention may be implemented in other computer system configurations, including hand-held devices, netbooks, portable computers, multiprocessor systems, microprocessor based or programmable consumer electronics, network personal computers, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments, where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices. In addition, the terms “mobile node”, “mobile station”, “mobile device”, “M2M module”, “M2M device”, “networked sensor”, “industrial controller”, or “user equipment” can also refer to module 101 or its functional capabilities. Other possibilities exist as well for the configuration or combination of components illustrated in Figure 1b without departing from the scope of the present invention.

Figure 1c

Figure 1c is a graphical illustration of components within a module, in accordance with exemplary embodiments. Figure 1c is illustrated to show a combination of components useful for leveraging the efficient and secure communication techniques described in the present invention. In addition to the components illustrated in Figure 1b above, module 101 can include a an eUICC 107, a battery 101k, a MNO public key 502, a wireless module private key 112a, a connection to an actuator 101y, a USB interface 101v, a CPU wake controller 101u, a flash memory 101w, a symmetric key 127, a random number generator 128, cryptographic algorithms 141, a radio 101z, and other components illustrated in Figure 1c. Not all of the components

Petitioner Samsung Ex-1004, 0371

illustrated in Figure 1c are required for many exemplary embodiments, and some of the components illustrated in Figure 1c may also be optionally omitted in some exemplary embodiments.

The CPU 101b can comprise a general purpose processor appropriate for the low power consumption requirements of a module 101, and may also function as a microcontroller. CPU 101b could be a processor with an ARM® core, or possibly an ATOM® core or processors, and other possibilities exist as well. The CPU 101b can include registers, a cache memory, and arithmetic logic units. Clock 160 can comprise a crystal oscillator generating sine or square wave outputs at a frequency to drive a system bus 101d, CPU 101b, and RAM 101e, in addition to other functionality. In exemplary embodiments, clock 160 can comprise a temperature-compensated crystal oscillator (TCXO), a voltage-controlled crystal oscillator (VCXO), or a voltage-controlled temperature-compensated crystal oscillator (VCTCXO), and other possibilities exist as well. Clock 160 could include circuits and logic to keep time while module 101 is both in an active state and a dormant state.

Sensor 101f could be a device to collect environmental data or data regarding (i) a monitored unit for M2M applications or (ii) user 113 for applications where module 101 comprises a mobile phone and user 113 is an individual person such as a mobile phone subscriber. Sensor 101f could collect data such as, but not limited to, temperature, humidity, pressure, visible light levels, radiation, shock and/or vibration, voltage, current, weight, pH levels, orientation/motion, or the presence of specific chemicals. Sensor 101f could also be a microphone. Sensor 101f could be a magnetic strip reader for credit cards and similar cards, or an antenna for either near-field RF communications, such as, but not limited to, reading an RF identity tag. An antenna for a sensor 101f could also collect longer-range RF signals, such as, but not limited to, reading long-range radio frequency identity tags. Sensor 101f could also collect biometric data such as, but not limited to, heart rate, glucose levels, body temperature, or other health measurements for a user 113. The sensor 101f can provide data to the CPU 101b in the form of analog or digital data, which can be communicated via a system bus 101d or physical

Petitioner Samsung Ex-1004, 0372

interface 101a and other electrical interfaces are possible as well. A sensor measurement can comprise the analog or digital data collected by CPU 101b from sensor 101f.

A sensor measurement from sensor 101f can include processing of the analog or digital data input CPU 101b by sensor 101f, such as, but not limited to, averaging over time, using mathematic formulas to convert the raw data from sensor 101f into a usable form. Module 101 may also collect sensor data or sensor values using a sensor 101f and CPU 101b, where the data or values are derived from electrical signals output by a sensor 101f. A sensor measurement can comprise the sensor data or sensor values. If module 101 comprises a "point of presence" payment terminal, then a sensor measurement could comprise data read from a payment card. As contemplated herein, the terms "sensor measurement" and "sensor data" can be used interchangeably, and can also be considered functionally equivalent. Although a single sensor 101f is shown in Figure 1c, a module 101 could include multiple sensors. Each of the multiple sensors 101f could include a sensor identity 151, which could comprise a number or string to identify the sensor 101f. A sensor 101f could be external to module 101, and also a plurality of sensors 101f may be used and they also can connect to module 101 when module 101 uses radio 101z as a base station for a WiFi network.

Actuator 101y could be a device to control a parameter or state for a monitored unit in M2M applications for module 101, such as, but not limited to, changing a voltage or current, activating a switch or relay, turning on or off a microphone or speaker, activating or deactivating a light, and other examples are well known in the art. Actuator 101y could also be a speaker. Actuator 101y could be controlled by module 101 via a digital or analog output from CPU 101b, which could also be transmitted or sent via system bus 101d or a physical interface 101a. Although actuator 101y is illustrated as external to wireless module 101 in Figure 1c, actuator 101y could also be internal to module 101, and module 101 could include multiple actuators 101y. A module 101 could include multiple actuators 101y each with an actuator identity 152. Sensors and actuators are well known to those of ordinary skill in the art, and thus are not described in additional detail herein.

Petitioner Samsung Ex-1004, 0373

Module 101 can include a Universal Serial Bus (USB) interface 101v. In accordance with an exemplary embodiment, module 101 can comprise a wireless module and include a radio 101z. Note that the use of a radio 101z is not required for module 101, which could also obtain a connection to the IP Network 111 via a wired line such as Ethernet. Although not illustrated, radio 101z could include antennas for reception and transmission of RF signals, and even multiple antennas could be used. Although a single radio 101z is illustrated in module 101, module 101 could also contain multiple radios 101z. Radio 101z can support wireless LAN standards such as, but not limited to, WiFi, Bluetooth, and Zigbee, or similar wireless LAN standards. Note that module 101 may also operate as a base station in a wireless LAN, such as, but not limited to, an 802.11 base station. When module 101 operates a wireless LAN, radio 101z can function as either a client/node and/or a base station 103 to support communication from other wireless nodes in physical proximity, such as, but not limited to, other nodes within an exemplary 50 meters. The other wireless nodes could comprise a sensor 101f and/or actuator 101y, and in this case a sensor could be referred to as a "networked sensor" and an actuator could be referred to as a "networked actuator".

In accordance with exemplary embodiments, module 101 can store module private key 112a, MNO public key 502, and module identity 110, and a symmetric key 127 in memory/RAM 101e during operation, such as when CPU 101b is active and the module 101 is connected to a network such as a wireless network 102 during data transmissions. Module private key 112a preferably is recorded in nonvolatile memory such as, but not limited to, flash memory 101w, so that module 101 has access to its private key 112a after the private key has been derived or loaded, including times when a battery 101k has been fully drained or removed from module 101 (if module 101 does not utilize a persistent power source such as land-line power). Symmetric key 127 can be a secure, shared private key for use with symmetric encryption or symmetric ciphering algorithms 211 (in Figure 2c below). Symmetric key 127 may also include an expiration time 133, such that symmetric key 127 may only be used by module 101 and/or eUICC 107 during a limited period of time, such symmetric key 127 remaining only valid for a

Petitioner Samsung Ex-1004, 0374

day, or a week, or during a session (where the session comprises multiple messages and/or responses between a module 101 and a wireless network 102), etc.

Module identity 110 is preferably a unique identifier of module 101, and could comprise a number or string such as, but not limited to, a serial number, an international mobile subscriber identity number (IMSI), international mobile equipment identity (IMEI), or an Ethernet media access control (MAC) address. According to an exemplary embodiment, module identity 110 can also comprise a serial number or string that is written into hardware of module 101 upon manufacturing or distribution of module 101 (also depicted and described in connection with a step 511 in Figure 5b below). In this case, module identity 110 could be recorded in a read only memory 101c, where read only memory 101c could not be easily erased or otherwise tampered with. Read only memory 101c could also comprise a protected memory and the address for accessing the module identity 101 within the ROM 101c could comprise a protected address.

A protected address can comprise an address accessible to a CPU 101b and readable by CPU 101b where the data within the protected address is not modified, changed, or updated by a CPU 101b under normal operating conditions. Also note that the protected address can comprise one form of a nonvolatile memory, where a memory records data. In exemplary embodiments module identity 110 may preferably be permanently or persistently associated with the physical hardware of module 101, which can be helpful for the security procedures contemplated herein. Module identity 110 can function as a basic identifier for services from mobile network operator 104, eUICC subscription manager 109, wireless network 102, M2M service provider 115, or server 105 in order to properly identify module 101 among a plurality of modules. Module private key 112a and an associated module public key 112b could be unique to module 101 and uniquely associated with module identity 110, according to a preferred embodiment.

MNO public key 502 in module 101 could be obtained from downloading the key over the IP Network 111, or optionally also written into nonvolatile memory of module 101 upon manufacture or distribution. MNO public key 502 could be obtained using a domain name or Internet address that is recorded in nonvolatile memory upon the configuration of module 101,

Petitioner Samsung Ex-1004, 0375

such as, but not limited to, during installation or distribution, and module 101 could fetch the MNO public key 502 upon connecting to a wireless network 102 or other connection to the IP Network 111. Additional elements besides those depicted in Figure 1c could also be recorded in volatile memory 101e, which could comprise a RAM 101e. For example, cryptographic algorithms 141 could also be recorded in RAM 101e as well. Note that values and related data can also be recorded in both RAM 101e and nonvolatile memory 101w at the same time, such that data in nonvolatile memory 101w allows module 101 to access the data after a shutdown state, but moving the same data into RAM 101e during an active state allows module 101 to more quickly perform operations using a CPU 101b. Other possibilities exist as well for the storage location of various values and data elements illustrated in Figure 1c without departing from the scope of the present invention.

Module 101 may also contain cryptographic algorithms 141, which may comprise a suite of algorithms or subroutines that can be utilized for (i) deriving a pair of keys comprising a public key and a private key, (ii) encrypting data using public keys, (iii) decrypting data using private keys, (iv) processing secure hash signatures using private keys, and (v) verifying secure hash signatures using public keys, and related software, firmware, or subroutines for implementing a cryptographic system, including symmetric ciphering algorithms. Cryptographic algorithms 141 could utilize publicly available software libraries within tools such as, but not limited to, OpenSSL maintained by The OpenSSL Project (http://www.openssl.org/), libgcrypt maintained by The Free Software Foundation (http://www.gnu.org/software/libgcrypt/), and similar libraries such as, but not limited to, libmcrypt and Crypto++. Note that cryptographic algorithms 141 could also use proprietary cryptographic libraries as well. In addition to implementing asymmetric encryption/ciphering, such as, but not limited to, used with RSA and ECC cryptography, cryptographic algorithms 141 can provide symmetric ciphering where a shared private key is utilized to both encrypt and decrypt, such as, but not limited to, with the Advanced Encryption Standard (AES) cipher suite.

Petitioner Samsung Ex-1004, 0376

As illustrated in Figure 1c, module 101 may also contain a random number generator 128. Random number generator 128 may contain a seed 128b. The creation of random numbers with a high degree of entropy may be important the use of cryptographic algorithms 141. 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 101f 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). Note that values or data for each of the elements listed in the previous sentence could be utilized in a "module random seed file" instead of or in addition to a state. The use of a "module random seed file" with a random number generator 128 is also depicted and described in connection with Figure 1d of U.S. Patent Application Serial No. 14/084,141, filed November 19, 2013 in the name of John Nix, which is hereby incorporated by reference in its entirety.

Figure 1d

Figure 1d is a graphical illustration for authenticating with a wireless network using a physical UICC, in accordance with conventional technology. Figure 1d illustrates the components and interfaces for using a physical UICC in order to a module 101 conduct an authentication with a wireless network 102 according to wireless WAN standards which use a pre-shared secret key K recorded in the physical UICC 116. The wireless network could be an LTE, LTE Advanced, or a 3G network, and also based on related standards. With a 3G network, the pre-shared secret key K is also known as "Ki". The module 101 can include a network application 101x, a UICC driver 114, and a physical interface supporting the ISO/IEC 7816-3 electrical standards, such as the third edition published on November 1, 2006. The physical UICC 116 can be a smart card in the form factor of a mini-SIM, micro-SIM, or nano-SIM, connected to the physical interface such as ISO/IEC 7816-3 and related electrical standards. The physical interface can include six electrical contacts known as C1 through C6, where C1 provides a power supply to the physical UICC 116, C2 provides a reset signal input, C3 provides

Petitioner Samsung Ex-1004, 0377

a clock signal input, etc. The network application 101x can comprise software or firmware for the module 101 to communicate with the wireless network 102 using the standards that include layer 2 messages between module 101 and wireless network 102 such as, but not limited to, radio resource control (RRC) messages, security mode commands, ciphering, and authentication. The network application 101x can communicate with a radio 101z (described in Figure 1c) using the system bus 101d.

A network application 101x in a Figure 1d can be similar or equivalent to a network application 101x depicted and described in connection with Figure 1b. The UICC driver 114 can comprise a driver within a set of drivers 101g within module 101, where drivers 101g are also depicted and described in connection with Figure 1b. A physical UICC 116 can support other and additional functionality for a module 101 than the authentication functionality depicted in Figure 1b, such as, but not limited to, (i) recording a set of network parameters equivalent to a set of network parameters 201 in Figure 2a below in order to module 101 to identify and select a wireless network 102, (ii) recording an address book with a list of phone numbers for user 113, (iii) recording a list of recent SMS messages and telephone numbers dialed, and/or (iv) recording and implementing a personal identification number (PIN) in order for a user 113 to authenticate and access the module 101 with the UICC 116, and other functionality of a physical UICC 116 is possible as well. The physical UICC 116 can also include (i) an IP Multimedia Services Identity Module (ISIM) application and data and/or a (ii) Universal Subscriber Identity Module (USIM) application for the module 101 to utilize when communicating with the wireless network 102.

After power-up of the module 101 from a powered off state, the module 101 can use the UICC driver 114 to read data from the physical UICC 116 such as a set of network parameters 203 (depicted in Figure 2a below) as well as an IMSI or equivalent value as a network module identity. The set of network parameters 203 or IMSI in a physical UICC 116 may not be encrypted (or associated with an eUICC profile 107d) and the set of network parameters can be directly read by the UICC driver 114. The module 101 can use the set of network parameters to tune a radio 101z to particular frequencies for the wireless network 102 and search for a beacon

Petitioner Samsung Ex-1004, 0378

signal from a base station 103. The beacon signal can include codes such as a mobile country code (MCC) and mobile network code (MNC) that can match values in either the network parameters or IMSI. Upon finding and selecting a base station 103, the module 101 can send a random access channel (RACH) message and subsequently an identity value recorded in the physical UICC 116 such as an IMSI, temporary mobile subscriber identity (TMSI), a globally unique temporary identity (GTUI), or a similar value to identify the module 101 using the physical UICC 116 with the wireless network 102.

In order to authenticate a module 101 with the wireless network 102, the wireless network 102 can record a set of authentication tokens or vectors associated with a network identity sent by the module 101, such as a GTUI value. An authentication vector 117 for the module's 101 network identity can comprise a vector or set of values that includes a random number (RAND) 118, response (RES) 119, a network authentication token (AUTN), and a sequence number. The value AUTN and sequence number is not shown in Figure 1d and subsequent figures such as Figure 1e and Figure 3, but the value AUTN and sequence number can be used by module 101 with a physical UICC 116 or eUICC 107 in order to authenticate the wireless network 102. The sequence number can prevent replay attacks and the AUTN value can comprise a digital signature or message digest value the physical UICC 116 or eUICC 107 can also calculate using the RAND 118 value in order for the module 101 to authenticate the wireless network 102. The values for the authentication vector 117 that includes a RAND 118 and a RES 119 can be calculated by a home subscriber server (HSS) for the mobile network operator 104 associated with the wireless network 102 and provided by the mobile network operator 104 to servers associated with the wireless network 102. An exemplary format for the use of a RAND 118 with a response RES 119 is described in ETSI standard TR 131 900 v.10.0.0 and related documents. Other possibilities exist as well for the format, structure, and data elements within an authentication vector 117 without departing from the scope of the present invention.

In order to conduct an authentication of module 101, after receiving a RACH message and the network module identity such as an IMSI, TMSI, or GTUI value, the wireless network

Petitioner Samsung Ex-1004, 0379

102 can send a RAND 118 from the authentication vector 117. The module 101 can receive the RAND 118 value using the network application 101x and the radio 101z. The network application 101x can send the RAND 118 value to the UICC driver 114, and the UICC driver 114 can send the RAND 118 value through the physical interface such as ISO/IEC 7816-3 to the physical UICC 116. After receiving the exemplary RAND 118 message, in order to conduct an authentication, module 101 using a physical UICC 116 could take steps to demonstrate to a wireless network 102 that the physical UICC 106 records the same pre-shared secret key K for the network module identity as recorded by a mobile network operator 104 associated with the wireless network 102. Physical UICC 116 can properly respond to the RAND 118 using message digest algorithms by calculating a secure hash value RES 119 using the RAND 118 and the recorded secret key K. The physical UICC 116 could use algorithms specified in ETSI TS 135 205 – 209, as well as subsequent and related standards, in order for the physical UICC 116 to calculate a secure hash value such as a RES 119. The calculation and processing of a RES 119 using a RAND 118 and a secret key K is also depicted and described in connection with steps 306 and 311 of Figure 3. Other possibilities exist as well for a physical UICC 116 or an eUICC 107 to calculate a RES 119 value using a RAND 118 and a secret key K without departing from the scope of the present invention.

After the calculation of a RES 119 value in response to the RAND 118, the physical UICC 116 can send the RES 119 to the UICC driver 114 through the physical interface such as ISO/IEC 7816-3. The device driver 114 can send the RES 119 value to the network application 101x and the network application 101x can send the RES 119 value to the wireless network 102 using a radio 101z and the base station 103. The wireless network 102 can take steps to compare the received RES 119 with a recorded RES 119 value in the authentication vector 117. If the received RES 119 matches the recorded RES 119 in the authentication vector 117 then the module 101 with the physical UICC 116 can be considered authenticated. The authentication of module 101 by wireless network 102 is also depicted and described in connection with a step 308a of Figure 3. After successful authentication, the module 101 and wireless network 102 can

Petitioner Samsung Ex-1004, 0380

then take subsequent steps for a module 101 to have access to the IP network 111 including the public Internet, as well as configuring services such as voice and SMS.

Figure 1e

Figure 1e is a graphical illustration for authenticating with a wireless network using an eUICC, in accordance with exemplary embodiments. A module 101 with an eUICC 107 can perform the equivalent steps for authentication with a wireless network 102, such that a module 101 can use an eUICC 107 instead of a physical UICC 116. The wireless network 102 can perform the same steps as (i) recording an authentication vector 117 from a mobile network operator 104 associated with the wireless network 102, (ii) receiving a RACH message and a network module identity such as a GTUI or TMSI from the module 101, (iii) sending values from the authentication vector 117 including a RAND 118, and (iv) receiving a RES 119 and comparing the received RES 119 with a recorded RES 119 in the authentication vector 117 in order to authenticate the module 101 using an eUICC 107 instead of a physical UICC 116. In other words, the use of an eUICC 107 by module 101 can be transparent to a wireless network 102, such that a module 101 with an eUICC 107 instead of a physical UICC 116 can be fully "backward compatible" with standards, software, and infrastructure deployed on a wireless network 102.

A module 101 in Figure 1e can include a network application 101x, an eUICC driver 129, an eUICC 107, and an operating system 101h. The network application 101x can be equivalent or similar to a network application 101x depicted and described in connection with Figure 1d and Figure 1b above. The use of an eUICC 107 instead of a physical UICC 116 within module 101 can also be transparent to network application 101x, via the use of eUICC driver 129. In other words, in exemplary embodiments, the same or equivalent network application 101x can be used for either (i) a module 101 with a physical UICC 116 or (ii) a module 101 with an eUICC 107, since the eUICC driver 129 can perform the identical input and output functions as a UICC driver 114 when communicating with the network application 101x. The use of an eUICC driver

Petitioner Samsung Ex-1004, 0381

129 is also depicted and described in connection with Figure 1b above. The eUICC driver 129 can communicate with the network application 101x using the operating system 101h. The internal communication between network application 101x and eUICC driver 129 using an operating system 101h could comprise sharing memory 101e, such that network application 101x writes messages such as, but not limited to, an exemplary RAND 118 value into the shared memory 101e and eUICC driver 129 reads the values from the shared memory 101e. In another embodiment, the internal communication between network application 101x and eUICC driver 129 using an operating system 101h could comprise using loopback UDP ports within operating system 101h, such that network application 101x sends a UDP datagram with the RAND 118 value using a first UPD loopback port, and the eUICC driver 129 receives the UDP datagram with the RAND 118 value using a second UDP loopback port. Similar steps could be taken as well for an eUICC driver 129 to send data such as a RES 119 to the network application 101x using the operating system 101h.

As illustrated in Figure 1e, eUICC driver 129 can also communicate with the eUICC 107 using the operating system 101h. Two differences between conventional technology illustrated in Figure 1d and the exemplary embodiment illustrated in Figure 1e include (i) the eUICC driver 129 communicates with the eUICC 107 using operating system 101h instead of a physical interface such as ISO/IEC 7816-3 and related electrical standards, and (ii) the eUICC 107 can operate as a separate program or application within memory 101e or memory 101w instead of a physically separate application operating on a physical UICC 116. The eUICC driver 129 can communicate with the eUICC 107 using the equivalent steps and procedures for an network application 101x to communicate with an eUICC driver 129 described in the paragraph above, including using shared memory or sending UDP loopback messages on internal UDP loopback ports. Other possibilities for the communication between eUICC driver 129 and eUICC 107 exist as well without departing from the scope of the present invention. In addition, although eUICC driver 129 and eUICC 107 are depicted in Figure 1e and Figure 1b as separate elements, programs, and/or processes for a module 101, the eUICC driver 129 could be optionally

Petitioner Samsung Ex-1004, 0382

combined with an eUICC 107 such that the network application 101x can communicate directly with the eUICC 107 using the operating system 101h.

The eUICC 107 can include an eUICC profile 107d which can contain the same information used by a physical UICC 116 in Figure 1d above, including a set of network parameters, a network module identity, and a key K. In other words, the data recorded in a eUICC 107 in the form of a profile 107d can allow and support the eUICC 107 in Figure 1e to operate in an equivalent manner as a physical UICC in Figure 1d for the authentication steps illustrated in Figure 1d and Figure 1e. Although not illustrated in Figure 1e, the eUICC 107 could also perform the similar or equivalent functions of a physical UICC including (i) recording a set of network parameters equivalent to a set of network parameters 201 in Figure 2a below in order to module 101 to identify and select a wireless network 102, (ii) recording an address book with a list of phone numbers for user 113, (iii) recording a list of recent SMS messages and telephone numbers dialed, and/or (iv) recording and implementing a personal identification number (PIN) in order for a user 113 to authenticate and access the module 101 with the eUICC 107. Other functionality of an eUICC 107 for a module 101 is possible as well without departing from the scope of the present invention.

As illustrated in Figure 1e, the network application 101x in module 101 can receive a RAND 118 value from wireless network 102 in order to authenticate the module 101. The network application 101x can send the RAND 118 value to the eUICC driver 129. The eUICC 107 can read a RAND 118 value from the network application 101x using the eUICC driver 129. After receiving the exemplary RAND 118 message, in order to conduct an authentication, module 101 using an eUICC 107 could take steps to demonstrate to a wireless network 102 that the module 101 records the same pre-shared secret key K for the network module identity as recorded by a mobile network operator 104 associated with the wireless network 102. eUICC 107 can properly respond to the RAND 118 using message digest algorithms by calculating a secure hash value RES 119 using the RAND 118 and the recorded secret key K from the profile 107d. The eUICC 107 could use algorithms specified in ETSI TS 135 205 – 209, as well as

Petitioner Samsung Ex-1004, 0383

subsequent and related standards, in order for the eUICC 107 to calculate a secure hash value such as a RES 119. The calculation and processing of a RES 119 using a RAND 118 and a secret key K for an eUICC 107 is also depicted and described in connection with steps 306 and 311 of Figure 3. Other possibilities exist as well for an eUICC 107 to calculate a RES 119 value using a RAND 118 and a secret key K, without departing from the scope of the present invention. As illustrated in Figure 1e, the eUICC 107 can send the RES 119 to the eUICC driver 129, and the eUICC driver 129 can send the RES 119 to the network application 101x. The network application 101x can then send the RES 119 to the wireless network 102, and the wireless network 102 could perform a step 308a as depicted and described in connection with Figure 3 in order to authenticate the module 101 using the eUICC 107 and profile 107d.

Figure 1f

Figure 1f is a graphical illustration of an exemplary system that includes a module, a mobile network operator, and an eUICC in accordance with exemplary embodiments. System 199 in Figure 1f can include a mobile network operator 104 and a module 101. The mobile network operator 104 can communicate with the module 101 using a wireless network 102, and the wireless network 102 could comprise the radio access portion of the mobile network operator 104, such as a collection of base stations 103 using licensed radio spectrum such as, but not limited to, the 700 Mhz band for LTE, and other possibilities exist as well for the wireless network 102. The mobile network operator 104 can include a server 105 with an IP address 106a. The server 105 with MNO 104 in Figure 1f can comprise a Mobility Management Entity (MME) in LTE networks, or equivalent functionality to receive authentication requests from modules 101 with other wireless wide-area networking technology. The MME can support radio bearer activation/deactivation processes for the module 101 and authenticating the module 101 by recording an authentication vector 117, where the authentication vector 117 can be received from an HSS.

Petitioner Samsung Ex-1004, 0384

The server 105 can comprise a server as depicted and described in connection with server 105 in Figure 1k and Figure 1m of U.S. Patent Application Serial No. 14/084,141, filed November 19, 2013 in the name of John Nix, which is hereby incorporated by reference in its entirety. The IP address 106a can include a subnet prefix 106d and an interface identifier 106e. The IP address 106a can comprise an IPv6 address, where the subnet prefix 106d comprises the first 64 bits of a 128 bit IPv6 address, and the interface identifier 106e can comprise the last 64 bits of a 128 bit IPv6 address as shown in Figure 1f. Other nodes connected to the wireless network 102 can also include IPv6 addresses with different values for the subnet prefix 106d and the interface identifier 106e. A module 101 can include both a network application 101x and an eUICC 107, where a network application 101x is depicted and described in connection with Figure 1b and an eUICC 107 is depicted and described in connection with Figure 1a, Figure 1b, Figure 1c, and Figure 1e.

In an exemplary embodiment, different elements within module 101 can be associated with different IP addresses. The network application 101x can be associated with an IP address 106b and the eUICC 107 can be associated with an IP address 106c. The wireless network 102 could assign the module 101 the subnet prefix 106d used by module 101 with wireless network 102, and an operating system 101h could assign the interface identifier 106e used by the network application 101x and the eUICC 107. Other possibilities exist as well for the source of IP addresses in a system 199, but an end result can comprise the eUICC 107 having a unique IPv6 address 106c such that a server 105 such as an MME can communicate with the eUICC 107 directly by sending a packet with a RAND 118 value from server 105 address 106a to eUICC 107 address 106c.

Although not illustrated in Figure 1f, the exemplary IP addresses for server 105 and eUICC 107 can be associated with port numbers, such that server 105 can use a first port number with the IP address 106a when sending a RAND 118, and eUICC 107 could use a second port number with the IP address 106c when receiving the RAND 118. Server 105 can use a third port number when receiving a RES 119, and eUICC 107 could use a fourth port number when

Petitioner Samsung Ex-1004, 0385

sending the RES 119. The first and third port numbers could be the same value or number, and the second and fourth port numbers could be the same value or number. In an exemplary embodiment, the RAND 118 and RES 119 in system 199 can be formatted according to the UDP Lite protocol, as specified in IETF RFC 3828, which is also incorporated by reference herein. The term "UDP Lite" described in the present invention may also refer to any connectionless protocol supported on IP Network 111 and wireless network 102 where checksums may be partially disabled, thereby supporting the transfer of bit errors within a datagram.

As illustrated in Figure 1f, an eUICC 107 operating in module 101 could be an application with a unique IPv6 address 106c, and the network application 101x utilize a different IPv6 address 106b. The two IP addresses could be on the same subnet 106d used by a module 101, and the network application 101x could communicate with the eUICC 107 locally within module 101 using the two different IPv6 addresses 106b and 106c. The network application 101x could communicate with the eUICC 107 locally for exemplary "other data" depicted in Figure 1f, which could comprise the storing of an address book in the eUICC 107, reading a set of network parameters by the network application 101x from the eUICC 107 with the eUICC profile 107d, etc. In an exemplary embodiment, the eUICC 107 could communicate with the mobile network operator 104 for authentication, thus potentially bypassing the network application 101x for separate handling of RAND 118 and RES 119 values depicted in Figure 1e above. The authentication messages comprising a RAND 118 and a RES 119 could be communicated between the eUICC 107 with IP address 106c to the mobile network operator 104 with IP address 106a without the use of a network application 101x.

The eUICC 107, with an associated IP address 106c could also communicate with the eUICC subscription manager 109 by sending a packet from IP address 106c to an IP address of a server associated with the eUICC subscription manager, such as the exemplary data for a step 205 depicted and described in connection with Figure 2a and Figure 3 below. Note that the eUICC 107 with the IP address 106c can communicate with the eUICC subscription manager 109 without the wireless network 102, but rather through an IP network 111. The connectivity

Petitioner Samsung Ex-1004, 0386

for the IP network 111 could be provided by a different wireless network 102 than the wireless network 102 associated with the MNO 104. Although the use of a specific, unique IP address 106c for eUICC 107 is illustrated in Figure 1f, an eUICC 107 does not require a separate IP address 106c in other embodiments, and the eUICC 107 could share an IP address 106b with a network application 101x or other processes or elements within module 101.

Figure 2a

Figure 2a is a graphical illustration of an exemplary profile for an eUICC, including encrypted data, decryption steps, and decrypted data for the profile, in accordance with exemplary embodiments. Two exemplary forms of an eUICC profile are illustrated in Figure 2a: an encrypted eUICC profile 107c and an eUICC profile 107d. As contemplated herein, an eUICC profile, such as the exemplary eUICC profile 107c and 107d, can be similar to profiles for an eUICC contemplated in ETSI specification TS 103 383 v12.2.0 and related standards, but with differences to the currently published standards, as described below. An eUICC profile 107d can comprise the data from an encrypted eUICC profile 107c, where (i) a first portion of the data, comprising ciphertext 208a, has been decrypted, and (ii) a second portion of the encrypted eUICC profile 107c, comprising ciphertext 208b remains encrypted. Thus, an encrypted eUICC profile 107c can include a first portion, or ciphertext 208a and a second portion, or ciphertext 208b as depicted in Figure 2a. As contemplated herein, an encrypted eUICC profile 107c can be referred to as “profile 107c”, and the eUICC profile 107d can be referred to as “profile 107d”. Both profile 107c and profile 107d can include a profile identity 107e. Profile identity 107e can comprise a number or string such that various elements illustrated in Figure 1a can properly refer to, select, and or identity a profile 107c or profile 107d, including elements such as a mobile network operator 104, eUICC subscription manager 109, module 101, and/or an eUICC 107.

A profile 107c or profile 107d in exemplary systems herein, including systems 100, 300, and 500 can comprise several different possible embodiments. The profiles could be recorded in

Petitioner Samsung Ex-1004, 0387

a file or data set, and stored in nonvolatile memory associated with an eUICC 107, such as, but not limited to, a flash memory 101w. 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. An application layer protocol such as transport layer security (TLS) and additional ciphering at the data-link layer could be utilized as well, in addition to sending and receiving the data for a profile 107c as ciphertext 208a and 208b. The exemplary forms for a profile 107c and 107d in Figure 2a can represent data for a file recorded in a module, such as, but not limited to, (i) storing in a volatile memory 101e when the profiles 107c or 107d are being processed or accessed by a CPU 101b, or (ii) storing in an nonvolatile memory such as flash memory 101w when the profile 107c and 107d are stored long term, including times when a battery 101k may be removed from module 101.

Note that profile 107c with at least two distinct portions, comprising ciphertext 208a and ciphertext 208b, could be recorded in separate segments or in distinct location within module 101 or with an eUICC subscription manager 109, and the two or multiple portions together can comprise a profile 107c. In other words, the portions of ciphertext 208a and 208b (and other data in a profile 107c or profile 107d) can be recorded in different locations while comprising a profile 107c. Other possibilities exist as well for the structure and recording of the exemplary data for a profile 107c and 107d without departing from the scope of the present invention. Although the label “Stored w/ Subscription Manager 109” is depicted with an encrypted eUICC profile 107c, the encrypted eUICC profile 107c can also be stored as the format depicted in Figure 2a within a module 101 or an eUICC 107, until at least a step 206 is performed to decrypt the first ciphertext 208a, as described in this Figure 2a and Figure 3 below.

A first portion of profile 107c can include ciphertext 208a, where ciphertext 208a can include a set of network parameters 201, a first network module identity 202, and a first key K 203. Ciphertext 208a can include these elements in a ciphered string or file, such that a third party would not feasibly be able to ready the plaintext within ciphertext 208a without a key such as eUICC profile key 107b. Ciphertext 208a can comprise the set of network parameters 201,

Petitioner Samsung Ex-1004, 0388

the first network module identity 202, and the first key K 203 as plaintext ciphered with a eUICC profile key 107b, as depicted and described in connection with Figure 2b below. The set of network parameters 201 could comprise a list of values and settings for a module 101 to utilize in connecting with a mobile network operator 104. The set of network parameters 201 could include a list of numbers or strings for values such as (i) allowed frequencies or frequency bands to scan, (ii) preferred access lists for roaming onto other wireless networks, (iii) criteria for a module 101 to select base stations 103 in idle mode, (iv) support for emergency services, (v) supported languages or character encoding, (vi) codes to search for in beacons broadcast by a wireless network 102, (vii) parameters for a radio 101z to use when connecting to a wireless network 102, (viii) names or addresses for a server 105 associated with a MNO 104 in order for a module 101 to send data, etc.

A first network module identity 202 within a ciphertext 208a in profile 107c can comprise a subscriber identity or related identifier of module 101 when connected to a MNO 104 through a wireless network 102. In an exemplary embodiment, the first network module identity 202 can comprise an international mobile subscriber identity (IMSI), a globally unique temporary identity (GTUI), a media access control (MAC) address, a temporary mobile subscriber identity (TMSI) or a similar number or string to identify a module 101 with wireless network 102. Note that a network module identity such as the first network module identity 202 can be different than a module identity 110, such that a network module identity can be assigned by a mobile network operator 104, while a module identity 110 can be assigned by manufacturer. In other words, a network module identity such as the first network module identity 202 can change over time for a module 101, while the module identity 110 can remain the same. The eUICC identity 107a can also remain the same value or number while a network module identity changes.

A first key K 203 within a ciphertext 208a in profile 107c can comprise a standards-based shared secret key K for use in wireless WAN networks based on ETSI, 3GPP, and related standards. As currently specified in ETSI/3GPP standards for LTE and LTE Advanced

Petitioner Samsung Ex-1004, 0389

networks, the shared secret key K, (i) recorded in a SIM or UICC, and a MNO 104 HSS, and (ii) described in 3GPP TS 33.401 V12.9.0 and related standards, comprises a pseudo-random number with a length of 128 bits. The length of key K for standards-based wireless networks 102 may be extended in the future. The use of shared secret key K for authentication of a module 101, and also for ciphering and data integrity, with a wireless network 102 that implements ETSI and/or 3GPP standards is also defined in the specifications ETSI TS 135 205 – 209 and related standards. Both the first key K 203 and the second key K 204 can comprise a shared secret key K as described in 3GPP TS 33.401 V12.9.0 figure 6.2-1 and related standards. A mobile network operator 104 using the function of an authentication center, possibly within a home subscriber server (HSS) can generate or process authentication vectors 117 comprising an random number (RAND), an authentication token (AUTN), a response (RES), and a sequence number using the first key K 203 recorded in a eUCC profile 107c or 107d for the first network module identity 202. Likewise, authentication vectors 117 can be generated by a HSS and sent to a MME for the second network module identity 209a with the second key K 204.

In exemplary embodiments, the first key K 203 depicted in Figure 2a is also depicted and described as operating as a standards-based shared secret key K in Figure 3 below at a step 306. Using the properties of a standards-based key K, a module 101 or an eUICC 107 can use the first key K 203 and a first random number RAND 118 received to process or calculate a first response RES 119. Step 306 with a first key K 203 can comprise an authentication for a module 101 (comprising a “mobile phone”, “mobile station”, or “user equipment”) within standards such as 3GPP TS 33.401 V12.9.0 and related standards using a shared secret key K. As contemplated herein, the use of the term “random number” can comprise a pseudo-random number with a high degree of information entropy that may not be purely mathematically random, but can be considered a random number and referred to as a random number for the purposes herein.

In an exemplary embodiment, as described in Figure 2e and step 302a of Figure 3 below, the first key K 203 can be optionally recorded in ciphertext 208a with an additional layer of encryption, such that the first key K 203 is recorded as a ciphertext 208c within ciphertext 208a.

Petitioner Samsung Ex-1004, 0390

In other words, upon conversion of ciphertext 208a into plaintext using a profile deciphering algorithm 206, the first key K 203 can retain an additional layer of encryption as ciphertext 208c with other data in a profile 107d that may be plaintext. This optional additional layer of encryption for the first key K 203 is also depicted within the profile 107d, where ciphertext 208c optionally remains in profile 107d after the conversion of ciphertext 208a into plaintext using a step 206. As described below, the optionally additional layer of encryption for ciphertext 208c with the first key K 203 can be (i) processed into plaintext first key K 203 (ii) after a subsequent deciphering with an asymmetric ciphering algorithm 219 as illustrated in Figure 2e.

Note that the additional layer of encryption for the first key K 203, in the form of using a ciphertext 208c, can be optionally omitted and the first key K 203 could be plaintext after the conversion of the first portion of profile 107c as ciphertext 208a into plaintext in a profile 107d using a step 206. Thus, the dashed lines around the first key K 203 as a ciphertext 208c indicate the use of ciphertext 208c is optional, depending on the security requirements for an MNO 104 when distributing electronically the first key K 203. In another embodiment as described in Figure 3, the fist key K 203 can comprise a null value, such as the value for a key K in order to support emergency services if module 101 has no valid UICC, and in this case the use of additional encryption via ciphertext 208c can be omitted for a first key K 203. In a related embodiment, the first key K 203 can be omitted entirely from a profile 107c and profile 107d, and the eUICC 107 can subsequently use a null value for the first key K 203.

A second portion of profile 107c can include ciphertext 208b, where ciphertext 208b can include a second key K 204a and a second network module identity 209a. Ciphertext 208b can be ciphered with a symmetric key 127, where the ciphering and deciphering of a portion of ciphertext 208b is depicted and described in connection with Figure 2c below. In an exemplary embodiment, the second network module identity 209a can comprise an international mobile subscriber identity (IMSI), a globally unique temporary identity (GTUI), a media access control (MAC) address, or similar number or string to identify a module 101. In exemplary embodiments, the second network module identity 209a can be a different number or value than

Petitioner Samsung Ex-1004, 0391

the first network module identity 202. Although the second network module identity 209a is illustrated in Figure 2a as internal to ciphertext 208b, the second module identity 209a could be external to ciphertext 208b, such as, but not limited to, the second network module identity 209a being within a profile 107c or profile 107d and external to ciphertext 208b. In other words, in exemplary embodiments, the second network module identity 209a may optionally not be ciphered with the symmetric key 127, while the second key K 204a can be ciphered with the symmetric key 127. As contemplated herein, the term second network identity 209a comprises an encrypted second network identity 209a, where the second network identity 209 is the plaintext version of the encrypted second network identity 209a. Likewise, the term second key K 204a comprises an encrypted second key K 204a, where the second key K 204 is the plaintext version of the encrypted second key K 204a.

In another exemplary embodiment, the second network module identity 209 can comprise the same number or value as the first network module identity 202, or the second network module identity 209 can be optionally omitted. In this case, if (A) the second network module identity 209 comprises the same number or value as the first network module identity 202, or the second network module identity 209 is optionally omitted, then (B) the mobile network operator 104 can preferably support the use of two different shared secret keys K (i.e. first key K 203 and second key K 204) for the same network module identity 202. However, given the current functionality of an HSS and related infrastructure for wireless networks 102, the use of two different network module identities (i.e. the first network module identity 202 and the second network module identity 209) with two different shared secret keys K (i.e. first key K 203 and second key K 204, respectively) may be more compatible or suitable for deployed and operational HSS infrastructure.

A second key K 204a (as an encrypted form of plaintext second key K 204) within a ciphertext 208b in profile 107c can comprise a standards-based shared secret key K for use in wireless WAN networks based on ETSI, 3GPP, and related standards. The use of a second key K 204a (in an unencrypted form of second key K 204) can be equivalent to a first key k 203, but

Petitioner Samsung Ex-1004, 0392

comprise a different random number. The second key K 204 can comprise a random number that is 128 bits in length in order to support 4G networks such as LTE that are widely deployed in 2013, although the length of either first key K 203 or second key K 204 may be a longer number in the future, such an exemplary 256 bits and other possibilities exist as well for the key length. A second key K 204 can also be used with standards-based authentication with a wireless network 102, where the second key K 204 in Figure 2a is also depicted and described as operating as a standards-based shared secret key K in Figure 3 below at a step 311.

The list of exemplary data for encrypted eUICC profile 107c and an eUICC profile 107d comprises an exemplary set, and the profiles could also include additional data to the exemplary data illustrated in Figure 2a. The additional data for a profile 107c or 107d could include (i) a set of cryptographic parameters for eUICC 107, (ii) a set of cryptographic algorithms, such as the exemplary cryptographic algorithms described within ETSI TS 135 205 – 209 and related standards, (iii) a name or address for an eUICC subscription manager 109 associated with the profile 107c, (iv) a name or address for a server 105 associated with a mobile network operator 104, (v) a digital signature of the profile 107d processed with a private key from either eUICC subscription manager 109 or MNO 104, (vi) a date or timestamp for processing the profile 107c or 107d, (vii) and similar or related values for a module 101 and/or eUICC 107 to utilize the profiles. This exemplary additional data which is not depicted in Figure 2a could be included within or external to any of ciphertext 208a and ciphertext 208b.

Note that the profile identity 107e may preferably be external to ciphertext 208a and ciphertext 208b, in order that module 101 and/or eUICC 107 can take steps to identify a profile 107c or 107d. In addition, although a single profile 107c and profile 107d are illustrated in Figure 2a, a module 101 and/or an eUICC 107 could include a plurality of profiles 107c and/or 107d, where each of the plurality of profiles could comprise different data associated with different wireless networks 102. In an exemplary embodiment, more than one profile 107c or profile 107d could be associated with the same wireless network 102, such that a mobile network operator 104 can prefer for the same module 101 to utilize different network access credentials

Petitioner Samsung Ex-1004, 0393

over time, such that the same module 101 could use a different key K and a different network module identity with the same wireless network 102 or mobile network operator 104 over time. Different profiles 107c or 107d can also be identified by the use of a different profile identity 107e. Each profile 107c can be associated with an eUICC profile key 107b as an encryption key (shown in Figure 2b below), although multiple profiles 107c could also share the same eUICC profile key 107b.

A module 101 can receive a profile 107c using a step 205. A profile 107c can be recorded with an eUICC subscription manager 109 before being received by a module 101. As depicted in Figure 2a, a module 101 can receive the profile 107c at a step 205 using the IP network 111. The use of a step 205 by a module 101 is depicted and described in connection with Figure 3 below. The module 101 can receive the profile 107c using a network that is different than wireless network 102 associated with the network access credentials comprising the first key K 203 and the first network module identity 202. In an exemplary embodiment, module 101 can receive the profile 107c in a step 205 using an initial wireless network 102, where module 101 connects with and authenticates with the initial wireless network 102 using an initial eUICC profile 107d different than the eUICC profile 107d depicted in Figure 2a. Or, module 101 could receive a profile 107c using a wireless LAN network or a wired connection via a physical interface 101a such as a USB interface 101v. In another exemplary embodiment, module 101 can receive the profile 107c from a manufacturer, distributor, end user, or technician taking steps to load the profile 107c into a nonvolatile memory within module 101 or eUICC 107. Upon receipt of a profile 107c by module 101, the module 101 can record or store the profile 107c with an eUICC 107.

A module 101 can use an eUICC 107 to decrypt the first portion or ciphertext 208a in a profile 107c using a step 206. Before a step 206, a module 101 can receive an eUICC profile key 107b, where the eUICC profile key 107b can comprise a symmetric ciphering key. The use of a step 206 by module 101 and/or eUICC 107 is also depicted and described in connection with Figure 2b and Figure 3 below. Note that both eUICC subscription manager 109 and module 101

Petitioner Samsung Ex-1004, 0394

can record profile 107c with ciphertext 208a for a period of time, and the step 206 can be taken (i) after receiving eUICC profile key 107b and (ii) before module 101 authenticates with a wireless network 102 using the eUICC profile 107c. A step 206 can covert the ciphertext 208a into plaintext, such that an eUICC 107 can read the values in order to authenticate with a wireless network 102 using the first key K 203. By encrypting the first network module identity 202 and the first key K 203, these network access credentials can remain secure, such that a profile 107c can be transferred in normal physical media (such as disks, drives, or files transferred electronically) or in communications channels outside the control of a mobile network operator 104 and/or eUICC subscription manager 109.

As depicted in Figure 2a, after a step 206 to convert profile 107c into profile 107d, where the ciphertext 208a is decrypted using the eUICC profile key 107b, the ciphertext 208b with the second key K 204a can remain encrypted and thus the second key K can continue to remain secure within a profile 107d. In addition, although ciphertext 208b is depicted in a profile 107c as external to, or separate from, ciphertext 208a, ciphertext 208b could optionally be included within ciphertext 208a. In this case, where ciphertext 208b is within ciphertext 208a for a profile 107c, the result of a step 206 to generate a profile 107d can remain the same, where the ciphertext 208a can be decrypted by step 206 and ciphertext 208b remains encrypted in the resulting profile 107d from a step 206.

A module 101 can use an eUICC 107 to decrypt the second portion or ciphertext 208b in a profile 107d using a step 207. Before a step 207, a module 101 can take the previous steps 205 and 206 in order to record a profile 107d with an eUICC 107. Before a step 207, module 101 can receive a symmetric key 127, where the symmetric key 127 can comprise a symmetric ciphering key. In exemplary embodiments, module 101 can receive the symmetric key 127 from a mobile network operator 104 after a user associated with module 101 performs a separate authentication step 308b as depicted and described in connection with Figure 3 and Figure 4 below. By a mobile network operator 104 only sending symmetric key 127 after the second authentication step 308b, the second key K 204 can remain secured, while a user is allowed to access the

Petitioner Samsung Ex-1004, 0395

wireless network 102 (perhaps temporarily or with other constraints such as limiting access to the Internet but allowing emergency calls) using the first key K 203.

In this manner and by using a second, separate authentication step 308b before sending symmetric key 127, the decryption of network access credentials such as the second key K 204 can remain in the control of a mobile network operator 104, thereby increasing the security of exemplary systems illustrated herein, such as systems 100, 300, and 500. By ciphering the second key K 204 with symmetric key 127, security over conventional technology for an eUICC can be increased for both a user and a mobile network operator. With conventional technology for an eUICC, where only the first key K 203 is used for authentication and ciphering of data between module 101 and wireless network 102, the decryption of the first key K 203 can be outside the control of a mobile network operator 104. With conventional technology contemplated for an eUICC, an end user outside the control or a contractual relationship with mobile network operator 104, including possibly fraudulent users or imposters of valid users, could (i) take steps to obtain a plaintext first key K 203 and associated plaintext first network module identity 202 and (ii) use the credentials to fraudulently access the wireless network 102. In contrast and as contemplated herein, the symmetric key 127 to decrypt the second key K 204a can preferably be only made available to users who authenticate with mobile network operator using a step 308b as described below (or an equivalent step or related commercial arrangements between a user and a mobile network operator 104).

In exemplary embodiments, use of two sets of network access credentials comprising at least the first key K 203 and the second key K 204 allows a user with an eUICC profile 107c to connect to the wireless network 102 using the first key K 203, such that the module 101 can have connectivity to the mobile network operator 104 via the wireless network 102 (and also IP network 111) in order to conduct separate authentication steps 308b. The security steps for a mobile network operator 104 to control the decryption of the first key K 203 can be lowered (thus making the distribution of profile 107c simpler, less costly, and less complex), while a

Petitioner Samsung Ex-1004, 0396

mobile network operator 104 can retain full control over the decryption of the second key K 204a into a usable second key K 204 associated with the second network module identity 209.

The use of a step 207 by module 101 with an eUICC is also depicted and described in connection with Figure 2c and Figure 3 below. A module 101 can record profile 107d with ciphertext 208b for a period of time, and the step 207 can be taken (i) after recording profile 107d, and (ii) before module 101 authenticates with a wireless network 102 using the second key K 204. A step 207 can covert the ciphertext 208b into plaintext, such that an eUICC 107 can read the values in order to authenticate with a wireless network 102 using the second key K 204.

A step 207 can convert the encrypted second key K 204a into a plaintext key K 204. As illustrated in Figure 2a, a step 207 can also convert the encrypted network module identity 209a into a plaintext network module identity 209 as well. As discussed above in this Figure 2a, the network module 209 can be optionally omitted from a step 207, such that the plaintext network module identity 209 could be recorded in a profile 107d, and the plaintext network module identity 209 could be included in the first portion, or ciphertext 208a, in a profile 107c. In another embodiment, the second network module identity 209 can be received by module 101 from wireless network 102 after the module authenticates using the first key K 203. Although not illustrated in Figure 2a, an eUICC 107 can continue to record the plaintext network module identity 209 and plaintext second key K 204 in an eUICC profile after the second key K 204 is decrypted using the symmetric key 127. The module 101 can record the second key K 204 in a protected memory address within ROM 101c or nonvolatile memory 101w.

For embodiments where the first key K 203 is recorded within a ciphertext 208c in a profile 107d after a step 206, the first key K 203 can be converted from ciphertext 208c into a plaintext first key K 203 using a key deciphering step 217 as depicted and described in connection with Figure 2e below. The key deciphering step 217 could use an asymmetric ciphering algorithm 219 with input of (i) ciphertext 208c and (ii) the eUICC private key 215 in order to output the plaintext first key K 203. As described above, the use of a ciphertext 208c can be optionally omitted, and the first key K 203 could be recorded as plaintext in a profile

Petitioner Samsung Ex-1004, 0397

107d. In this case, a step 217 for data in profile 107d can be omitted, and thus step 217 with ciphertext 209c is depicted in Figure 2a with a dashed line.

Although the first key K 203 and the second key K 204a are depicted in Figure 2a as recorded within an eUICC profile 107c or eUICC profile 107d, the first key K 203 and the second key K 204a can be (i) recorded in a nonvolatile memory of module 101, such as, but not limited to, a flash memory 101w, and (ii) without the use of an eUICC 107. In other words, embodiments contemplated herein can be used without an eUICC 107, such that (i) a module 101 can use a first key K 203 to authenticated with a wireless network 102, (ii) after authentication with the first key K 203, the module can receive a symmetric key 127 to decrypt the second key K 204a into second key K 204, and (iii) the module can authenticate with the wireless network 102 using the second key K 204. In other words, an eUICC 107 can be omitted and a module 101 can perform the same steps for (i) receiving encrypted network access credentials and (ii) decrypting the encrypted network access credentials without requiring the use of an eUICC 107.

In embodiments where a module 101 does not include an eUICC 107, the module can record the first key K 203 and the encrypted second key K 204a in a file or memory address without requiring the use of a profile 107c and 107d. For example, the first key K 203 could be recorded in a regular, physical UICC, and the second key K 204a could also be recorded in a regular, physical UICC as well. The regular, physical UICC could (i) receive the symmetric key 127 and decrypt the second key K 204a, and (ii) subsequently record the decrypted second key K 204. The module 101 and UICC could use the decrypted second key K 204 to authenticate with the wireless network 102 where the first key K 203 was previously used. Other possibilities exist as well for a module 101 to (i) use a first key K 203 and an encrypted second key K 204a without departing from the scope of the present invention.

Figure 2b

Figure 2b is a graphical illustration for ciphering and deciphering a profile using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments.

Petitioner Samsung Ex-1004, 0398

An eUICC profile 107d can be (i) ciphered using a profile ciphering algorithm 210 and (ii) deciphered with a profile deciphering algorithm 206. Both the profile ciphering algorithm 210 and the profile deciphering algorithm 206 can include a symmetric ciphering algorithm 211 and the use of an eUICC profile key 107b. An eUICC subscription manager 109, or another node outside a module 101 as illustrated in Figure 1a, can use a profile ciphering algorithm 210 to encrypt an eUICC profile 107c. The processing and computational steps for performing a profile ciphering algorithm 210 could be conducted on a server associated with the eUICC subscription manager 109. The server associated with the eUICC subscription manager 109 can be similar to a server 105 illustrated in Figure 1a, with the difference being the server associated with the eUICC subscription manager 109 can be co-located, associated with, or under the operational control of an eUICC subscription manager 109. Data for an eUICC profile 107d used in a profile ciphering algorithm 210 can comprise the exemplary data illustrated for a profile 107d in Figure 2a above, and an eUICC subscription manager 109 could receive the data for the profile 107d from a mobile network operator 104. The mobile network operator 104 could process, generate, or derive the exemplary values in a profile 107d that can include the network parameters 201, the first network module identity 202, the first key K 203, and the ciphertext 208b. As contemplated herein, the MNO 104 could also function as a eUICC subscription manager 109, and thus in embodiments the profile 107d could be generated by a MNO 104 as well.

Symmetric ciphering algorithm 211 in a profile ciphering algorithm 210 can utilize a key such as an eUICC profile key 107b to encrypt or cipher data. Examples of symmetric ciphers for a symmetric ciphering algorithm 210 include (i) an Advanced Encryption Standard (AES) cipher, as specified in Federal Information Processing Standards (FIPS) Publication 197, and (ii) Triple Data Encryption Standard (Triple DES), as described in NIST Special Publication 800-67 Revision 1, “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (Revised January 2012)”. Other symmetric ciphers and/or combinations of symmetric ciphers can be utilized as well for a symmetric ciphering algorithm 210 without departing from the scope of the present invention. In general, a symmetric ciphering algorithm 211 in a profile ciphering

Petitioner Samsung Ex-1004, 0399

algorithm 210 (and other steps for symmetric ciphering contemplated herein) can accept input of plaintext and a key, and using the two sets of input data, the symmetric ciphering algorithm 211 can perform multiple rounds of mixing, substituting, rotating, and/or perform XOR functions with the input in order to produce a ciphertext output. Although not illustrated in Figure 2b and Figure 2c, a set of cryptographic parameters can also be input into symmetric ciphering algorithms 211 in order to specify parameters or configurations of the symmetric ciphering algorithm 211, such as, but not limited to, the selection of 128, 192, or 256 bits with AES.

A cipher key used with a symmetric ciphering algorithm 211, such as, but not limited to, the exemplary eUICC profile key 107b can comprise a random or pseudo-random number, with an appropriate length or number of bits for the symmetric ciphering algorithm 211. The exemplary eUICC profile key 107b for use in a profile ciphering algorithm 210 could be shared between an eUICC subscription manager 109 and an eUICC 107 in a module 101 in several different ways. The eUICC profile key 107b could be recorded in or with the eUICC 107 upon manufacturing of module 101. The eUICC profile key 107b could be securely received by a module 101 using a wireless network 102 from the eUICC subscription manager 109 before the module 101 performs a step that includes a profile deciphering algorithm 206. An encrypted eUICC profile key 107b could be received by module 101 and then decrypted by module 101 using an asymmetric ciphering algorithm 219 as depicted and described in connection with Figure 2e below. The eUICC profile key 107b could also be derived by a module 101 and an eUICC subscription manager 109 (or another server performing the steps in a profile ciphering algorithm 210) using a key exchange such as, but not limited to, a Diffie-Hellman key exchange or an Elliptic Curve Diffie-Hellman key exchange.

Other possibilities exist as well for a module 101 and an eUICC subscription manager 109 (or another server performing the steps in a profile ciphering algorithm 210) to securely share a eUICC profile key 107b without departing from the scope of the present invention. In addition, although a single eUICC profile key 107b is illustrated in Figure 2b, an eUICC subscription manager 109 and an eUICC 107 could use multiple eUICC profile keys 107b,

Petitioner Samsung Ex-1004, 0400

including embodiments where a first encrypted eUICC profile 107c is associated with a first eUICC profile key 107b and a second encrypted eUICC profile 107c is associated with a second eUICC profile key 107b. Further, each encrypted eUICC profile 107c could be uniquely associated with a different eUICC profile key 107b. Each of the different eUICC profile keys 107b could be securely transferred between the eUICC 107 and the eUICC subscription manager 109 using either (i) asymmetric ciphering 219 as illustrated in Figure 2e below, or (ii) a key exchange, as depicted and described in connection with step 303 of Figure 3 below.

With a profile ciphering algorithm 210, the symmetric ciphering algorithm 211 can accept input of (i) the eUICC profile key 107b, and (ii) and an eUICC profile 107d plus an optional security token 212, in order to output an encrypted eUICC profile 107c. The encrypted eUICC profile 107c can be reasonably secured, such that deciphering the profile 107c without the eUICC profile key 107b would be infeasible. After ciphering with a symmetric ciphering algorithm 211, deciphering the ciphertext without the cipher key would require extensive dedicated computational resources such as hundreds of servers or more for many years or longer. The optional security token 212 can include a string or number in order to enhance the security of the ciphertext output by a symmetric ciphering algorithm 211. The optional security token 211 could comprise a random number or other value, such that the input and output of a symmetric ciphering algorithm 211 is properly padded, where the length of input and output are appropriate for the symmetric ciphering algorithm.

Although the input of eUICC profile 107d is depicted in Figure 2b with a label of “plaintext”, the eUICC profile 107d in a profile ciphering algorithm 210, the “plaintext” eUICC profile 107d can include encrypted data such as ciphertext 208b, where ciphertext 208b can include encrypted data ciphered with a different key than eUICC profile key 107b. In other words, a profile 107c can include multiple layers of ciphering, where different layers use different cipher keys, and the exemplary a profile ciphering algorithm 210 with the eUICC profile key 107b can be used to encrypt the ciphertext 208a illustrated in Figure 2a above. As

Petitioner Samsung Ex-1004, 0401

noted above with Figure 2a, ciphertext 208b can be either (i) included inside ciphertext 208a, or (ii) remain external to ciphertext 208a.

After a server associated with an eUICC subscription manager 109 generates the output of an encrypted profile 107c from a profile ciphering algorithm 210, the encrypted profile 107c can be transferred to module 101 through either unsecured channels, or channels that are not under the full control of an eUICC subscription manager 109 or a mobile network operator 104 associated with the profile 107c. The module 101 can receive the profile 107c through an IP network 111, including using the public Internet, or a manufacturer, distributor, technician, or end user could load the profile 107c into the module (such as, but not limited to, using a USB interface 101v). This initial loading of profile 107c by a manufacturer, distributor, technician, or end user may be required for the first use or startup of a module 101, but then module 101 may preferably receive additional or subsequent profiles 107c at later times using IP network 111 and other automated, electronic means using a network including a wireless network 102.

A module 101 or an eUICC 107 within module 101 can process the encrypted profile 107c using a profile deciphering algorithm 206 as depicted in Figure 2b and also depicted and described in Figure 2a. Note that the module 101 or eUICC 107 could record the encrypted profile 107c for a period of time, and take the steps to decrypt the profile 107c in a profile deciphering algorithm 206 after receiving the eUICC profile key 107b associated with the profile 107c. Or the eUICC profile key 107b could be recorded in a module 101 or with an eUICC 107 before profile 107c is received, and the steps for a profile deciphering algorithm 206 could be performed after the receipt of an instruction from an eUICC subscription manager 109 or at a specified time or under specified conditions (such as a module 101 needing or preferring to connect to a wireless network 102 for the first time). An exemplary use and sequence for a profile deciphering algorithm 206 is depicted and described in connection with Figure 3 below. Other possibilities exist as well for the time that a module 101 or an eUICC 107 can process a profile deciphering algorithm 206 without departing from the scope of the present invention. As

Petitioner Samsung Ex-1004, 0402

contemplated herein, the use of the term “step 206” can refer to the use of a profile deciphering algorithm 206, and a “step 207” can refer to the use of a key K deciphering algorithm 207, etc.

A profile deciphering algorithm 206 can include a symmetric ciphering algorithm 211. The symmetric ciphering algorithm 211 can be equivalent to or the same as the symmetric ciphering algorithm 211 in a profile ciphering algorithm 210 operated by a server and as described above. The symmetric ciphering algorithm 211 can accept input of the eUICC profile key 107b as a cipher key. The module 101 or eUICC 107 could securely receive the eUICC profile key 107b using the steps described above in connection with a profile ciphering algorithm 210. An exemplary transfer or key exchange for module 101 to receive eUICC profile key 107b is also described in Figure 2e and Figure 3 below. The symmetric ciphering algorithm 211 in a profile deciphering algorithm 206 can also accept input of the encrypted eUICC profile 107c, which could comprise ciphertext 208a.

The symmetric ciphering algorithm 211 in a profile deciphering algorithm 206 can decrypt the ciphertext 208a in order to output the profile 107d, where the ciphertext 208a is converted to plaintext. Ciphertext 208b in a profile 107c can remain encrypted using the symmetric key 127 after a profile deciphering algorithm 206. In other words, the profile deciphering algorithm 206 can convert a portion of the profile 107c into plaintext, where the portion comprises ciphertext 208a. As depicted in Figure 2a above, exemplary plaintext in a profile 107d resulting from a profile deciphering algorithm 206 can include a first network module identity 202 and the first key K 203. The resulting plaintext from a profile deciphering algorithm 206 can also optionally include a security token 212. Security token 212 could comprise the string or value also optionally input into the symmetric ciphering algorithm 211 in a profile ciphering algorithm 210. The security token 212 can include a padding value to make the length of the security token 212 and profile 107d a desired value for the symmetric ciphering algorithm 211 or other requirements such as making the encrypted profile 107c a desired length.

Figure 2c

Petitioner Samsung Ex-1004, 0403

Figure 2c is a graphical illustration for ciphering and deciphering a key K using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments. A second key K 204a can be (i) ciphered using a key K ciphering algorithm 213 and (ii) deciphered with a key K deciphering algorithm 207. Both the key K ciphering algorithm 213 and the key K deciphering algorithm 207 can include a symmetric ciphering algorithm 211 and the use of a symmetric key 127. A mobile network operator 104 can use a key K ciphering algorithm 213 to encrypt the second key K 204a. The processing and computational steps for performing a key K ciphering algorithm 213 could be conducted on a server associated with the mobile network operator 104 such as a server 105 illustrated in Figure 1a. Other possibilities exist as well for the location or association of a computer to process a key K ciphering algorithm 213 without departing from the scope of the present invention.

A key K ciphering algorithm 213 can include a symmetric ciphering algorithm 211. The symmetric ciphering algorithm 211 can similar to the symmetric ciphering algorithm 211 as depicted and described in connection with Figure 2b above. A symmetric ciphering algorithm 211 can include a collection of different symmetric ciphers, such that a first symmetric cipher comprising the AES cipher could be used in a Figure 2b, while a different symmetric cipher could be used in a Figure 2c. Or, the same algorithm within symmetric ciphering algorithm 211 can be used in a symmetric ciphering algorithm 211 in Figure 2b and Figure 2c. The symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 can accept input of a symmetric key 127 and plaintext in the form of a second key K 204. The second key K 204 could represent a random number, such as, but not limited to, an exemplary 128 random number currently used as a shared secret key K in standard LTE networks and a different length for second key K 204 could be used as well. The second key K 204 could be derived or processed by the function of an authentication center with a home subscriber server (HSS). Although not illustrated in Figure 2c, but as illustrated in Figure 2a, the plaintext as input into a symmetric ciphering algorithm 211 can also include a second network module identity 209. The input into a symmetric ciphering algorithm 211 for a key K ciphering algorithm 213 can also include a number, value, or string for

Petitioner Samsung Ex-1004, 0404

a security token 212. The use of a security token 212 is depicted and described in connection with Figure 2b above. Thus, a mobile network operator 104 could also use a key K ciphering algorithm 213 to encrypt other data in addition to a second key K 204.

The symmetric key 127 input into a symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 can comprise a random number processed or generated by a server 105, where the server 105 is associated with a mobile network operator 104. The server processing or deriving a symmetric key 127 can comprise or be associated with an HSS for an LTE or LTE advanced network. As illustrated in Figure 2c, the symmetric key 127 can comprise a cipher key for the symmetric ciphering algorithm 211. A cipher key used with a symmetric ciphering algorithm 211, such as, but not limited to, the exemplary symmetric key 127 can comprise a random or pseudo-random number, with an appropriate length or number of bits for the symmetric ciphering algorithm 211 in a key K ciphering algorithm 213. Using the input of the symmetric key 127 and the plaintext second key K 204, the symmetric ciphering algorithm 211 could output an encrypted second key K 204a. As illustrated in Figure 2c and Figure 2a above, the encrypted second key K 204a could be included in ciphertext 208b. The symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 may also optionally include a security token 212, as illustrated.

After processing the ciphertext 208b, the mobile network operator 104 can either (i) include the ciphertext 208b in a profile 107d and send the profile 107d to an eUICC subscription manager 109, or (ii) send the ciphertext 208b directly an eUICC subscription manager 109 for the eUICC subscription manager 109 to include the ciphertext 208b in a profile 107d. Ciphertext 208b could be recorded in or with an eUICC profile 107d, where an eUICC subscription manager 109, or another server associated with an eUICC subscription manager 109 can subsequently encrypt the eUICC profile 107d using a profile ciphering algorithm 210 depicted and described in connection with Figure 2b above. Other possibilities exist as well for the timing an sequence of steps for transferring and recording a ciphertext 208b output from a key K ciphering algorithm 213 without departing from the scope of the present invention. After profile

Petitioner Samsung Ex-1004, 0405

107d with ciphertext 208b has been created, the profile 107d can be ciphered with a profile ciphering algorithm 210 to create an encrypted profile 107c, as illustrated in Figure 2b above.

The exemplary symmetric key 127 for use in a key K ciphering algorithm 213 could be shared between a module 101 with an eUICC 107 and the mobile network operator 104 in several different ways. The symmetric key 127 could be sent from the mobile network operator 104 (possibly using a server 105) to a module 101 after (i) the module properly authenticates with the mobile network operator 104 and/or a wireless network 102 associated with the MNO 104 using the first key K 203, and (ii) a user 113 associated with the module 101 authenticates with the MNO 104. Note that if MNO 104 sends the symmetric key 127 to module 101 after module 101 uses the first key K 203 to authenticate, then the ciphering or encryption of the channel used to send the symmetric key K 127 can be within the control of MNO 104 (whereas the communications channel and ciphering keys used to send encrypted profile 107c may be outside the control of MNO 104). The symmetric key K 127 could also be derived by a module 101 and an MNO 104 using a key exchange, where the symmetric key K 127 could be derived using a RAND 118 value received by the module 101 after authenticating with the first key K 203, where the module 101 and/or eUICC 107 derives the symmetric key K 127 using the RAND 118 value and the first key K 203. Other possibilities exist as well for a module 101 and a mobile network operator 104 to securely share a symmetric key 127 without departing from the scope of the present invention.

A module 101 or an eUICC 107 within module 101 can process the ciphertext 208b using a key K deciphering algorithm 207 as depicted in Figure 2c. Note that the module 101 or eUICC 107 could record the ciphertext 208b for a period of time, and take the steps to decrypt the ciphertext 208b with a key K deciphering algorithm 207 after receiving or deriving the symmetric key 127. Or the symmetric key 127 could be recorded in a module 101 or with an eUICC 107 before ciphertext 208b is decrypted, and the steps for a key K deciphering algorithm 207 could be performed after the receipt of an instruction from the MNO 104 to decrypt the second key K 204a. An exemplary use and sequence for a key K deciphering algorithm 207 is

Petitioner Samsung Ex-1004, 0406

depicted and described in connection with Figure 3 below. Other possibilities exist as well for the time that a module 101 or an eUICC 107 can process a key K deciphering algorithm 207 without departing from the scope of the present invention.

A key K deciphering algorithm 207 can include a symmetric ciphering algorithm 211. The symmetric ciphering algorithm 211 can be equivalent to or the same as the symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 performed by an MNO 104 and as described in this Figure 2c above. The symmetric ciphering algorithm 211 can accept input of the symmetric key 127 as a cipher key. The module 101 or eUICC 107 could securely receive or derived the symmetric key 127 using the steps described above in connection with a key K ciphering algorithm 213. The symmetric ciphering algorithm 211 in a key K deciphering algorithm 207 can also accept input of the encrypted key K 204a, which could comprise ciphertext 208b. Additional data, such as, but not limited to a second module identity 209a could optionally be included within ciphertext 208b.

The symmetric ciphering algorithm 211 in a key K deciphering algorithm 207 can decrypt the ciphertext 208b in order to output the plaintext second key K 204, such that the ciphertext 208b is converted to plaintext. The resulting plaintext from a key K deciphering algorithm 207 can also optionally include a security token 212. Security token 212 could comprise the string or value also optionally input into the symmetric ciphering algorithm 211 in a key K ciphering algorithm 213. The security token 212 can include a padding value to make the length of the security token 212 and second key K 204a a desired value for the symmetric ciphering algorithm 211 or other requirements such as making the ciphertext 208b a desired length.

Figure 2d

Figure 2d is a graphical illustration of a public key and a private key for an eUICC, in accordance with exemplary embodiments. An eUICC 107 within a module 101 can include an eUICC private key 215, which can be associated with an eUICC public key 214. The eUICC

Petitioner Samsung Ex-1004, 0407

private key 215 and eUICC public key 214 can comprise a public key infrastructure (PKI) key pair for eUICC 107. The eUICC subscription manager 109 can record the eUICC public key 214 along with an eUICC identity 107a, such that the eUICC subscription manager 109 can properly associate one of a plurality of eUICC public keys 214 with the proper eUICC 107. Although not illustrated in Figure 2d, an eUICC subscription manager 109 could record the eUICC public key 214 and an associated eUICC identity 107a in a database. The use of an eUICC ID 107a is also depicted and described in connection with Figure 3 below.

The eUICC private key 215 and eUICC public key 214 could be processed using RSA algorithms or elliptic curve cryptography (ECC) algorithms, and other possibilities exist as well for the format of PKI keys without departing from the scope of the present invention. An ECC key length of 283 bits provides security similar to an RSA key length of approximately 2048 bits, and in an exemplary embodiment the eUICC key pair can utilize an ECC algorithm, although an RSA algorithm or other algorithms for PKI keys could also be utilized by an eUICC 107. The eUICC private key 215 can be processed or derived using a random number. eUICC public key 214 can comprise a key recorded in an X.509 certificate that also includes a module identity 110 and/or eUICC identity 107a, although the use of an X.509 certificate with an eUICC public key 214 is not required. The eUICC public key 214 in the form of an X.509 certificate can optionally be signed by a certificate authority. The keys can support standards such as, but not limited to, the International Organization for Standardization (ISO) ISO/IEC 9594 series of standards (herein incorporated by reference) and the Internet Engineering Task Force (IETF) RFC 5280 titled “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (herein incorporated by reference), including future updates to these standards.

Several possibilities exist for the source of an eUICC private key 215 and eUICC public key 214. The eUICC private key 215 and eUICC public key 214 be generated using standard software tools such as, but not limited to, Openssl, libmcrypt, and/or and Crypto++, and other tools to generate public and private keys exist as well. Public and private keys as contemplated

Petitioner Samsung Ex-1004, 0408

herein could be recorded in a file such as, but not limited to, a *.pem file (Privacy-enhanced Electronic Mail), a file formatted according to Basic Encoding Rules (BER), Canonical Encoding Rules (CER), or Distinguished Encoding Rules (DER), or as text or binary file. Other formats for public and private keys may be utilized as well, including proprietary formats. A module 101 could derive the PKI key pair using a set of cryptographic algorithms and a key pair generation algorithm. 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.

A manufacturer of module 101 or an eUICC subscription manager 109 could also derive the eUICC private key 215 and eUICC public key 214 in a server, and load the eUICC private key 215 into a nonvolatile memory of module 101 before distribution of the module 101. The manufacturer of module 101 could send or make available the eUICC public key 214 to an eUICC subscription manager 109. The module 101 could send record the eUICC public key 214 and 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.

Although Figure 2d illustrates an eUICC private key 215 and eUICC public key 214, a module 101 could use a PKI key pair associated with module 101 instead of being associated with an eUICC 107 in order to use an asymmetric ciphering algorithm as depicted in Figure 2e below. In other words, a module 101 and an eUICC subscription manager 109 could use a module private key 112a and a module public key 112b in order to obtain the same functionality of an eUICC private key 215 and an eUICC public key 214. A module private key 112a and a module public key 112b for a module 101 could have the same properties and characteristics for an eUICC private key 215 and an eUICC public key 214 as described herein. Other possibilities exist as well for the source or use of a PKI key pair for an eUICC private key 215 and eUICC public key 214 without departing from the scope of the present invention.

In exemplary embodiments, both the eUICC subscription manager 109 and the eUICC 107 can include a set of digital signature algorithms 221, in order to sign and verify messages between (i) an eUICC 107 and eUICC subscription manager 109, and (ii) eUICC subscription manger 109 and MNO 104. Digital signature algorithms 221 can also verify signatures such as, but not limited to, comparing that (i) a first secure hash value received from a sending node matches (ii) a second secure hash value calculated using a recorded public key associated with the sending node. Digital signature algorithms 221 can utilize algorithms in National Institute of Standards (NIST) "FIPS 186-4: Digital Signature Standard", or IETF RFC 6979 titled “Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)”. The use of ECDSA algorithm within a set of digital signature algorithms 221 may be preferred if keys such as, but not limited to, eUICC private key 215 and eUICC public key 214 are based on elliptic curve cryptography. Digital signature algorithms 221 could also include an RSA digital signature algorithm (DSA) for use with RSA-based public and private keys. Other PKI standards or proprietary techniques for securely generating digital signatures and verifying digital signatures may be utilized as well in digital signature algorithms 221. As depicted and described in connection with Figure 3 below, a digital signature algorithm 221 can be used in a step 205 in order to authenticate an eUICC 107 operating in a module 101 with an eUICC subscription manager 109.

As illustrated in Figure 2d, the eUICC subscription manager 109 may also be associated with an eUICC subscription manager public key 220 and an eUICC subscription manager private key 222, and the two keys can comprise a PKI key pair for the eUICC subscription manager 109. The eUICC subscription manager public key 220 and an eUICC subscription manager private key 222 can be formatted and processed by algorithms equivalent or similar to the algorithms and format for the eUICC public key 214 and the eUICC private key 215 described in this Figure 2d above. The eUICC subscription manager public key 220 can optionally be signed by a certificate authority. An eUICC 107 can use the digital signature algorithms 221 and the eUICC subscription manager public key 220 to verify a digital signature from the eUICC subscription

Petitioner Samsung Ex-1004, 0410

manager 109. Although not illustrated in Figure 2d, the eUICC 107 or module 101 could also record a public key associated with the mobile network operator 104, and use the public key associated with the mobile network operator 104 to verify a digital signature from the mobile network operator 104 using the digital signature algorithms 221.

Figure 2e

Figure 2e is a graphical illustration for ciphering and deciphering a key for an eUICC using an asymmetric ciphering algorithm using a PKI key pair, in accordance with exemplary embodiments. An eUICC subscription manager 109 could process or calculate a key ciphering algorithm 216 and a module 101 or eUICC 107 could process or calculate a key deciphering algorithm 217. The eUICC key ciphering algorithm 216 can use an asymmetric ciphering algorithm 219 with an input of (i) an eUICC public key 214 as a cipher key and (ii) the eUICC profile key 107b as plaintext in order to output ciphertext of an encrypted eUICC key 218. The plaintext eUICC profile key 107b can comprise a random number of appropriate length for processing a profile ciphering algorithm 210 and profile deciphering algorithm 206 as depicted and described in connection with Figure 2b above. As illustrated in Figure 2e, the input into a key ciphering algorithm 216 could also include an optional security token 212, where a security token 212 is depicted and described in connection with Figure 2b above.

An asymmetric ciphering algorithm 219 within a key ciphering algorithm 216 and a key deciphering algorithm 217 an comprise an algorithm for utilizing public key infrastructure (PKI) techniques to both (i) encrypt plaintext with a public key and (ii) decrypt plaintext with a private key. Example algorithms within asymmetric ciphering algorithm 219 include an RSA algorithm and an elliptic curve cryptography (ECC) algorithm, and other asymmetric ciphering algorithms could be utilized as well. The use and application of RSA algorithms and cryptography are described within IETF RFC 3447 titled “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”, herein incorporated by reference, among other published standards for the use of RSA algorithms. The use of an RSA algorithm in an

Petitioner Samsung Ex-1004, 0411

asymmetric ciphering algorithm 219 for encryption and decryption, can also be processed according to the description of the RSA algorithm according to the Wikipedia entry for "RSA (algorithm)" as of September 9, 2013, which is incorporated by reference herein. The use and application of an ECC algorithm for asymmetric ciphering algorithm 219 can conform with algorithms within IETF RFC 6090 titled "Fundamental Elliptic Curve Cryptography Algorithms" (herein incorporated by reference), among other published standards using ECC. Asymmetric ciphering algorithm 219 can also utilize elliptic curve cryptography algorithms for the Wikipedia entry for "Elliptic curve cryptography" as of September 9, 2013, which is incorporated by reference herein.

ECC algorithms (with corresponding ECC-based PKI keys) may utilized for asymmetric ciphering algorithm 219 according to exemplary preferred embodiments in order to maintain high security with smaller key lengths, compared to RSA, thereby helping to comparably reduce the message lengths, radio frequency spectrum utilization, and processing power required by module 101. RSA algorithms (with corresponding RSA-base PKI keys) for asymmetric ciphering algorithm 219 may be utilized in other embodiments in order to maintain compatibility with deployed or legacy software and systems that supports RSA based keys and algorithms.

After an eUICC subscription manager 109 uses a eUICC key ciphering algorithm 216 to convert a plaintext eUICC profile key 107b into a ciphertext as an encrypted eUICC key 218, the eUICC subscription manager can send the ciphertext to the module 101. The eUICC subscription manager could send the ciphertext as an encrypted eUICC key 218 to module 101 using an IP network 111, and the IP network 111 could comprise the public Internet. In this manner, the module 101 can securely receive the encrypted eUICC key 218 in order to perform, process, or calculate a key deciphering algorithm 217. Third parties with access to the encrypted eUICC key 218 would not feasibly be able to read the plaintext eUICC profile key 107b, even with access to the eUICC public key 214. The module 101 could receive the encrypted eUICC key 218 along with an eUICC profile identity 107e in order to determine a profile 107c associated with the encrypted eUICC key 218, where a subsequent step (after deciphering the

Petitioner Samsung Ex-1004, 0412

encrypted eUICC key 218) could comprise a profile deciphering algorithm 206. The module 101 could receive the encrypted eUICC key 218 either before or after receiving the profile 107c.

After receiving the encrypted eUICC key 218, the module 101 or eUICC 107 could decrypt the encrypted eUICC key 218 using a key deciphering algorithm 217. A key deciphering algorithm 217 can include a asymmetric ciphering algorithm 219. The asymmetric ciphering algorithm 219 can be equivalent to or the same as the asymmetric ciphering algorithm 219 in a key ciphering algorithm 216 operated or processed by an eUICC subscription manager 109 as described in this Figure 2e above. The asymmetric ciphering algorithm 219 in a key deciphering algorithm 217 can accept input of the eUICC private key 215 as a cipher key. The asymmetric ciphering algorithm 219 in a key deciphering algorithm 217 can also accept input of the encrypted eUICC key 218 as a ciphertext. The key deciphering algorithm 217 can use an asymmetric ciphering algorithm 219 with an input of (i) an eUICC private key 215 as a cipher key and (ii) the encrypted eUICC key 218 as ciphertext in order to output plaintext of an eUICC profile key 107b. As illustrated in Figure 2e, the plaintext could also optionally include a security token 212. After processing a plaintext eUICC profile key 107b from a key deciphering algorithm 217, module 101 or eUICC 107 could use the plaintext eUICC profile key 107b in order to perform a profile deciphering algorithm 206 as illustrated in Figure 2b.

Although exemplary embodiments can include the use of a key ciphering algorithm 216 and a key deciphering algorithm 217 in order to securely transfer the eUICC profile key 107b from an eUICC subscription manager 109 to a module 101, a key ciphering algorithm 216 and a key deciphering algorithm 217 can be omitted in other exemplary embodiments. For example, if the eUICC subscription manager and module 101 or eUICC 107 support the use of a secure key exchange such as Diffie-Hellman or ECDH, then the eUICC profile key 107b could be mutually derived by the two nodes and the encrypted eUICC key 218 would not need to be transferred through an IP network 111 between the two nodes.

In another embodiment, as depicted in Figure 2e, the key ciphering algorithm 216 and key deciphering algorithm 217 may also be used with ciphertext 208c with an encrypted first key

Petitioner Samsung Ex-1004, 0413

K 203 and a plaintext of the first key K 203, if a profile 107d includes ciphertext 208c with encrypted first key K 203. In this case, a mobile network operator 104 could perform the key ciphering algorithm 216 with input of (i) the plaintext first key K 203 and (ii) the eUICC public key 214 in order to output ciphertext 208c. The ciphertext 208c can include the encrypted first key K 203, although the ciphertext 208c could also include other data such as the network parameters 201. The MNO 104 could send the ciphertext 208c (with the encrypted first key K) to the eUICC subscription manager 109 in a step 302b in Figure 3 for inclusion in the profile 107d and profile 107c. As depicted in Figure 2e, a module 101 or eUICC 107 could perform the key deciphering algorithm 217 on the ciphertext 208c with the first encrypted key K 203 in order to obtain the plaintext first key K 203. In this manner, the first key K 203 is not shared as plaintext with any entities besides the MNO 104 and a module 101 with the eUICC 107. In other words, a MNO 104 can use a key ciphering algorithm 216 to prevent the sharing of a plaintext first key K 203 with an eUICC subscription manager 109.

In addition, although Figure 2e illustrates an eUICC subscription manager as performing the eUICC key ciphering algorithm 216 and the module 101 or eUICC 107 as performing the eUICC key deciphering algorithm 217, an alternative embodiment contemplates that the eUICC subscription manager 109 performs the eUICC key deciphering algorithm 217 and the module 101 or eUICC 107 performs the eUICC key ciphering algorithm 216. In this alternative embodiment, the module 101 can (i) derive the eUICC profile key 107b, and (ii) send the ciphertext comprising the encrypted eUICC key 218 to the eUICC subscription manager 109. In this alternative embodiment, the module 101 can (i) use the eUICC subscription manager public key 220 to cipher the derived eUICC profile key 107b, (ii) send the encrypted eUICC profile key 107b to the eUICC subscription manager 109, and (iii) the eUICC subscription manager 109 can decrypt the encrypted eUICC profile key 107b using the eUICC subscription manager private key 222. In this alternative embodiment, the eUICC subscription manager 109 could (i) use the eUICC key deciphering algorithm 217 to decrypt the encrypted eUICC key 218 received from

Petitioner Samsung Ex-1004, 0414

the module 101, and then (ii) subsequent encrypt the profile 107d into a profile 107c using a profile ciphering algorithm 210 as depicted and described in connection with Figure 2b above.

Figure 3

Figure 3 is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments. System 300 can include an eUICC subscription manager 109, an IP network 111, a mobile network operator 104, a module 101. A module 101 can include a network application 101x and an eUICC 107. The network application 101x can perform the operations for communicating with the wireless network 102 (i) at the data-link layer using standards for PLMN networks such as, but not limited to exemplary radio resource control standards within ETSI TS 136 331 v.10.7 entitled “LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification”, which is herein incorporated by reference, and (ii) at the network layer using Internet Protocol. Other standards for communication at the data-link layer between a network application 101x and a mobile network operator 104 can be utilized as well without departing from the scope of the present invention. The (i) mobile device 101, using the network application 101x, and (ii) the mobile network operator 104 can send and receive data using the wireless network 102 depicted and described in connection with Figure 1a. Although a single module 101 is illustrated in system 300 in Figure 3, a system 300 could include a plurality of modules 101.

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 network application 101x and the eUICC 107 can send and receive data locally within the module 101 using an eUICC driver 128 as depicted and described in connection with Figure 1b and Figure 1e. The module 101, using a network application 101x, can send and receive data with the eUICC subscription manager 109 using the IP network 111. As illustrated in Figure 3, the

Petitioner Samsung Ex-1004, 0415

module 101 can send and receive data with the eUICC subscription manager 109 in a step 205 using an initial network.

The initial network could comprise a different wireless network 102 than a wireless network 102 (i) for the mobile network operator 104, and (ii) used for a first authentication 304 and a second authentication 310. In other words, module 101 can send and receive data for an eUICC profile 107c through a initial network that is different than the wireless network 102 associated with the mobile network operator 104. The network application 101x could support different standards for wireless networking technologies, such that the different wireless network 102 used to access the eUICC subscription manager 109 could comprise exemplary networks such as WiFi or LTE Advanced, and the network application 101x could use LTE to communicated with the mobile network operator 104. Other possibilities exist as well for the network application 101x to support communication with a variety of different networks without departing from the scope of the present invention.

The left side of network application 101x in Figure 3 for communication with the mobile network operator 104 can comprise communication through a radio 101z with the wireless network 102, and the right side of network application 101x can comprise internal communication within module 101 as described in the paragraph above and also Figure 1e above. The internal communication between network application 101x and eUICC 107 using an operating system 101h could comprise either (i) sharing memory 101e, where module 101 writes data such as, but not limited to, an exemplary RAND 118 value and eUICC 107 reads the values from the shared memory 101e, or (ii) using loopback UDP ports within operating system 101h, such that network application 101x sends a UDP datagram with the RAND 118 value using a first UPD loopback port, and the eUICC 107 receives the UDP datagram with the RAND 118 value using a second UDP loopback port. For an operating system 101h within module 101 using IPv4 addresses, the addresses used for the UDP loopback ports could comprise addresses in the range of the 127.0.0.0/8 address block. For an operating system 101h within module 101 using IPv6 addresses, the addresses used for the UDP loopback ports could comprise an ::1

Petitioner Samsung Ex-1004, 0416

address. In another embodiment illustrated in Figure 1f above, the eUICC 107 can communicate with the MNO 104 directly for embodiments where the eUICC 107 includes an IP address 106c.

At a step 301, a module 101 can record an eUICC identity 107a, an address 109a of an eUICC subscription manager 109, and an eUICC private key 215 associated with the eUICC 107. A manufacturer, distributor, technician, end user, or installer of module 101 could record the data for a step 301 in module 101, or the data could be downloaded or accessed separately via an IP network 111, including the public Internet. Other data could be included in a step 301 as well, such as, but not limited to, the software or firmware comprising the eUICC 107, an eUICC profile key 107b, an eUICC public key 214, an eUICC subscription manager public key 220, an eUICC driver 128, an initial profile 107d or 107c, and policy rules for allowing access to the profiles, and other additional data could be included in a step 301 as well. Additional optional data for recording with an eUICC 107 in a step 301 are depicted on the second line of step 301 in Figure 3.

In an exemplary embodiment, a manufacturer of module 101 records the exemplary data for an eUICC 107 in a step 301, such that a module 101 can being operations and connecting to an initial wireless network 102 upon power-up in order to establish initial communications, including allowing the communication with the eUICC subscription manager 109 through the initial wireless network 102. As noted above in this Figure 3, an initial wireless network 102 used for the eUICC 107 to access the eUICC subscription manager 109 can be different than the wireless network 102 used to access the mobile network operator 104. The address 109a of an eUICC subscription manager 109 could comprise either an IP address or a domain name, and in an exemplary embodiment the address 109a comprises a domain name and the module 101 can query for the IP address associated with the domain name for address 109a via either a domain name system (DNS) query or a secured DNS query (DNSSEC). A module 101 can connect with an initial wireless network 102 (different than the depicted wireless network 102 in Figure 3) after a step 301 in order to communicate with an eUICC subscription manager 109.

Petitioner Samsung Ex-1004, 0417

At a step 302a, an eUICC subscription manager 109 could record data for the eUICC 107. The data could include (i) an eUICC identity 107a, (ii) a profile 107c, (iii) an eUICC public key 214, (iv) an eUICC subscription manager public key 220 and private key 222, (v) an eUICC profile key 107b with an associated eUICC profile identity 107e, (vii) a module identity 110 (for embodiments where the module identity 110 for the eUICC 107 is known before the eUICC 107 sends and receives data with the eUICC subscription manager 109), (viii) and parameters for a symmetric ciphering algorithm 211 and an asymmetric ciphering algorithm 219 used by the eUICC 107. The parameters for a symmetric ciphering algorithm 211 and an asymmetric ciphering algorithm 219 used by the eUICC 107 could specify the ciphers used, such as (i) selecting an exemplary 128 or 192 bit keys for use with an AES cipher for a symmetric ciphering algorithm 211 used with a eUICC 107 and eUICC identity 107a, and (ii) selecting an exemplary elliptic curve or RSA algorithm for use with an asymmetric ciphering algorithm 219. The eUICC subscription manager 109 could also record related data for the operation of eUICC 107 with eUICC subscription manager 109 in a step 302a.

At a step 302a, the eUICC subscription manager 109 could receive the profile 107d from the mobile network operator 104, and an exemplary profile 107d is depicted and described in connection with Figure 2a. Or, eUICC subscription manager 109 could receive a subset of data for the exemplary profile 107d from the MNO 104 in a step 302a without receiving the entire profile 107d. As one example, the MNO 104 may not know the eUICC profile identity 107e for the eUICC profile 107d, and thus the MNO 104 may not send the complete profile 107d but the MNO 104 could send data for the profile 107d to the eUICC subscription manager 109 in a step 302a. In an exemplary embodiment, the eUICC subscription manager 109 could receive a subset of data for the profile 107d using the IP network 111 over a secured link or connection to the MNO 104. The profile 107d in a step 302a could include both ciphertext 208b and plaintext of a set of network parameters 201, a first network module identity 202, and a first key K 203. As depicted and described in connection with Figure 2a, the ciphertext 208b could comprise an encrypted second key K 204a. The ciphertext 208b could also include the second network

Petitioner Samsung Ex-1004, 0418

module identity 209a. In an exemplary embodiment, the plaintext first key K 203 could be optionally omitted from being received from an MNO 104 in a step 302a, and the eUICC subscription manager 109 can receive the first key K 203 in the form of a ciphertext 208c below in a step 302b. The eUICC subscription manager 109 could use a server or a plurality of servers similar to a server 105 in order to take the processing and communication steps described herein for an eUICC subscription manager 109 in this step 302a and also additional steps for an eUICC subscription manager 109 described throughout Figure 3.

After a module 101 powers up and established connectivity with the IP network 111, an eUICC 107 operating in a module 101 could then perform a step 205 in order to receive an eUICC profile 107c using the IP network 111. The use and operation of a step 205 is also depicted and described in connection with Figure 2a above. In a step 205, an eUICC 107 could send an eUICC identity 107a to the eUICC subscription manager 109. The module 101 could use a network application 101x to send the eUICC identity 107a, such as the network application 101x writing data with the eUICC identity 107a to a physical interface 101a, and the physical interface 101a could include a radio 101z. Or, using the exemplary embodiment illustrated in Figure 1f above, the eUICC 107 could be associated with an IP address 106c, and the eUICC 107 could send the eUICC identity 107a to the eUICC subscription manager 109 without using a separate network application 101x associated with the wireless network 102. During a step 205 for a module 101 or eUICC 107, an eUICC subscription manager 109 could receive the eUICC identity 107a and perform a step 302b. In an exemplary embodiment, both a module identity 110 and an eUICC identity 107a could be sent by an eUICC 107 or a module 101 in a step 205. Or, the eUICC identity 107a could comprise a module identity 110, and the module identity 110 could be sent in a step 205. Other possibilities exist as well for identifying a module 101 or an eUICC 107 with an eUICC subscription manager 109 without departing from the scope of the present invention.

In an exemplary embodiment, a message with the eUICC identity 107a in a step 205 could include a digital signature, where the digital signature is processed using (i) the eUICC

Petitioner Samsung Ex-1004, 0419

private key 215 recorded in a step 301 and (ii) a digital signature algorithm 221. The message with the eUICC identity 107a and a digital signature in a step 205 could preferably include a random number or string, including a nonce or a "number used once" such as, but not limited to, an exemplary security token 212 in order to prevent replay attacks.

An eUICC subscription manager 109 can take several actions in a step 302b after receiving an identity for the eUICC 107 or module 101. A first action in a step 302b could comprise authenticating an eUICC 107 or a module 101 based on the eUICC identity 107a received in the message. In a step 302b, eUICC subscription manager 109 can authenticate the message with eUICC identity 107a according to message digest, or using the eUICC profile key 107b which could be recorded in the eUICC 107 in a step 301 above. In addition, the eUICC subscription manager could authenticate using a digital signature algorithm 221, where the message with the eUICC identity 107a could include a digital signature, as described in the paragraph above.

Both the eUICC 107 and the eUICC subscription manager 109 could use the eUICC profile key 107b as a cipher key with a symmetric ciphering algorithm 211 to encrypt/decrypt data sent with the eUICC identity 107a, where the successful encryption and decryption of data with eUICC identity 107a using the eUICC profile key 107b on both ends could be confirmation that the eUICC 107 or module 101 is authenticated, since both parties would only be able to mutually successfully encrypt and decrypt by sharing the same eUICC profile key 107b. In another embodiment, the eUICC profile key 107b could be used as a private key with a digital signature algorithm 211 (instead of the eUICC private key 215), in order for the eUICC 107 with the eUICC 107a to be authenticated. For embodiments where the module 101 with the eUICC 107 sends a digital signature with the eUICC identity 107a, the eUICC subscription manager 109 could use the eUICC identity 107a to select the eUICC public key 214 or eUICC profile key 107b from a database. In this manner, the eUICC subscription manager 109 could communicate with a plurality of eUICCs 107 and select the appropriate keys using the eUICC identity 107a.

Petitioner Samsung Ex-1004, 0420

A second action in a step 302b could comprise the eUICC subscription manager 109 authenticating with an eUICC 107 or a module 101. The eUICC subscription manager 109 could also authenticate with an eUICC 107 at a step 302b within a step 205, such that eUICC 107 can confirm an identity of the eUICC subscription manager 109, using any of the same or equivalent steps described in the paragraph above for an eUICC 107 to authenticate with an eUICC subscription manager 109. The eUICC subscription manager 109 could send the eUICC 107 a digital signature processed using a digital signature algorithm 221 and the eUICC subscription manager private key 222. The eUICC 107 could verify the digital signature using a eUICC subscription manager public key 220 (which could be recorded with an eUICC 107 in a step 301). The eUICC 107 could also receive data encrypted with a eUICC profile key 107b, and successful decryption of the data by the eUICC 107 using a symmetric ciphering algorithm 211 could confirm the eUICC subscription manager 109 also holds the eUICC profile key 107b. Note that a system 300 could include multiple eUICC keys 107b, such that a first eUICC profile key 107b is used with a step 301 and step 205 in Figure 3, and a second eUICC profile key 107b could be used with a subsequent step 206 below. Other possibilities exist as well for an eUICC 107 and an eUICC subscription manager 109 to perform a 2-way authentication in a step 205 and a step 302b in Figure 3 without departing from the scope of the present invention.

In another exemplary embodiment, where data received from an MNO 104 does not include a plaintext first key K 203 for inclusion in a profile 107d, for a third action in a step 302b, the eUICC subscription manager 109 could send the eUICC identity 107a (or the module identity 110) and the eUICC public key 214 to the MNO 104. In this embodiment, the MNO 104 could also use the key ciphering algorithm 216 depicted and described in connection with Figure 2e above in order to encrypt the first key K 203 with the eUICC public key 214. The output of an MNO 104 using a key ciphering algorithm 216 could comprise a ciphertext 208c of an encrypted first key K 203. Thus, at a step 302b for the embodiment described in this paragraph, the eUICC subscription manager 109 could receive the first key K 203 for a profile 107d as ciphertext 208c (instead of a plaintext first key K 203 for profile 107d in Figure 2a), In this

Petitioner Samsung Ex-1004, 0421

manner, the first key K 203 in a profile 107d could be recorded as ciphertext 208c, which is also depicted and described as an optional format for the first key K 203 in Figure 2a and Figure 2e.

In an exemplary embodiment, the MNO 104 can send the ciphertext 208c only after a user 113 conducts a separate authentication step 308b below. In other words, a step 308b could also be used concurrently with a step 302b, where the step 302b includes the receipt of an encrypted first key K 203 in a ciphertext 208c. In this manner, the MNO 104 can retain control over the release of an encrypted first key K 203, such that the first key K 203 in a ciphertext 208c is only received by an eUICC subscription manager 109 in a step 302 or a eUICC 107 in a step 205 after a user 113 (associated with the module 101 with the eUICC 107) authenticates with the MNO 104. In this embodiment, a separate authentication step 308b below can be optionally omitted, and the use of an encrypted second key K 204a in ciphertext 208b can also be omitted. In this embodiment, a user 113 of the module 101 can access the wireless network 102 of the mobile network operator 104 using the first key K 203 which has been (i) encrypted by the mobile network operator 104 using a key ciphering algorithm 216 in a step 302b, and (ii) only available to module 101 or eUICC 107 (or eUICC subscription manager 109) after a user 113 conducts an authentication step 308b with MNO 104.

After the eUICC subscription manager 109 receives and/or processes all the data for a profile 107d, including subsets of data from a MNO 104 described for this step 302b above, a fourth action in a step 302b could comprise the eUICC subscription manager 109 ciphering a profile 107d using a profile ciphering algorithm 210, in order to convert profile 107d with plaintext into a profile 107c with ciphertext. Some elements in a profile 107c could remain plaintext as well, such as the exemplary profile identity 107e. The eUICC subscription manager 109 could use an eUICC profile key 107b, where the eUICC profile key 107b in a profile ciphering algorithm 210 can be different than an eUICC profile key 107b used to authenticate eUICC 107 with eUICC identity 107a. Or, the same eUICC profile key 107b could be used to both cipher profile 107d and authenticate eUICC 107. Note that this fourth action in a step 302b could also take place at an earlier time than at step 302b, such that eUICC subscription manager

Petitioner Samsung Ex-1004, 0422

109 could assemble and cipher the profile 107d into a profile 107c at an earlier time, such as before receiving the eUICC identity 107a, or concurrent with a step 301a. Other possibilities exist as well for the timing and sequence for an eUICC subscription manager to assemble and process a profile 107c without departing from the scope of the present invention.

After a step 302b, the eUICC subscription manager 109 can send the authenticated eUICC 107 a profile 107c in a step 205, as depicted in Figure 3. Either the eUICC subscription manger 109 or the eUICC 107 can select the profile 107c to be received by the eUICC 107. In one embodiment, a module 101 can search for radio beacons from base stations 103 for wireless networks 102 surrounding the module 101, and upon finding new possible wireless network 102 to connect with, the module 101 or eUICC 107 could query or request the eUICC subscription manager 109 for a profile 107c associated with a mobile network operator 104 for a radio beacon observed by the module 101. Commercial business arrangements among the user of module 101, the eUICC subscription manager 109, and the mobile network operator 104 can determine the availability of a profile 107c for a module 101 with an eUICC 107.

In another embodiment, the eUICC subscription manager 109 could periodically send the module 101 and/or eUICC 107 new profiles 107c as they become available to a user 113 of a module 101 or available to the eUICC subscription manager 109. In a preferred embodiment, the eUICC subscription manager 109 can send the profile 107c to the module 101 using a network application 101x, where the network application 101x forwards the data to the eUICC 107. As described above in this Figure 3, the network application 101x could communicate with the eUICC 107 using the operating system 101h as illustrated in Figure 1e, and other possibilities exist as well. Note that eUICC subscription manager 109 sends the profile 107c, where the network access credentials (including the first key K 203) are encrypted with an eUICC profile key 107b, and in this manner intermediate nodes on the IP network 111 would not feasibly be able to read the data within the profile 107c.

In an exemplary embodiment, the eUICC subscription manager 109 can send the module 101 a pointer, uniform resource locator (URL), domain name, or related address for a location of

Petitioner Samsung Ex-1004, 0423

the eUICC profile 107c in a step 205 as opposed to the actual, full profile 107c. In this embodiment, the module 101 could receive the pointer, uniform resource locator, domain name, or related address for the location of the eUICC profile 107c and subsequently download the eUICC profile 107c from an IP address associated with the pointer, uniform resource locator, domain name, or related address for a location of the eUICC profile 107c.

As depicted in Figure 3, after receiving the profile 107c from the eUICC subscription manager 109 in a step 205, the eUICC 107 can receive data for decrypting the profile 107c in a step 303. Note that if eUICC profile key 107b (in the form of a symmetric key as illustrated in Figure 2b) has already be shared between the eUICC 107 and the eUICC subscription manager 109 before a step 206 below, then a step 303 could separately be omitted. For example, if an eUICC profile key 107b has been recorded with an eUICC 107 in a module 101 by a manufacturer of module 101, then that eUICC profile key 107b could be used in a step 206 below, and a separate step 303 could be omitted. In other exemplary embodiments, the eUICC 107 can receive data for processing or deriving the eUICC profile key 107b for a step 206 below using the step 303 illustrated in Figure 3. A step 303 can include the receipt by eUICC 107 of either (i) an encrypted eUICC key 218, or (ii) data for a key exchange. The encrypted eUICC key 218 received by an eUICC 107 in a step 303 could comprise an eUICC profile key 107b that is ciphered using a key ciphering algorithm 216 illustrated in Figure 2e. For embodiments where data for a key exchange is received in a step 303, the algorithms used with a key exchange could comprise a Diffie Hellman key exchange, or an Elliptic Curve Diffie Hellman key exchange (ECDH).

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. A summary of ECDH is included in the Wikipedia article titled “Elliptic Curve Diffie-Hellman” (http://en.wikipedia.org/wiki/Elliptic_curve_Diffie %E2%80%93Hellman from September 24, 2013, which is herein incorporated by reference. An ECDH key exchange in a step 303 could

Petitioner Samsung Ex-1004, 0424

comprise the message received by a eUICC 107 including a common base point G. The base point G could also be sent from an eUICC 107 to eUICC subscription manager 109. The base point G for an ECDH key exchange in a step 303 could also be recorded with the eUICC in a step 301 above, and in this case the message at a step 303 received by an eUICC 107 could comprise a signal to initiate or use a key exchange for deriving the eUICC profile key 107b. Note that the eUICC subscription manager 109 and the eUICC 107 could take additional steps to process the eUICC profile key 107b after an ECDH key exchange at step 303, such as taking the output of an ECDH key exchange and inputting that output into a secure hash algorithm in order to obtain the eUICC profile key 107b. Other algorithms besides an ECDH or Diffie Hellman key exchange can be utilized as well at a step 303, including a key exchange according to the American National Standards Institute (ANSI) standard X-9.63.

After completing a step 303, an eUICC 107 operating in a module 101 could read and utilize the eUICC profile key 107b. In embodiments where the eUICC profile key 107b in a step 303 above comprises an encrypted eUICC key 218, a step 217 from Figure 2e can be utilized by the eUICC 107 in order to decrypt the eUICC key 218 into a plaintext of eUICC profile key 107b. The plaintext eUICC profile key 107b can be used by the eUICC 107 in a step 206 to decrypt (x) the profile 107c received in a step 205 above into (y) a profile 107d. The use of an eUICC profile key 107b for a step 206 is also depicted and described in connection with Figure 2a above and also Figure 2b. Plaintext within a profile 107d can be read after a step 206, although in exemplary embodiments and as illustrated in Figure 2a, the profile 107d can continue to record ciphertext 208b and ciphertext 208c.

In an exemplary embodiment, after a step 206 in Figure 3 to convert received profile 107c to profile 107d, if (A) a ciphertext 208c that includes the first key K 203 is present in profile 107d (as depicted in Figure 2a above), then (B) eUICC 107 could also use a key deciphering algorithm 217 on ciphertext 208c in order to extract the plaintext first key K 203. Note that ciphertext 208a could be ciphered by an eUICC subscription manager 109 (using a profile ciphering algorithm 210) and ciphertext 208b and/or ciphertext 208c could be encrypted

Petitioner Samsung Ex-1004, 0425

by a mobile network operator 104 (using a key ciphering algorithm 216). In other words, a module 101 with an eUICC 107 can use (i) a profile deciphering algorithm 206 with an eUICC profile key 107b to decrypt ciphertext 208a, (ii) a key deciphering algorithm 217 with an eUICC private key 215 to decrypt ciphertext 208c, and/or (ii) a key K deciphering algorithm 207 with a symmetric key 127 to decrypt ciphertext 208b.

After reading plaintext in profile 107d, module 101 could then utilize the profile 107d to conduct a first authentication 304 with the mobile network operator 104. As depicted in Figure 3, the first authentication 304 can comprise (i) module 101 sending an attach message 305 with network module identity 202, (ii) the eUICC 107 and module 101 receiving a RAND 118, (iii) the eUICC 107 using a step 306 in order to calculate a RES 119, and (iv) the module 101 sending the RES 119. Although not illustrated in Figure 3, a first authentication 304 could include other data such as receiving the equivalent of an "OK" message upon successful authentication, the receipt of additional network parameters 202 after successful authentication, etc. The module 101 can use a profile 107d from a step 206 above in order to conduct the first authentication 304. The profile 107d in an eUICC 107 could be selected and activated in order to connect with a wireless network 102 associated with mobile network operator 104. As contemplated herein and throughout the present invention, an activated profile 107d can comprise a selected and enabled network access application state as illustrated in Figure D.1 of ETSI TS 103 383 v.2013-02 for the activated profile 107d, and other possibilities exist as well. As illustrated in Figure 3 after a step 206, the module 101 can use a network application 101x in order to attach to the wireless network 102 and communicate with the mobile network operator 104.

Within a first authentication 304, the module 101 can send a first attach message 305, and the first attach message 305 can include the first network module identity 202. With a 4G LTE network, the first attach message 305 could comprise a radio resource connection request message, or a similar message could be utilized with other wireless networking standards as well, such as LTE Advanced or WiMAX. An exemplary radio resource connection request is described in section 5.3.3 within ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal

Petitioner Samsung Ex-1004, 0426

Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification", which is herein incorporated by reference. Although not illustrated in Figure 3, the module 101 and wireless network 102/mobile operator 104 could take additional related steps before sending the exemplary first attach message 305, such as, but not limited to, module 101 synchronizing a clock 160 with wireless network 102, module 101 sending a message on a random access control channel (RACH) in order to have a timeslot and frequencies for sending the first attach message 305, etc.

As depicted in Figure 3, after receiving and processing the first attach message 305, the mobile network operator can send a first random number (RAND) 118. Although not illustrated in Figure 3, a network authentication token "AUTN" and a sequence number could be sent with the first RAND 118. An exemplary format for the use of a RAND 118 with a response RES 119 is described in ETSI standard TR 131 900 v.10.0.0 and related documents. In a first authentication 304 the module 101 and the eUICC 107 can receive the first RAND 118. The eUICC 107 can conduct a step 306 with an input of the first RAND 118 and the first key K 203 in order to calculate a first RES 119. The use of a RAND 118 with a RES 119 in a step 306 could comprise a general use of a message digest authentication, and another exemplary message digest authentication is also described in IETF RFC 2617, titled "HTTP Authentication: Basic and Digest Access Authentication". After receiving the exemplary first RAND 118 message, in order to conduct a first authentication 304, module 101 using an eUICC 107 could take steps to demonstrate to MNO 104 that module 101 has access to the same first key K 203 as recorded by the MNO 104 in a step 302a or step 302b above. MNO 104 could record the expected RES 119 value with a set of authentication vectors 117 for the first network module identity 202, as depicted in Figure 1d and Figure 1e.

Module 101 can properly respond to a challenge/nonce (such as a first RAND 118) in a message digest authentication by sending a secure hash value calculated using (i) the challenge/nonce and (ii) the first key K 203. The secure hash value can comprise the first RES 119. In exemplary embodiments, eUICC 107 and wireless network 102 could use algorithms

Petitioner Samsung Ex-1004, 0427

specified in ETSI TS 135 205 – 209, as well as subsequent and related standards, in order for module 101 using eUICC 107 to (i) calculate a secure hash value, and (ii) process related steps for a first authentication 304. After processing a first RES 119 in a step 306 using the first key K 203, the eUICC 107 could send the first RES 119 to the network application 101x in module 101. Module 101 could then send the first RES 119 to the mobile network operator 104 using the wireless network 102, as depicted in Figure 3 and thereby complete a first authentication step 304 for the module 101.

In another embodiment for a first authentication step 304, (i) module 101 could send (i) the first network module identity 202 a digital signature processed using a digital signature algorithm 221 and the eUICC private key 215, and (ii) MNO 104 could verify the digital signature using a digital signature algorithm 221 and the eUICC public key 214. Other possibilities exist as well for steps within a first authentication 304 using a eUICC private key 215 with the first network module identity 202 or the eUICC identity 107a in a first authentication step 304 without departing from the scope of the present invention. In an exemplary embodiment, as depicted in Figure 1f above, the eUICC 107 could include an IP address 106c with an interface identifier 106e associated with the eUICC 107, and in this case the module 101 could send the first RES 119 value from the eUICC 107 to the MNO 104 through the wireless network 102.

In a step 308a the mobile network operator 104 can receive the first RES 119. A server 105 such as a mobility management entity (MME) for the mobile operator network 104 associated with the wireless network 102 could compare the received first RES 119 with an internally recorded RES 119 from the authentication vector 117. As noted above, the authentication vector 117 could be received by the server 105 from the HSS of the mobile network operator 104 before a step 308a. If the received first RES 119 matches the internally stored first RES 119 value, the wireless network 102 and mobile network operator 104 can consider or process that the module 101 is authenticated for a step 308a. The wireless network 102, the MNO 104, and the module 101 can take subsequent steps (not shown) for the module

Petitioner Samsung Ex-1004, 0428

101 to access the IP network 111, in order to conduct authentication of the module 101 or a user associated with the module 101 with a second factor in a step 308b below.

In a step 308b, the mobile network operator 104 can conduct a separate authentication of either a user 113 associated with a module 101 or the module 101 using a second factor. In other words, the mobile network operator 104 can use a step 308b to authenticate the user 113 of module 101 or the module 101 using steps and a process that is different than the first authentication 304. Note that this use of a separate authentication step 308b can be different than conventional technology used in authenticating a module 101 in a step 304, since other values and tokens besides the first key K 203 can be used in the authentication step 308b. The additional authentication step 308b can be useful for a mobile network operator 104 to authenticate a module 101 with an eUICC 107 and profile 107d, since the profile 107d with the first key K 203 may be transferred to module 101 in a communications channel outside the control of mobile network operator 104. As one example, the profile 107d with the first network key K 203 could be transferred to an eUICC 107 from the eUICC subscription manager 109 using an IP network 111, as depicted in Figure 3 in a step 205. The mobile network operator 104 may not have control over the IP network 111 used in a step 205. The mobile network operator 104 may not have control over the security keys and algorithms used to encrypt the profile 107d into a profile 107c, and thus the security of the first key K 203 upon which the MNO 104 depends for authentication and ciphering of data with module 101 may be outside the control of MNO 104. As one example, the MNO 104 may not be able to separately authenticate the identity of a user of module 101 with the eUICC 107, before the profile 107d was received by module 101 and eUICC 107 in a step 205.

Consequently, without a separate authentication step 308b the user 113 of module 101 with the eUICC 107 may be unknown to MNO 104, and a separate identity of the user 113 or module 101 (other than network module identity 202) may preferably be authenticated in a step 308b. Thus, a MNO 104 may use a separate authentication step 308b in order to authenticate a user 113 of module 101 with the eUICC 107 and the first key K 203 in exemplary embodiments.

Petitioner Samsung Ex-1004, 0429

The user 113 can have a contractual or business relationship with MNO 104 in order to pay for voice and/or data services from the MNO 104, and thus the MNO 104 can preferably identify and authenticate a user 113 in a step 308b.

A step 308b can comprise the authentication and/or secure identification of (i) a user 113 of module 101 or (ii) module 101 using a second factor. Although a step 308b is depicted in Figure 3 as being performed after a first authentication 304, a step 308b could be performed before a step 304 (including with a step 302b as described in step 302b above). The use of a second factor in an authentication step 308b can comprise a two-factor authentication, where the first factor can be the successful completion of authentication using a step 304 and step 308a described above. The steps for authenticating a user 113 or module 101 in a step 308b could comprise many different forms without departing from the scope of the present invention. In one embodiment, where the user 113 of module 101 comprises a subscriber to telecommunication and data services from MNO 104, the user 113 could present identification to a representative of the MNO 104 in a step 308b. The identification could be in the form of a physical identity such as, but not limited to, a drivers license or a passport (along with a value that can be associated with the eUICC profile 107d such as the module identity 110 or the eUICC identity 107a). The representative of the MNO 104 could record the identification in a web browser with connectivity to a database shared by a server 105.

In another embodiment of an authentication of a user 113 of module 101 (with the eUICC profile 107d recorded with an eUICC 107 in module 101 from a step 205) could enter information into a web page provided by MNO 104, where the user 113 first (i) authenticates on the web page and then (i) enters identification information for the module 101 or eUICC 107. The user 113 could first authenticate with the MNO 104 via a web page by entering a valid identity and a password (where the identity and password for the web page in a step 308b could be previously established between the user 113 and the MNO 104 before a step 308b). In another embodiment for a step 308b, a user 113 could call a telephone number operated by or associated with a MNO 104 and provide identification information via voice or entering

Petitioner Samsung Ex-1004, 0430

information such as dual-tone multi-frequency (DTMF) digits via interactive voice response (IVR). The identification information could include either a credit card number or a personal identification number (PIN) for the user 113 (where the PIN may be previously shared or established between the user 113 and the mobile network operator 104). The user 113 could also send a text message to MNO 104 from module 101 (i) using the module 101 authenticated link with MNO 104 established in a first authentication 304, where (ii) the text message include identification information for a user 113.

In accordance with preferred exemplary embodiments for the verification of an identity of user 113 in a step 308b (including an authentication of user 113 in a step 308b), the user 113 can send data to a MNO 104 from module 101 using a data connection via wireless network 102 associated with (and established after) the first authentication 304. In this manner, data and voice connectivity between the MNO 104 and module 101 could be established with a first authentication step 304, and the user 113 and MNO 104 can conduct an authentication step 308b (or equivalently a verification of an identity of the user 113) to confirm the identity of the user 113 via the established data and voice connectivity using the wireless network 102. In other words, the user 113 could verify or authenticate an identity of the user 113 of module 101 through the wireless network 102 in a step 308b, where (a) module 101 had conducted a first authentication step 304 and 308a with MNO 104 using the first key K 203 recorded in a profile 107d, in order to (b) support or conduct a separate verification or authentication of a user 113. In an exemplary embodiment, the user 113 could enter identifying information for a step 308b in a web page accessed through a user interface 101j on module 101, where data connectivity for the web page is provided to module 101 through the wireless network 102 after a first authentication step 304.

The authentication or verification of user 113 identity in a step 308b can comprise authenticating module 101with a second factor, where the first factor can comprise the first key K 203 and the second factor can comprise information provided by a user 113 in a step 308b. Other possibilities exist as well for those of ordinary skill in the art for (a) a user 113 of module

Petitioner Samsung Ex-1004, 0431

101 with the first key K 203 to (b) authenticate or verify an identity of the user 113 in a step 308b without departing from the scope of the present invention. In these exemplary embodiments for a user 113 to authenticate or verify an identity for the user 113 for module 101 with the MNO 104, the MNO 104 could record information or data received from the user 113 in a database, such that a server 105 for MNO 104 sends the symmetric key 127 in a step 309 below after an identity of the user 113 is verified or authenticated in a step 308b. In exemplary embodiments illustrated in Figure 3, the module 101 can access the wireless network 102 with the first key K 203 in order to (i) establish communication with the IP network 111, (ii) support authentication of a user 113 in a step 308b through the IP network 111, and then (iii) subsequently receive a symmetric key 127 in order to decrypt a ciphertext 208b with a second key K 204a.

In other exemplary embodiments, module 101 could comprise a module supporting "machine-to-machine" applications and communications, and the module could be different than a traditional mobile phone or smartphone for (i) placing voice telephone calls or (ii) supporting a user interface 101j in the form of a touch screen and web browser. The module 101 could include a sensor 101f for collecting data and an actuator 101y for controlling or changing a state associated with a monitored unit for the module 101. In these embodiments, and as depicted and described in connection with Figure 1a, module 101 can be associated with an M2M service provider 115, and the M2M service provider 115 could be associated with a plurality of modules 101, as opposed to an individual with a telephone number for voice services to module 101.

Each of the different modules 101 in the plurality of modules 101 could include different values for module identities 110, eUICC identities 107a, profile identities 107e, and the first network module identities 202. In these embodiments for a step 308b where the module 101 supports M2M applications for an M2M service provider 115, in a step 308b in Figure 3, the MNO 104 could verify that (a) module 101 with eUICC 107 and the profile 107d from a step 304 is (b) properly associated with an M2M service provider 115. In exemplary embodiments, the MNO 104 ould conduct a step 308b by securely or properly determining that an identity from

Petitioner Samsung Ex-1004, 0432

module 101 is associated with M2M service provider 115, and an exemplary identity for module 101 include any of a module identity 110, an eUICC identity 107a, a profile identity 107e, and/or the first network module identity 202.

In exemplary embodiments where module 101 supports M2M application and the module 101 is associated with an M2M service provider 115, MNO 104 could take several possible actions in a step 308b for authenticating or verifying that an identity from module 101 in Figure 3 is associated with an M2M service provider 115. The proper association of an identity of module 101 with M2M service provider 115 may be necessary or useful for contractual and business relationships between MNO 104 and M2M service provider 115, such as, but not limited to, allowing MNO 104 to bill or invoice M2M service provider 115 for data services that MNO 104 provides to module 101. In a first exemplary embodiment for a step 308b in Figure 3 where module 101 supports M2M applications with a M2M service provider 115, MNO 104 could securely send to M2M service provider 115 an identity of module 101, such as, but not limited to module identity 110, eUICC identity 107a, profile identity 107e, and/or the first network module identity 202 through an IP network 111. The MNO 104 could also send the identity of module 101 in a query or request message. Although not illustrated in Figure 3, the MNO 104 could also send the M2M service provider 115 a digital signature received from module 101 before a step 308b, where the digital signature was (i) processed by module 101 using a digital signature algorithm 221 and an eUICC private key 215, and (ii) sent from the module 101 to the MNO 104.

In a step 308b, the M2M service provider 115 could (i) receive the identity of module 101 (such as, but not limited to module identity 110, eUICC identity 107a, profile identity 107e, and/or the first network module identity 202), (ii) verify or determine the identity of module 101 properly belongs to M2M service provider 115, and (iii) send a response confirming the module 101 with the identity is validly associated the M2M service provider 115. The response from the M2M service provider 115 (or data within a message from M2M service provider 115 to MNO 114) for a step 308b can comprise a second factor for MNO 104 in authenticating module 101

Petitioner Samsung Ex-1004, 0433

with eUICC 107 and profile 107d. In this manner, MNO 104 can confirm module 101 with the first network identity 202 is authenticated or verified as belonging to or being associated with M2M service provider 115 in a step 308b.

In another exemplary embodiment for a step 308b, the M2M service provider 115 could also send MNO 104 a list of pre-authorized identities for one or a plurality of modules 101 before a step 308b (and in this case the list can comprise the second factor to authenticate module 101). MNO 104 could query the list of identities received upon receiving an identity of module 101, such as, but not limited to, the first network module identity 202 received in the first attach message 305. Other possibilities exist as well for an MNO 104 to authenticate or verify that an identity of module 101 is associated with a M2M service provider 115 in a step 308b without departing from the scope of the present invention.

After successfully verifying or confirming in a step 308b that module 101 in Figure 3 is associated with a known user 113 or M2M service provider 115, MNO 104 can send a symmetric key 127 in a step 309. A network application 101x in the module 101 can receive the symmetric key 127 and the module 101 can forward the symmetric key 127 to the eUICC 107. As depicted and described in connection with Figure 2a and Figure 2c, the symmetric key 127 can be used by module 101 to decrypt the ciphertext 208b, where the ciphertext 208b can include a second key K 204a. The symmetric key 127 can also previously be used by MNO 104 to encrypt the ciphertext 208b. The ciphertext 208b could be delivered to eUICC subscription manager 109 for including the ciphertext 208b in the profile 107d, as described above in step 302a. The ciphertext 208b could be sent to module 101 from the eUICC subscription manager 109 across the IP network 111 as profile 107c in a step 205 as described above in this Figure 3.

In exemplary embodiments, the MNO 104 can send the symmetric key 127 in a step 309 through the wireless network 102, where the connection between module 101 and MNO 104 could be initiated by the first attach message 305 and authenticated by a first authentication 304. Since the MNO 104 controls the nodes and ciphering steps for the transmission of symmetric key 127, the symmetric key 127 can be securely sent by MNO 104 and received by module 101 with

Petitioner Samsung Ex-1004, 0434

ciphering and keys used at the data-link layer under the control of MNO 104 (whereas MNO 104 may not control the keys and ciphering of sending the first key K 203). Also note no entities, including the module 101, a user 113, an M2M service provider 115, an eUICC subscription manager 109, or unauthorized third parties could feasibly read the ciphertext 208b with the second key K 204a until they receive the symmetric key 127.

In an exemplary embodiment of a step 309 in Figure 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. As described in connection with a key ciphering algorithm 216 in Figure 2e, the MNO 104 could select and read the eUICC public key 214 (using a received associated identity such as the first network module identity 202), and use an asymmetric ciphering algorithm 219 to encrypt the symmetric key 127. 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 and the asymmetric ciphering algorithm 219. For a step 309 in Figure 3, the use of encryption for a symmetric key 127 with an asymmetric ciphering algorithm 219 is optional, and the symmetric key 127 could be sent in a form where encryption is applied at the data-link layer according to standards for the wireless network 102. Other possibilities exist as well for a module 101 to securely receive a symmetric key 127 in a step 309 without departing from the scope of the present invention. As described above in connection with a step 302b, in exemplary embodiments, the module 101 receives the symmetric key 127 after the MNO 104 authenticates or verifies that a user 113 or M2N service provider 115 is associated with module 101, and until the receipt of the symmetric key 127 the ciphertext 208b cannot be feasibly decrypted.

After a step 309, a module 101 with an eUICC 107 can use the symmetric key 127 to decrypt ciphertext 208b, where ciphertext 208b can include the second key K 204a. A module 101 or eUICC 107 can use a key K deciphering algorithm 207 with input from the received symmetric key 127 and the ciphertext 208b from profile 107d to output a plaintext second key K

Petitioner Samsung Ex-1004, 0435

204. Although not illustrated in a step 207 in Figure 3, but as illustrated in a step 207 in Figure 2a, a module 101 can use an eUICC 107 to also decrypt a second network module identity 209a for the second key K 204 using the symmetric key 127. The second network module identity 209a can be recorded in the ciphertext 208b. The second network module identity 209a can be different than the first network module identity 202, such as a different number or value for an IMSI. The second network module identity 209a can be the same length as the first network module identity 202. The use and operation of a key K deciphering algorithm 207 is also depicted and described in connection with Figure 2a and Figure 2e above.

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 such that the plaintext second key K 204 remains available to module 101 after power or a battery 101k is removed from module 101. The plaintext second key K 204 could also be recorded in a protected memory within module 101, such that the operating system 101h or CPU 101b may prevent read or write access to the protected memory by other processes than the eUICC 107. In other words, with a protected memory, other applications such as, but not limited to, applications that are downloaded from an “app store” or equivalent and installed by end users on the module 101 may be prevented by the operating system 101h from having access to the plaintext second key K 204 recorded in the protected memory.

In another embodiment, a module 101 may optionally not store the plaintext second key K 204 in nonvolatile memory, such that the second key K 204 continues to be recorded for a long-term basis only as ciphertext 208b in a nonvolatile memory such as flash 101w. The module 101 could perform a key K deciphering algorithm 207 each time a plaintext second key K 204 is needed for authentication purposes, including related key derivation of a CK and IK plus other derived keys. In this manner (by storing the second key K 204 in ciphertext 208b in module 101) a plaintext second key K 204 may not be (i) stored in module 101 for a relatively long time such as several hours or longer, and also (ii) recorded outside a nonvolatile memory.

Petitioner Samsung Ex-1004, 0436

In another embodiment, (A) the plaintext second key K 204 is recorded only in a volatile memory within CPU 101b such as a register or cache memory, where access to the register or cache memory is limited to the eUICC 107, and (B) after a successful authentication using the second key K 204, such as, but not limited to, a second authentication 311 below, the plaintext second key K 204 is flushed from the register or cache memory within CPU 101b. In this manner, after (A) a first time that module 101 conducts a step 207 to obtain a plaintext second key K 204 and the module 101 completes a full power cycling, then (B) the plaintext second key K 204 may not be recorded in any of a volatile memory, a non-volatile memory, or a protected memory within module 101 (but module 101 could record an encrypted second key K 204a in a ciphertext 208b).

For the embodiments where the second key K 204 is not recorded as plaintext in a nonvolatile memory within module 101, the module 101 can perform a step 207 with a ciphertext 208b recorded in a nonvolatile memory a second time to process or obtain the plaintext second key K 204. In other words, the second key K 204 can be recorded on a long-term basis as a ciphertext 208b for eUICC 107 within module 101, in an exemplary embodiment, thereby increasing the security of the second key K 204. In this case, either (i) the symmetric key 127 could be recorded in a nonvolatile memory 101w in order to allow decrypting of the ciphertext 208b, or (ii) the module 101 could receive the symmetric key 127 a second time by conducting a step 309 a second time. The module 101 can reconnect with the wireless network 102 and the MNO 104 using the first network identity 202 and the first key K 203 a second time, after the module 101 has already received the symmetric key 127 a first time. The MNO 104 may optionally authenticate the user 113 or M2M service provider 115 a second time such as a second step 308b (before sending the symmetric key 127 a second time) in order to confirm a second use of the first key K 203 is authorized.

After a module 101 with an eUICC 107 processes a key K deciphering algorithm 207 to obtain a plaintext second key K 204, the module 101 can connect with the wireless network 102 and mobile network operator 104 using the second network module identity 209 and the second

Petitioner Samsung Ex-1004, 0437

network key 204. The module 101 using a network application 101x could send a second attach message 305 with the second network module identity 209. In another embodiment, the module 101 could send the second attach message 305 with the first network module identity 202, and in this case the MNO 104 could record from the previous steps 302b and 308b that a key K associated with the first network module identity 202 should change to the second key K 204.

But, given existing deployed infrastructure and systems for a mobile network operator 104, the use of two different keys K with the same network module identity may be more difficult to support, and for this case and with preferred embodiments, the module 101 attaches with the MNO 104 the second time with the second network module identity 209 that has been deciphered from (i) a ciphertext 208b in a step 207 above, or (ii) a ciphertext 208a in a step 206 above. The second attach message 305 can be equivalent to the first attach message 305, but with a change of module 101 sending the second network module identity 209. With a 4G LTE network, the second attach message 305 could comprise a radio resource connection request message, or a similar message could be utilized with other wireless networking standards as well, such as LTE Advanced or WiMAX. An attach message such as 305 in Figure 3 could also comprise module 101 using a globally unique temporary identity (GTUI) that can be associated with the second network module identity 209. Other possibilities exist as well for the format or structure of an attach message 305 without departing from the scope of the present invention.

After sending the second attach message 305, the module 101 with a eUICC 107 can conduct a second authentication 310 with the mobile network operator 104. The module 101 and eUICC 107 could take the equivalent steps as the first authentication 304 depicted and described in this Figure 3, but with a difference of using the second network module identity 209 and the second key K 204. In a second authentication 310, the mobile network operator 104 could send the module 101 a second RAND value 118 through the wireless network 102. A server 105 associated with MNO 104, such as, but not limited to, a HSS could have previously processed an authentication vector 117 comprising at least (i) the second RAND value 118, (ii) a network authentication token AUTN and sequence number (not shown), and (iii) a response value RES

Petitioner Samsung Ex-1004, 0438

119 for the second network module identity 209 and the second key K 204. The server 105 or HSS associated with the MNO 104 could send the authentication vector 117 to a server or MME that module 101 communicates with through the wireless network 102. The module 101 could receive the second RAND 118 using the network application 101x, and forward the second RAND 118 to the eUICC 107. The communication steps between a network application 101x and an eUICC 107 in Figure 3 could also use the steps depicted and described in connection with Figure 1e.

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. The MNO could record the second key K 204 in an authentication vector 117 a step 302a or step 302b above. Module 101 can properly respond to a challenge/nonce (such as a second RAND 118) in a message digest authentication by sending a secure hash value calculated using (i) the challenge/nonce and (ii) the second key K 204. The secure hash value can comprise the second RES 119. In exemplary embodiments, the eUICC 107 and wireless network 102 could use algorithms specified in ETSI TS 135 205 – 209, as well as subsequent and related standards, in order for module 101 using eUICC 107 to (i) calculate a secure hash value, and (ii) process related steps for a second authentication 310. After processing a second RES 119 in a step 311 using the second key K 204, the eUICC 107 could send the second RES 119 to the network application 101x in module 101. Module 101 could then send the second RES 119 to the mobile network operator 104 using the wireless network 102, as depicted in Figure 3 and thereby complete a second authentication step 310 for the module 101. In an exemplary embodiment, as depicted in Figure 1f above, the eUICC 107 could include an IP address 106c with an interface identifier 106e associated with the eUICC 107, and in this case the module 101 could send the second RES 119 value from the eUICC 107 to the MNO 104 through the wireless network 102.

Petitioner Samsung Ex-1004, 0439

At a step 312, the mobile network operator can receive the second RES 119 from the module 101 using the wireless network 102. A server 105 for the mobile operator network 104 associated with the wireless network 102 could compare the received second RES 119 with an internally recorded RES 119. The server 105 could receive an authentication vector 117 comprising at least the second RAND 118, second RES 119, and AUTN token for the second network module identity 209 before sending the second RAND 118 in a step 310 above. If the received second RES 119 matches the internally stored second RES 119 value, the wireless network 102 and mobile network operator 104 can consider or process that the module 101 is authenticated for a step 312. The wireless network 102, the MNO 104, and the module 101 can take subsequent steps (not shown) for the module 101 to access the IP network 111, including allowing module 101 to place and receive telephone calls and/or access the public Internet.

In an exemplary embodiment that utilizes the steps illustrated in Figure 3, the fist key K 203 can comprise a null value or the number zero, which is contemplated in standards and supported by commercial wireless networks 102 in order to support emergency services for a module 101 without a valid UICC or eUICC. The MNO 104 and wireless network 102 can provide limited access to the IP network 111, such that a user 113 of module 101 with a null or zero value for the first key K 203 could performs steps to authenticate or verify the user 113 identity in a step 308b. The limited access to the IP network 111 may not include access to the public Internet, but could include access to a server such as a web server for the user 113 to enter identification information. The data-link layer may not be encrypted due to the use of a null value for the first key K 203, but the application or transport layer could secure communication from a web browser on the module 101 to the web server, such as using transport layer security (TLS). Other possibilities exist as well for ciphering or securing data at the application or transport layer in a step 308b to authenticate a user 113 without encryption at the data-link layer (such as without encryption by the wireless network 102 due to a null value for first key K 203). In this embodiment where the first key K 203 comprises a null or zero value, after authentication of a user 113 or M2M service provider 115 in a step 308b, the second key K 204 used with a

Petitioner Samsung Ex-1004, 0440

second authentication 310 can comprise a regular key K such as a non-null value or a random number.

Figure 4

Figure 4 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments. The processes and operations, described below with respect to all of the logic flow diagrams may include the manipulation of signals by a processor and the maintenance of these signals within data structures resident in one or more memory storage devices. For the purposes of this discussion, a process can be generally conceived to be a sequence of computer-executed steps leading to a desired result.

These steps usually require physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, or otherwise manipulated. It is convention for those skilled in the art to refer to representations of these signals as bits, bytes, words, information, elements, symbols, characters, numbers, points, data, entries, objects, images, files, or the like. It should be kept in mind, however, that these and similar terms are associated with appropriate physical quantities for computer operations, and that these terms are merely conventional labels applied to physical quantities that exist within and during operation of the computer.

It should also be understood that manipulations within the computer are often referred to in terms such as listing, creating, adding, calculating, comparing, moving, receiving, determining, configuring, identifying, populating, loading, performing, executing, storing etc. that are often associated with manual operations performed by a human operator. The operations described herein can be machine operations performed in conjunction with various input provided by a human operator or user that interacts with the computer.

Petitioner Samsung Ex-1004, 0441

In addition, it should be understood that the programs, processes, methods, etc. described herein are not related or limited to any particular computer or apparatus. Rather, various types of general purpose machines may be used with the following process in accordance with the teachings described herein.

The present invention may comprise a computer program or hardware or a combination thereof which embodies the functions described herein and illustrated in the appended flow charts. However, it should be apparent that there could be many different ways of implementing the invention in computer programming or hardware design, and the invention should not be construed as limited to any one set of computer program instructions.

Further, a skilled programmer would be able to write such a computer program or identify the appropriate hardware circuits to implement the disclosed invention without difficulty based on the flow charts and associated description in the application text, for example. Therefore, disclosure of a particular set of program code instructions or detailed hardware devices is not considered necessary for an adequate understanding of how to make and use the invention. The inventive functionality of the claimed computer implemented processes will be explained in more detail in the following description in conjunction with the remaining Figures illustrating other process flows.

Further, certain steps in the processes or process flow described in all of the logic flow diagrams below must naturally precede others for the present invention to function as described. However, the present invention is not limited to the order of the steps described if such order or sequence does not alter the functionality of the present invention. That is, it is recognized that some steps may be performed before, after, or in parallel other steps without departing from the scope and spirit of the present invention.

The processes, operations, and steps performed by the hardware and software described in this document usually include the manipulation of signals by a CPU or remote server and the maintenance of these signals within data structures resident in one or more of the local or remote memory storage devices. Such data structures impose a physical organization upon the collection

Petitioner Samsung Ex-1004, 0442

of data stored within a memory storage device and represent specific electrical or magnetic elements. These symbolic representations are the means used by those skilled in the art of computer programming and computer construction to most effectively convey teachings and discoveries to others skilled in the art.

At step 401, a module 101 can connect with a first wireless network 102. The first wireless network 102 could comprise a public land mobile network, a local area network such as WiFi, or the use of white-space spectrum. The module 101 could connect with the first wireless network 102 in order to obtain access to IP network 111 which could comprise the public Internet, although the IP network 111 could comprise a private network in some embodiments. Although not depicted in Figure 4, a step 401 could also comprise the module 101 connecting to a wired network through USB interface 101v. Upon conclusion of a step 401 the module 101 can use an IP address such as IP address 106b in Figure 1f in order to communicate with an eUICC subscription manager 109. As illustrated in Figure 1f, in an exemplary embodiment the eUICC 107 could also have an IP address 106c after a step 401, although the use of an IP address for eUICC 107 is not required and the module 101 can be associated with one IP address for all external communications.

The module 101 can then use a step 205 in order to receive an eUICC profile 107c. The eUICC profile 107c could be received from the eUICC subscription manager 109 using the wireless network 102 and/or IP network 111 from a step 401 above. The module 101 could record the received eUICC profile 107c with the eUICC 107, including sending the eUICC profile 107c to the eUICC 107 or sharing memory 101e or 101w between the eUICC 107 and a network application 101x. The module 101 could use a network application 101x in order to receive the eUICC profile 107 from the eUICC subscription manager in a step 205, as depicted and described in connection with Figure 3. The module 101 with an eUICC 107 could then decrypt the profile 107c in a step 206 using an eUICC profile key 107b. The eUICC profile key 107b could be recorded with an eUICC 107 before a step 206. The module 101 and/or eUICC 107 could receive the eUICC profile key 107b using a step 303 as depicted and described in

Petitioner Samsung Ex-1004, 0443

connection with Figure 3. The eUICC profile key 107b could be received using a key exchange, such as a Diffie-Hellman key exchange or an ECDH key exchange. Or, the eUICC profile key 107b could be recorded with the eUICC 107 by a module manufacturer. Other possibilities exist as well for a module 101 to record an eUICC profile key 107b before a step 206 without departing from the scope of the present invention. A module 101 and/or an eUICC 107 could use a profile deciphering algorithm 206 in a step 206, as depicted and described in connection with Figure 2a and Figure 2b. Upon conclusion of a step 206, a profile 107d could be recorded in an eUICC 107.

In a step 402, a module 101 can then select and activate the profile 107d from a step 206 in order to connect with a second wireless network 102. A module 101 could take several possible steps in order to select and activate the profile 107d. A module 101 could use radio 101z to search for radio beacons from base stations 103 for wireless networks 102 surrounding the module 101, and upon finding the second wireless network 102 to connect with, the module 101 could select the profile 107d. 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. A module 101 could receive an instruction from an eUICC subscription manager 109 in order to activate the profile 107d, where the instruction could be received through the first wireless network 102 in a step 401 above.

In another embodiment, a module 101 or eUICC 107 could query the eUICC subscription manager 109 through the first wireless network 102 before activating the profile 107d in a step 402. Commercial business arrangements among the user 113 of module 101, the eUICC subscription manager 109, and the mobile network operator 104 can determine the timing for activating a profile 107d for a module 101 with an eUICC 107 in a step 402, such as a user 113 entering a new contract for service with a MNO 104 for the profile 107d. As contemplated herein and throughout the present invention, an activated profile 107d can comprise a selected and enabled network access application state as illustrated in Figure D.1 of ETSI TS 103 383

Petitioner Samsung Ex-1004, 0444

v.2013-02 for the activated profile 107d. Other possibilities exist as well for a module 101 to activate a profile 107d in a step 402 without departing from the scope of the present invention.

In a step 304 in Figure 4, a module 101 using eUICC 107 can conduct a first authentication 304 with the second wireless network 102, using the first key K 203 recorded in the activated profile 107d. The module 101 could also send the first network module identity 202 from a profile 107d to the mobile network operator 104 in a step 304 in Figure 4. The second wireless network 102 in a step 304 in Figure 4 can be associated with a mobile network operator 104. The use of a first authentication 304 is also depicted and described in connection with Figure 3 above. As noted in a first authentication 304, the first key K 203 could comprise a key with a null value in an exemplary embodiment, although a random number could be used for a first key K 203 as well. As depicted in Figure 4, the steps 401 through 304 could comprise substeps within a step 403. The combined substeps comprising a step 403 can be used by a module 101 in exemplary embodiments including an embodiment illustrated in Figure 6 below.

Although not depicted in Figure 4, the mobile network operator 104 can conduct a separate step 308b to authenticate module 101 or a user 113 of module 101 using a second factor after a step 304. As described in a step 308b above, the second factor could comprise verifying or authenticating an identity of a user 113 associated with module 101. Note that the authentication of a user 113 can be conducted through the module 101 accessing a server 105 or a web page through the IP network 111 via the second wireless network 102 after the first authentication 304 using the first key K 203 (including embodiments where the first key K 203 comprises a null value).

In a step 309, the module 101 can receive a key from the second wireless network. The key in a step 309, as depicted in Figure 3 above, can comprise a symmetric key 127 in order to decrypt a ciphertext 208b within profile 107d. As also contemplated and described in connection with a step 309 in Figure 3, the key could comprise a module 101 receiving a ciphertext that includes a symmetric key 127 that has been ciphered with a key ciphering algorithm 216 using an asymmetric ciphering algorithm 219 and the eUICC public key 214, as illustrated in Figure

Petitioner Samsung Ex-1004, 0445

2e. For a key ciphering algorithm 216 used with a step 309, (i) the symmetric key 127 can comprise the plaintext (as opposed to the eUICC profile key 107b depicted in Figure 2e), and (ii) the MNO 104 could operate the key ciphering algorithm 216 instead of the eUICC subscription manager 109 depicted. In this embodiment of a step 309, a module 101 and/or an eUICC 107 could receive the key in the form of a ciphertext of symmetric key 127 in a step 309 and decrypt the ciphertext of symmetric key 127 with the eUICC private key 215 in order to read a plaintext symmetric key 127.

In a step 207 in Figure 4, the module 101 and/or eUICC 107 can decrypt the ciphertext 208b with the second key K 204a using the symmetric key 127. The module 101 can use a key K deciphering algorithm 207 as depicted and described in connection with Figure 2c above in order to read and record a plaintext second key K 204 from the ciphertext 208b in the profile 107d, where the profile 107d was previously decrypted and recorded using a step 206 above. As depicted in Figure 2a, the ciphertext 208b can also include a second network module identity 209a, so the eUICC 107 can also read the plaintext second network module identity 209 in a step 207, if a second network module identity 209a is included in a ciphertext 208b. In an exemplary embodiment, the second plaintext key K 204 is recorded in a protected, nonvolatile memory such as, but not limited to, a flash memory 101w. In this embodiment, the protected nonvolatile memory could comprise a memory address designated by the module 101, CPU 101b, operating system 101h, a module program 101i, or the eUICC 107 as a memory address that can only be written and read by the eUICC 107. Other possibilities exist as well to those of ordinary skill in the art for a plaintext second key K 204 to be recorded in a protected, nonvolatile memory in a step 207 without departing from the scope of the present invention.

In another embodiment, as described in a step 207 in Figure 3, the module 101 could record the encrypted second key K 204a in a nonvolatile memory, along with a symmetric key 127 (or an encrypted symmetric key 127 ciphered by a key ciphering algorithm 216). The module 101 or eUICC 107 could decrypt the encrypted symmetric key 127 in order to decrypt the ciphertext 208b that contains the second key K 204a each time the module 101 or eUICC 107

Petitioner Samsung Ex-1004, 0446

needs to read a plaintext second key K 204 for an conducting an authentication step 310, plus the subsequent derivation of additional keys such as CK and IK, Kasme, Kupenc, etc. using the plaintext second key K 204 and a RAND 118 value.

After reading a plaintext second key K 204 from a ciphertext 208b in a step 207 using the symmetric key 127, the module 101 and/or eUICC 107 can conduct a second authentication 310 step using the plaintext second key K 204, in order to authenticate with the second wireless network 102. The second wireless network 102 can comprise the same wireless network 102 the module 101 communicates with in a step 304 above. The use of a plaintext second key K 204 in a second authentication 310 step is depicted and described in connection with Figure 3. Although not illustrated in Figure 4, the module 101 could send a detach message or equivalent to temporarily disconnect from the second wireless network 102 after a step 309 and before a step 310 illustrated in Figure 4. A step 310 can comprise the module 101 sending a radio resource connection request to the second wireless network 102 with a network module identity associated with the second key K 204. A step 310 can be completed by a module 101 and/or an eUICC 107 sending a RES 119 value calculated using (i) a RAND 118 received and (ii) the second key K 204.

Although not illustrated in Figure 4, after a step 310 by a module 101 and/or an eUICC 107, the MNO 104 could verify the RES 119 and then the module 101 and the wireless network 102 associated with the MNO 104 could take subsequent steps for a module 101 to have access to the IP network 111 including the public Internet. The module 101 and/or eUICC 107 could derive session keys (such as, but not limited to a key CK) for encrypting data through the wireless network using a RAND 118 received in a step 310 and the second key K 204, and the module 101 and/or eUICC 107 could also derive an integrity key for a session (such as, but not limited to, an integrity key IK). Using an authenticated module 101 from a step 310, the MNO 104 can meter services rendered to a module 101 after a step 310 in order to bill or invoice a user 113 or M2M service provider 115.

Petitioner Samsung Ex-1004, 0447

Figure 5a

Figure 5a is a graphical illustration of a public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments. An eUICC 107 within a module 101 can include an eUICC private key 215, which can be associated with an eUICC public key 214. The eUICC private key 215 and eUICC public key 214 can comprise a public key infrastructure (PKI) key pair for eUICC 107. The MNO 104 can record the eUICC public key 214 along with an eUICC identity 107a, such that the MNO 104 can properly associate one of a plurality of eUICC public keys 214 with the proper eUICC 107. Although not illustrated in Figure 5a, a MNO 104 could record the eUICC public key 214 and an associated eUICC identity 107a in a database. The MNO 104 could receive the eUICC public key 214 and the eUICC identity 107a from an eUICC subscription manager 109 through an IP network 111 in a step 302a or step 302b of Figure 3. The use of, source, and additional details regarding an eUICC public key 214 and eUICC private key 215 are also depicted and described in connection with Figure 2d above.

The mobile network operator 104 could also be associated with an MNO private key 501 and an MNO public key 502, which could comprise a PKI key pair for the mobile network operator. The mobile network operator 104 could process or derive the PKI key pair using steps and algorithms equivalent to the steps and algorithms for an eUICC 107 to obtain the eUICC public key 214 and eUICC private key 215. The PKI keys depicted in Figure 5a could be processed using RSA algorithms or elliptic curve cryptography (ECC) algorithms, and other possibilities exist as well for the format of PKI keys without departing from the scope of the present invention. The public keys in Figure 5a can comprise keys recorded in an X.509 certificate, although the use of an X.509 certificates with public keys 214 and 502 are not required. The public key 214 and 502 in the form of an X.509 certificate can optionally be signed by a certificate authority. As illustrated in Figure 5a, the mobile network operator public key 502 can be recorded in the eUICC profile 107d. The MNO 104 could send the MNO public key 502 to the eUICC subscription manager 109 in a step 302a or 302b depicted and described in Figure 3, and the eUICC subscription manager 109 could include the MNO public key 502 in the

Petitioner Samsung Ex-1004, 0448

profile 107d. An eUICC profile 107d could also include the additional data for an eUICC profile 107d as depicted and described in Figure 2a, in addition to the MNO public key 502.

As illustrated in Figure 5a, the MNO 104 and eUICC 107 can both record a key derivation algorithm 503. Exemplary key derivation algorithm 503 could support a Diffie Hellman key exchange, an Elliptic Curve Diffie Hellman (ECDH) key exchange (ECDH), or similar algorithms for each node to mutually derive a key using public and private keys. For embodiments where (A) eUICC public key 214, eUICC private key 215, MNO public key 502, and MNO private key 501 utilize (i) elliptic curve cryptography (ECC) and (ii) a common, shared elliptic curve, then (B) a key derivation algorithm 503 in Figure 5a can comprise an algorithm for conducting an ECDH key exchange. The use of an ECDH key exchange was also described and contemplated between an eUICC subscription manager 109 and an eUICC 107 in step 303 in Figure 3 above. For embodiments where a key derivation algorithm 503 supports a Diffie Hellman key exchange, the key derivation algorithm 503 could record a multiplicative group of integers modulo p, where p is prime, and g is a primitive root mod p. In exemplary embodiments, p can be sufficiently large, such as, but not limited to, and exemplary prime number of at least 250 digits, and g can be a small number, such as, but not limited to, the number 5. In exemplary embodiments, additional values pertaining to the operation of a key derivation algorithm 503 can be transferred between two nodes using a token 505 described in a Figure 5b and Figure 5c below.

Figure 5b

Figure 5b is a graphical illustration of deriving a second key K using public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments. A mobile network operator 104 could process a MNO key exchange algorithm 504 in order to output or determine a second key K 204. A module 101 with an eUICC 107 could process an eUICC key exchange algorithm 505 in order to output or determine the same second key K 204. The MNO key exchange algorithm 504 and the eUICC key exchange algorithm 505 could include a key

Petitioner Samsung Ex-1004, 0449

derivation algorithm 503, and a key derivation algorithm 503 is also depicted and described in connection with Figure 5a above. The MNO 104 and module 101 could share or communicate a key exchange token 506 in order to operate the key exchange algorithm 505. In this manner, a module 101 with an eUICC 107 and a mobile network operator 104 could mutually derive or share the second key K 204 without MNO 104 transmitting or sending the second key K 204, even in an encrypted form such as a second key K 204a in a ciphertext 208b, to either (i) eUICC subscription manager 109 in a step 302a or step 302b, or (ii) to a module 101 in a profile 107c.

For a MNO key exchange algorithm 504, a mobile network operator 104 using a server 105 could input the mobile network operator private key 501, the eUICC public key 214, and a key exchange token 506 into a key derivation algorithm 503 in order to output the second key K 204. Note that the key derivation algorithm 503 in both a MNO key exchange algorithm 504 and an eUICC key exchange algorithm 505 can include additional or separate processing steps than those contemplated in a Diffie-Hellman key exchange and an ECDH key exchange. Additional steps than those contemplated in a Diffie-Hellman key exchange or ECDH key exchange for a key derivation algorithm 503 include transforming key output by these key exchange protocols into a key length and format compatible and suitable for a key K for use with wireless networks. In a key derivation algorithm 503, the output of a Diffie-Hellman key exchange and an ECDH key exchange could be input into a secure hash algorithm, such as SHA-256, which could then be truncated to select a 128 bit second key K 204 using a key derivation algorithm 503. For a MNO key exchange algorithm 504, the security key exchange token 506 can depend upon the algorithm used in a key derivation algorithm 503.

For embodiments where key derivation algorithm 503 comprises a Diffie-Hellman key exchange, the key exchange token 506 can comprise integer values of p and g. Or, with a Diffie-Hellman key exchange the security key exchange token 506 sent from a MNO 104 could comprise a value equal to g^a mod p where (x) the values or p and g have been previously shared between MNO 104 and eUICC 107, and (y) the value “a” can comprise the MNO private key 501. A security key exchange token 506 received by MNO 104 for input into a key derivation

Petitioner Samsung Ex-1004, 0450

algorithm for a eUICC 107 could comprise a value of g^b mod p, where b comprises the eUICC private key 215. For embodiments where key derivation algorithm 503 comprises an ECDH key exchange, the key exchange token 506 can a common base point G. The base point G could also be (i) recorded in an eUICC profile 107d, or (ii) sent from a mobile network operator 104 to module 101, or (iii) sent from the module 101 to the mobile network operator 104. Other algorithms besides an ECDH or Diffie Hellman key exchange can be utilized as well at a step 503, including a key exchange according to the American National Standards Institute (ANSI) standard X-9.63, and a key exchange token 506 could include a number or value associated with these other algorithms for a key derivation algorithm 503.

For an eUICC key exchange algorithm 505, a module 101 with an eUICC 107 could input the eUICC private key 215 and the mobile network operator public key 502 into a key derivation algorithm 503. Note that the input into the key derivation algorithm 503 could also optionally include a key exchange token 506. The key derivation algorithm 503 in an eUICC key exchange algorithm 505 could accept the input and output the second key K 204. The key derivation algorithm 503 in an eUICC key exchange algorithm 505 could be equivalent to the key derivation algorithm 503 in a MNO key exchange algorithm 504 described above. The key exchange token 506 in an eUICC key exchange algorithm 505 could comprise a value similar to the key exchange token 506 used in a MNO key exchange 504 described above. In a Diffie-Hellman key exchange for a key derivation algorithm 503 in a eUICC key exchange algorithm 505, the key exchange token 506 can comprise a value of either (i) integers p and g as described in a MNO key exchange 504, or (ii) number g^a mod p. In an ECDH key exchange for key derivation algorithm 503 in a eUICC key exchange algorithm 505, the key exchange token 506 can comprise a base point G. A key derivation algorithm 503 can output a second key K 204. Other possibilities exist as well for the use of PKI keys and tokens in key exchange algorithms for those of ordinary skill in the art without departing from the scope of the present invention.

Figure 5c

Figure 5c is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments. System 500 can include an eUICC subscription manager 109, an IP network 111, a mobile network operator 104, a mobile device 101. A module 101 can include a network application 101x and an eUICC 107. The operation of a system 500 can be similar to a system 300 in Figure 3, except for the steps noted in this Figure 5c where different steps can be taken than those within a Figure 3. As depicted for a system 500 in Figure 5c, like numerals for steps and messages for a system 500 in Figure 5c can comprise like steps and messages within a Figure 3. Different numerals discussed below can comprise different steps or messages for a system 500. Many of the same steps common for a system 500 in Figure 5c and a system 300 in Figure 3 will be summarized in this Figure 5c, while differences between the two systems (including the use of different numerals for different steps or messages) are described in more detail herein. As described in a step 302a and 302b in Figure 3, a mobile network operator 104 can send the eUICC subscription manager 109 information for a profile 107d in a step 302a or 302b, where the information can include the network parameters 201, the first network module identity 202, and the first key K 203. The listed exemplary data for a profile 107d from the previous sentence are also discussed for a profile 107d in Figure 2a.

For a step 507 in a system 500, the MNO 104 can omit sending an encrypted second key K 204a in a ciphertext 208b within the data for the profile 107d. In other words, the profile 107d can omit the second key K 204 in either a plaintext or ciphertext form after a step 507 in a system 500. The second key K 204 for a module 101 with eUICC 107 can be derived by a mobile network operator 104 in a MNO key exchange algorithm 504 and an eUICC key exchange algorithm 505 below in Figure 5c. Thus, in an embodiment illustrated in Figure 5c, the second key K 204 for a second authentication 310 does not need to be transferred to the eUICC subscription manager 109 from MNO 104 for the eUICC subscription manager 109 to include in a profile 107d. Similarly, in a system 500, the second key K 204 does not need to be transferred

Petitioner Samsung Ex-1004, 0452

to the eUICC 107 in a profile 107c. In embodiments where (x) the MNO sends network access credentials such as the first and second network module identities 202 and 209a and a first key K 203 are sent in a step 302b, then (y) a step 507 to omit the sending of the second key K 204 could take place with a step 302b instead of the step 302a as depicted. The MNO 104 can send the first and second network module identities 202 and 209a and a first key K 203 in a step 302a or a step 302b to the eUICC subscription manager 109. The MNO 104 can send to the eUICC subscription manager 109 the first and second network module identities 203 and 209a and a first key K 203 in a profile 107d in a step 302a or 302b, and the eUICC subscription manager 109 could receive the first and second network module identities 202 and 209a and a first key K 203 in a step 302a or a step 302b. Other possibilities for combinations of data sent from a MNO 104 to an eUICC subscription manager 109 in a step 302a, 302b, and 507 without departing from the scope of the present invention.

As depicted in Figure 5c, an eUICC 107 in module 101 could perform steps 301, then step 205 to receive a profile 107c, then receive an eUICC profile key 107b, and then convert the profile 107c into a profile 107d using the eUICC profile key 107b in a step 206. The eUICC profile key 107b could also be (i) ciphered with a key ciphering algorithm 216, sent from the eUICC subscription manager 109 as an encrypted eUICC profile key 218, (ii) and then deciphered by a module 101 and/or eUICC 107 with a step 217, as described in connection with Figure 2e above. The module 101 and/or an eUICC 107 could (i) receive an encrypted eUICC profile key 107b in the form of an key 218 and (ii) use a key deciphering algorithm 217 to decrypt the encrypted eUICC profile key 107b in order (iii) to read a plaintext eUICC profile key 107b and then (iv) use the plaintext eUICC profile key 107b to decrypt the ciphertext 208a.

As depicted in Figure 5c, after a module 101 sends a eUICC identity 107a and receives an eUICC profile 107c in a step 205, the module 101 can conduct a step 206 in order to decrypt a ciphertext 208a that can include a first key K 203 using an eUICC profile key 107b. For the embodiments contemplated in Figure 5c, where the second key K 204 can be derived or determined using a key exchange in steps 504 and 505 below, the second network module

Petitioner Samsung Ex-1004, 0453

identity 209a can be included in the ciphertext 208a (as opposed to being included in the ciphertext 208b as depicted in Figure 2a). One reason can be that a ciphertext 208b can be omitted from an eUICC profile 107d in embodiments where the second key K 204 can be mutually derived by the eUICC 107 and the MNO 104, so there may be no need to include a separate ciphertext 208b within the eUICC profile 107d.

After reading a first network module identity 202 and the first key K 203, the module 101 can conduct a first authentication 304. Note that the first key K 203 can comprise key with a null value, as contemplated in wireless network 102 standards which support the use of emergency services where a module 101 may not include a valid first key K 203. In this case where the first key K 203 comprises a null value, the use of a ciphertext 208a can also be optionally omitted, such that the receipt of an eUICC profile key 107b and the use of a ciphertext 208a could also be optionally omitted and a profile 107c could include plaintext for the first key K 203 and network module identity 202. As depicted and described in connection with Figure 3, a module 101 and MNO 104 could conduct a first authentication step 304 in order to authenticate the module 101 using the first key K 203. The first key K could comprise a non-null value in exemplary embodiments. A step 306 to calculate a first RES 119 value using the first key K 203 from a profile 107d could be included in a first authentication step 304.

The mobile network operator 104 could compare the first received RES 119 with a recorded RES 119 in order to authenticate the module 101 with the eUICC 107 in a step 308a. A mobile network operator 104 can authenticate the module 101 using a step 308a in order to provide access to the IP network 111, and the access to the IP network 111 can be limited (such as, but not limited to excluding access to the public Internet after a step 308a). The module 101 could use access to the limited or restricted IP network 111 in order for a user 113 of module 101 to conduct an authentication with the mobile network operator 104 using a second factor, as described in a step 308b in Figure 3.

After authenticating the module 101 with the first network module identity 202 and the first key K 203 in a step 308a, the mobile network operator 104 could authenticate a user 113 or

Petitioner Samsung Ex-1004, 0454

verify a M2M service provider 115 is associated with the module 101 in a step 308b. The authentication of a user 113 or M2M service provider 115 in a step 308b could comprise authenticating module 101 and/or eUICC 107 with a second factor, where the second factor comprises or includes a secure association of a user 113 or M2M service provider 115 with the module 101. As described in Figure 3 above, a step 308b could result in the secure association of an identity for the user 113 or the M2M service provider 115 with an identity of the module 101. After conduction a step 308b as depicted and described in connection with Figure 3 above, the MNO 104 can record the second network module identity 209 in the eUICC profile 107d is associated with a particular user 113 or a particular M2M service provider 115.

In a step 308b, the MNO 104 can also determine (i) the first network module identity 202 used in step 304 is associated with other identities such as module identity 110, profile identity 107e, eUICC identity 107a, and the second network module identity 209. By (i) authenticating a user 113 or (ii) verifying an identity for module 101 is associated with a M2M service provider 115 in a step 308b, MNO 104 can determine the second network module identity 209 (used in a subsequent authentication step 310) belongs to or is associated with a particular user 113 or M2M service provider 115. In other words, without a separate authentication step 308b in Figure 5 and Figure 3, MNO 104 may not be able to securely determine that the second network module identity 209 from a profile 107d belongs to a particular user 113 or M2M service provider 115. For embodiments where the module 101 is associated with a M2M service provider 115, then a step 308b in Figure 5c could comprise the MNO 104 verifying that an identity received in a first authentication 304 (such as, but not limited to, the first network module identity 202) is associated with an M2M service provider 115, such as checking the identity in a list of identities for modules 101 belonging to M2M service provider 115.

After successfully authenticating or verifying an identity of a user 113 or an M2M service provider 115 is associated with module 101 in a step 308b, MNO 104 could process an MNO key exchange algorithm 504 in order to record a second key K 204 for use in a subsequent second authentication 310 for module 101. The second authentication 310 can use different

Petitioner Samsung Ex-1004, 0455

network access credentials (i) associated with the module 101 and (ii) obtained by module 101 using an eUICC key exchange algorithm 505. Although not illustrated in Figure 5c, a MNO 104 could obtain the data for processing a MNO key exchange algorithm 504 in several different ways. A MNO 104 could receive the eUICC public key 214 for an MNO key exchange algorithm 504 from either (i) the module 101 or eUICC 107 directly after the first authentication 304 or (i) the eUICC subscription manager 109 in a step 302b above, where the eUICC subscription manager 109 could record the eUICC public key 214. Other possibilities exist as well for a MNO 104 to receive an eUICC public key 214 associated with an identity for module 101 such as the eUICC identity 107a. The recording of an eUICC public key 214 with an MNO 104 is also depicted and described in connection with Figure 5a above.

For a MNO key exchange algorithm 504 in Figure 5c, the MNO 104 could also input a key exchange token 506 and a MNO private key 501, in addition to the eUICC public key 214, as illustrated in Figure 5b above. After performing a MNO key exchange algorithm 504 in Figure 5c, the MNO 104 can record the second key K 204 for the second module identity 209 (which is associated with the first module identity 202 in the profile 107d). As contemplated for a key exchange token 506 in Figure 5a and Figure 5c, the key exchange token 506 could be any of the cases (A) initially processed, derived, or determined by the MNO 104, (B) shared between the MNO 104 and module 101 with the eUICC 107, such as, but not limited to, recording the key exchange token 506 in the profile 107d, or (C) initially processed, derived, or determined by module 101. Figure 5c illustrates an embodiment for case (A) with key exchange token 506, where the MNO 104 derives or determines the key exchange token 506 value and subsequent sends the key exchange token 506 value to the module 101 with the eUICC 107. The MNO 104 can send the key exchange token 506 in a message 508, and a network application 101x for the module 101 can receive the key exchange token 506 in the message 508 and forward the key exchange token 506 to the eUICC 107. For case (A) the MNO 104 can omit sending the key exchange token 506 until after the user 113 or M2M service provider 115 for module 101 has been successfully authenticated or verified in a step 308b.

Petitioner Samsung Ex-1004, 0456

In a related embodiment to the embodiment depicted in Figure 5c, for case (B) with key exchange token 506, a separate message 508, to communicate or transfer the key exchange token 506 between the MNO 104 and module 101 after a step 504, can optionally be omitted, since both sides (MNO 104 and module 101) could record the key exchange token 506 before a step 505 by a module 101 with an eUICC 107 below. For case (B), the MNO 104 could send a signal in a message 508 to the module 101 that the authentication step 308b of a user 113 or an M2M service provider 115 has been successfully completed, and thus module 101 could proceed with an eUICC key exchange algorithm 505 using the recorded key exchange token 506.

For case (C) with key exchange token 506, the eUICC 107 could derive or determine the key exchange token 506 and subsequently send the key exchange token 506 to the MNO in a message 508. In this case (C), the MNO 104 could receive the key exchange token 506 (i) before processing the MNO key exchange algorithm 504, and (ii) using the connection with the module 101 from the first authentication 304. For case (C), the MNO 104 can require the successful completion of an authentication step 308b for a user 113 or M2M service provider 115 before accepting the key exchange token 506 from the module 101.

In another exemplary embodiment, step 504 and step 505 can use different values for the key exchange token 506, and both MNO 104 and module 101 can send the tokens 506 in a message 508 to the other node. In exemplary embodiments, a message 508 comprising the key exchange token 506 can be transferred through the IP network 111, where access to the IP network 111 can be enabled by the first authentication 304 with the first key K 203. Other possibilities exist as well for the transfer of a key exchange token 506 between a MNO 104 and a module 101 with an eUICC 107 for conducting a key exchange without departing from the scope of the present invention.

As depicted in Figure 5c, a module 101 with an eUICC 107 can conduct an eUICC key exchange algorithm 505 in order to determine or read a second key K 204. As depicted and described for an eUICC key exchange algorithm 505 in Figure 5b above, the module 101 can input an MNO public key 502, an eUICC private key 215, and the key exchange token 506 into a

Petitioner Samsung Ex-1004, 0457

key derivation algorithm 503 in order to output the second key K 204. Note that the number, value, or sequence of bits for the second key K 204 determined by a MNO 104 in a step 504 can be equal to the number, value, or sequence of bits for the second key K 204 determined by a module 101 with an eUICC 107 in a step 505. The mutual derivation of the second key K 204 by a MNO 104 in a step 504 and a module 101 in a step 505 can be different and superior to conventional technology for either (i) a physical UICC or (ii) an eUICC, since the second key K 204 does not need to be transferred in either physical or electronic form, where the electronic form could include encrypting the second key K 204 into a ciphertext. Supporting the derivation of a second key K 204 as depicted and described herein can be superior to the electronic or physical distribution of a key K, since a different second key K 204 can be utilized by repeating steps 504 and 505 a second time, such as with a different key exchange token 506. In this manner, the second key K 204 associated with the second network module identity 209 could be rotated or changed periodically, thereby increasing the security of a system 500 compared to the use of a static, non-changing second key K 204 for the lifetime of a module 101 with a profile 107d.

After a step 505 in Figure 5c, the subsequent steps and messages for communication between the module 101 and the MNO 104 can be the same or equivalent to those in Figure 3 after a step 207. In other words, the second key K 204 as used by a module 101 and/or eUICC 107 for embodiments in a Figure 5c can be equivalent or similar to the processing and recording steps depicted and described in Figure 3, upon module 101 with an eUICC 107 reading the second key K 204 in a step 207 in Figure 3. In a system 500, the module 101 or eUICC 107 could record the second key K 204 in a protected, nonvolatile memory as described in a step 207 of Figure 3. Other possibilities exist as well without departing from the scope of the present invention for the location or techniques of storing the second key K 204 resulting from a step 505.

As depicted and described in connection with Figure 6 below, the module 101 could record the second key K 204 in a volatile memory (and not storing the second key K 204 in

Petitioner Samsung Ex-1004, 0458

nonvolatile memory), including potentially only within a register or cache memory of CPU 101b. In this manner, the security of the derived second key K 204 can be enhanced, since upon or after power off of a module 101, a third party could not probe or read nonvolatile memory looking for the second key K 204. Since a volatile memory could be flushed upon loss of power or other circumstances, a MNO 104 and module 101 could repeat the steps 504 and 505, respectively, including the transfer of a key exchange token 506, a subsequent time when a module 101 needs to process or derive a new, subsequent second key K 504. In other words, a module 101 can conduct a step 505 with a different key exchange token 506 at a later time after the first instance of a step 505 in order to derive a different, subsequent second key K 204.

After deriving the second key K 204 in a step 505 in Figure 5c, the module 101 with the eUICC 107 can authenticate with the MNO 104 using the wireless network 102, the second network module identity 209, the second key K 204. The module 101 could conduct a second authentication 310 with the mobile network operator using the second key K 204, as depicted in Figure 5c, which is also equivalent to the second authentication 310 depicted in Figure 3 above. Note that the module 101 could detach or disconnect from the wireless network 102 (i) after a sending/receiving a message 508 with key exchange token 506 and (ii) before sending the exemplary second attach message 303 with the second network module identity 209.

The eUICC 107 within module 101 could use (i) the second key K 204 from a step 505, and (ii) a second RAND 118 value from the MNO 104 to calculate a second RES 119 value in a step 311. The eUICC 107 can send the second RES 119 to the network application 101x, and the module 101 can send the second RES 119 to the mobile network operator 104 through the wireless network 102. The MNO 104 could compete the second authentication in a step 312 by verifying the second RES 119 is correct using (i) the second key K 204 derived by the MNO 104 in a step 504 above, and (ii) the second RAND 118 value sent to the module 101. Upon successful authentication using the second key K 204, as depicted and described in connection with Figure 3, the module 101 and MNO 104 could take subsequent steps after a step 312 for the module 101 to have access to the IP network 111 and also the public Internet.

In another embodiment contemplated in Figure 5c, the mobile network operator 104 can send the second key K 204 to the module 101 using the wireless network 102 in a message 508. In other words, the exemplary token 506 in Figure 5c could comprise the second key K 204, as opposed to an exemplary key exchange token 506. In this embodiment, the use of a key derivation algorithm 503 in a step 504 could use input of a random number from random number generator 128 into the key derivation algorithm 503 (instead of PKI keys), and the output could be the second key K 204. Or, the key derivation algorithm 503 in a step 504 could simply assign a random number to the second key K 204. After a step 308b and step 504, the mobile network operator 104 could send the second key K 204 in a message 508. The second key K 204 in a message 508 could be encrypted using a key ciphering algorithm 216. The message 508 with the second key K 204 as the token 506 could be received by the module 101 and decrypted using a key deciphering algorithm 217. In another embodiment, the token 506 received by a module 101 could comprise (i) the second key K 204 as plaintext at the application layer, but (ii) ciphered at the data-link layer using the first RAND value from a step 304 and the first key K 203. Other possibilities exist as well for a token 506 to comprise a second key K 204 without departing from the scope of the present invention.

The order of many of the steps and messages depicted within a system 500 could be changed without departing from the scope of the present invention. For example, a step 504 could also be conducted concurrently with a step 302b (instead of with a step 308b), such that a mobile network operator 104 could calculate a second key K 204 using a MNO key exchange algorithm 504 at the same time when MNO 104 sends the first network module identity 202 and first key K 203 to the eUICC subscription manager 109. After receiving (i) an eUICC identity 107a from an eUICC subscription manager 109 and (ii) and an eUICC public key 214 in a step 302b, the mobile network operator 104 can process a MNO key exchange algorithm 504 in order to calculate or process a second key K 204.

In an exemplary embodiment, a mobile network operator 104 could receive a list of eUICC public keys 214 and eUICC identities 107a from an M2M service provider 115 before

Petitioner Samsung Ex-1004, 0460

eUICC subscription manager 109 receives the eUICC identity 107a in a step 205. The MNO 104 could use the data received from a M2M service provider 115 (including a list of eUICC identities 107a and eUICC public keys 214) in order to derive the second key K 204 using a MNO key derivation algorithm 504 and the key exchange token 506. The MNO 104 could send the key exchange token 506 to an eUICC subscription manger 109 before the eUICC subscription manager 109 participates in a step 205 as illustrated in Figure 5c, and the eUICC subscription manager 109 could include the key exchange token 506 with the eUICC profile 107c, such that module 101 could receive the key exchange token 506 in the eUICC profile 107c.

In this embodiment (which can also comprise a case (B) for the transfer of key exchange token 506 for a message 508 as described above), a module 101 using an eUICC 107 with profile 107d and key exchange token 506 could potentially derive the second key K 204 before a step 308b, but in preferred embodiments the mobile network operator 104 does not allow the use of the second key K 204 until after an authentication step 308b of a user 113 or M2M service provider 115. In another embodiment, the values for the first network module identity 202 and the second network module identity 209 could be the same or equal, such that the module 101 uses the same network module identity for both first authentication 304 and a second authentication 310. In this case, the MNO 104 can support a change in key K used with the first network module identity 202 from the first key K 203 to the second key K 204. The first key K 203 can be included in a profile 107d, but the second key K 204 can be derived by an MNO 104 using a step 504 and a module 101 using a step 505. Other possibilities exist as well for a MNO 104 and a module 101 to mutually derive a second key K 204 for use with an eUICC 107 without departing from the scope of the present invention.

Figure 6

Figure 6 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments. An exemplary system 500 depicted and described in connection with Figure 5c can also support the

Petitioner Samsung Ex-1004, 0461

repeated derivation of a second key K 204 for a MNO 104 and module 101 with an eUICC 107. The use and support for different second keys K 204 over time can increase security, since the second key K 204 can be securely and periodically rotated, thereby enhancing the security and efficiency of a system 500, compared to either (i) physically changing a UICC each time a new key K is desired, or (ii) querying, downloading, and selecting a new profile 107c or profile 107d each time the use of a different key K is desired (including steps to communicate and record a second key K 204 in the profile 107d). In other words, the use of multiple second keys K 204 over time can be accomplished for the same profile 107d.

A step 403 in Figure 6 can comprise a module 101 with an eUICC 107 conducting the substeps for a step 403 as depicted and described in connection with Figure 4. In a step 403, a module 101 could connect with a first wireless network 102, receive an eUICC profile 107c, decrypt the profile 107c using an eUICC profile key 107b, activate the profile 107d, and authenticate with a second wireless network 102 using a first key K 203 from the profile 107d. As noted above, other possibilities exist as well for a module 101 to record an eUICC profile 107d, such as the loading of a profile 107d by a manufacturer, without departing from the scope of the present invention.

After successful authentication of the module 101 at the conclusion of a substep 304 in a step 403, a user 113 associated with the module 101 could conduct an authentication step 308b with the mobile network operator 104. A step 308b can be useful for a mobile network operator 104 to authenticate or securely associate (i) a module 101 with (ii) a legal entity contractually responsible for the services used by a module 101. The use of a step 308b is also described in Figure 3. Note that module 101 could be associated with an M2M service provider 115 instead of a mobile phone subscriber such as an individual, and in this case the M2M service provider 115 could take steps before a step 308b in order to inform or confirm with MNO 104 that module 101 with an identity such as module identity 110 or the first network module identity 202 belongs to or is associated with the M2M service provider 115.

Petitioner Samsung Ex-1004, 0462

In other words, a MNO 104 may not have control over the distribution or recipient of a profile 107c from an eUICC subscription manager 109 in a step 403, and a user authentication in a step 308b allows a MNO 104 to confirm, verify, or establish a contractual relationship with a user 113. Business contracts and procedures for an MNO 104 to provide service to a module 101 with an eUICC 107 with profile 107d could require that a user 113 successfully completes an authentication step 308b (with example steps described in Figure 3 above), before the MNO 104 provides service such as voice calls or access to the public Internet. The second factor in a step 308b can be data communicated between the MNO 104 and the user 113 to confirm an identity of the user 113. Examples of data for the second factor in a step 308b are described in connection with a step 308b in Figure 3. The first factor contemplated in a system 300 or system 500 can be the successful receipt of a RES 119 value in a first authentication 304. Upon conclusion of the step 308b the MNO 104 could securely determine and record that a module 101 with the first network module identity 202 and/or the second network module identity 209 from the profile 107d is associated with an authenticated user 113.

The module 101 could then perform a step 508 in order access a key exchange token 506. As described for a key exchange token 506 in Figure 5c, the module 101 could receive the token 506 in a step 508 (case A), or the module 101 could send the token 506 in a step 508 (case B). Step 508 can comprise sending or receiving the message 508 from Figure 5c. The key exchange token 506 could comprise a key exchange token 506 as depicted and described in connection with Figure 5b. Or, as described for a message 508 in Figure 5c, the key exchange token 506 could comprise the second key K 204, such as the second key K 204 encrypted by MNO 104 with a key ciphering algorithm 216 and decrypted by the module 101 with the eUICC 107 using a key deciphering algorithm 217. The key exchange token 506 at a step 508 could comprise parameters for a key derivation algorithm 503, such as a base point G if elliptic curve cryptography PKI keys are used with MNO public key 502, MNO private key 501, eUICC public key 214, and eUICC private key 215.

Petitioner Samsung Ex-1004, 0463

In another exemplary embodiment, key exchange token 506 with a Diffie Hellman key exchange for a key derivation algorithm 503 could comprise a multiplicative group of integers modulo p, where p is prime and g is primitive root mod p. Other possibilities for a key exchange token 506 in a message 508 exist as well without departing from the scope of the present invention, including the use of multiple values and numbers for a key exchange token 506. The key exchange token 506 transfer between MNO 104 and module 101 in a step 508 can use the second wireless network after the module 101 authenticates with the first key K 203, and thus the data-link layer for transfer of the key exchange token 506 could be ciphered using the first key K 203 (where a cipher key for the data-link layer is derived from the first key K 203 and a RAND 118 from a first authentication 304).

A module 101 with an eUICC 107 could then perform a step 505, which could comprise an eUICC key exchange algorithm 505 as depicted in Figure 5c using (i) the token 506 from a message 508 above, and (ii) the eUICC private key 215 and MNO public key 502. The output from an eUICC key exchange algorithm 505 can comprise the second key K 204. In an exemplary embodiment, the second key K 204 output from the eUICC key exchange algorithm 505 is recorded within a memory of module 101 on a temporary basis. After obtaining and reading the second key K 204 from a step 505, the module 101 can conduct a second authentication 310 with the MNO 104 using the second key K 204. The second key K 204 can be associated with a second network module identity 209, which could be recorded in the profile 107c and profile 107d for the eUICC 107 from a step 403 above. Exemplary details and steps for a second authentication 310 using the second key K 204 are depicted and described in connection with Figure 3 and Figure 5c above.

After the conclusion of the second authentication 310, the module 101 could have access to the public Internet through the IP network 111 of the wireless network 102. After a step 310 and before a subsequent step 601 below, the module 101 could continue using the second key K 204 with the second network identity 209 in many additional repeated steps 310, such that module 101 could use the second key K 204 for an exemplary period of time such as several

Petitioner Samsung Ex-1004, 0464

days or several months, and other possibilities exist as well for the continued use of a second key K 204 after a step 310 and before a step 601 in Figure 6. For example, a module 101 could repeat a step 311 in a second authentication 310 multiple times with the same wireless network 102 using the same number of value for the second key K 204 during a period of time before a step 601.

At a step 601 in Figure 6, a module 101 or a MNO 104 could determine if the use of a new second key K 204 is required or preferred. There could be several reasons that a different second key K 204 may be periodically preferred. Exemplary reasons include (i) the second key K 204 may only be temporarily stored within a volatile memory in CPU 101b, such that a power cycle of module 101 or CPU 101b could flush the volatile memory, and in this case module 101 and MNO 104 may need to derive a new second key K 204, (ii) ownership of module 101 may change, and business or legal contracts could stipulate that a previous second key K 204 with the prior owner of module 101 may no longer be valid and thus a new second key K 204 may be required, (iii) a MNO 104 and a module 101 or M2M service provider 102 may prefer to periodically rotate the second key K 204 in order to increase security of a system 500. For example, a module 101 may have a planned lifetime of more than a decade, and given the speed of change for mobile networking technology, a module 101 may prefer to support the change in a second key K 204 for accessing a wireless network 102 without downloading and installing a new, different profile 107d. Other possibilities exists as well for exemplary reasons why a module 101 and/or a MNO 104 could determine that the use of a new, second key K 204 is preferred or required in a step 601 without departing from the scope of the present invention. If a module 101 or MNO 104 determine a value of “no” for a step 601, then the module 101 could continue periodically performing repeated second authentication 310 steps using the same second key K 204, as illustrated in Figure 6.

As depicted in Figure 6, upon determination of a value of “yes” for a step 601, a module 101 could return to a step 508 and receive another key exchange token 506. As depicted in Figure 6, the module 101 could use a first authentication 304, which could comprise an

Petitioner Samsung Ex-1004, 0465

authentication with the first key K 203. A return to the first authentication 304 with the first key K 203 could be omitted in some embodiments, and thus the box for 304 depicted in Figure 6 is a dashed line.

In this embodiment where module 101 or MNO 104 determine or evaluates that a new second key K 204 is preferred at a step 601, the module 101 could return to a step 508 by attaching with the wireless network 102 again using the first network module identity 202 and the first key K 203. For example, if the second key K 204 is not available (such as being flushed from being stored only in a volatile memory, a potential error condition such as a reset of module 101, or the second key K 204 is no longer preferred to be used), then the module 101 with the eUICC 107 could use data recorded in the profile 107d to reconnect with the wireless network 102. For example, the first key K 203 and the first network identity 202 may be recorded in generally accessible nonvolatile memory, such as, but not limited to, a flash memory 101w within module 101 and subsequently the first key K 203 and the first network identity 202 could be used in a step 304 before a return to a step 508. Or, the module 101 and MNO 104 could continue to use the previous second key K 204 (if available) for a communications link to transfer the key exchange token 506, and thus the use of a step 304 with the first key K 203 is optional.

Upon return to a step 508 module 101 and MNO 104 could transfer a key exchange token 506 as described in a step 508 in Figure 6 above. Upon return to a step 508, the module 101 and MNO 104 could transfer a key exchange token 506 that has a different value or number from a key exchange token 506 transferred earlier (in order to support the derivation of a different second key K 204 than from a previous iteration). Using the new, different value for the key exchange token 506, the module 101 with the eUICC 107 could derive a new, different second key K 203. In this manner and by using the steps illustrated in Figure 6, a second key K 204 could operate as a key K for “temporary use”, and a different second key K 204 for use in a subsequent authentication 310 could be obtained by a repeated use of a step 505 with a new,

Petitioner Samsung Ex-1004, 0466

different key exchange token 506 for module 101 connecting with the same wireless network 102.

The module 101 and MNO 104 could continue to use the same network module identity (such as a second network module identity 209) upon a return to steps 508 through 310, or the MNO 104 could also send the module 101 a new, different network module identity in a message 508 upon a return to steps 508 through 310. A MNO 104 and a module 101 can repeat the use the steps 508 through 601 depicted and described in this Figure 6 in order to derive a series over time of second keys K 204 for the module 101 with the eUICC 107. Each member of the series (comprising a different second key K 204) could be associated with the second network module identity 209, and the second network module identity 209 could remain constant or can also change to different numbers or values for use in a step 310. Supporting a change in the second key K 204 can both increase the flexibility and security of a system 500 and related systems for a user and a mobile network operator 104.

Conclusion

Various exemplary embodiments have been described above. Those skilled in the art will understand, however, that changes and modifications may be made to those examples without departing from the scope of the claims.

Petitioner Samsung Ex-1004, 0467

CLAIMS

What is claimed is:

1. A method comprising:

(a) generating a first message comprising:

(1) an identity of an embedded universal integrated circuit card;

(2) a nonce; and

(3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;

(b) sending the first message via a network application to a subscription manager system;

(c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;

(d) storing a subscription manager public key which corresponds to a subscription manager private key;

(e) deriving a profile key using a key exchange algorithm based on at least:

(i) the second eUICC private key, and

(ii) the stored subscription manager public key, wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key;

(f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;

(g) receiving the symmetric key;

(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;

(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and

(j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.

2. The method of claim 1, wherein the subscription manager public key is downloaded via the network application.

Petitioner Samsung Ex-1004, 0468

3. The method of claim 1, wherein the step of storing the subscription manager public key occurs at the time of manufacture of the embedded universal integrated circuit card.

4. The method of claim 1, wherein the key exchange algorithm is a Diffie-Hellman key exchange.

5. The method of claim 1, wherein the key exchange algorithm is an Elliptic Curve Diffie-Hellman key exchange.

6. The method of claim 1, wherein the encrypted profile is encrypted in a manner so that intermediate nodes on an IP network would not be able to read data within the profile in an unencrypted form.

7. The method of claim 1, wherein subscription manager system stores the ciphertext and the symmetric key before step (a).

8. The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the identity of the embedded universal integrated circuit card included in the first message.

9. The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the digital signature included in the first message.

10. The method of claim 1, wherein the decrypted ciphertext is stored in nonvolatile memory of the embedded universal integrated circuit card.

11. The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a machine-to-machine module.

Petitioner Samsung Ex-1004, 0469

12. The method of claim 11, wherein the module comprises a module of a type selected from the group consisting of: vending machine, automobile, alarm system, tracking device, monitoring device, security system and remote control device.

13. The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a wireless module.

14. The method of claim 13, wherein the module is configured to communicate using one or more wireless technologies of types selected from the group consisting of: WiFi, WiMax, General Packet Radio Services, Enhanced Data rates for GSM Evolution and 3rd Generation Partnership Project technology.

15. The method of claim 13, wherein the module comprises a module of a type selected from the group consisting of the following: wireless handset, cellular phone, smartphone, laptop computer, tracking device, computer with a radio, circuit board with a radio, hand-held device, netbook, portable computer, multiprocessor system, microprocessor based consumer electronic, programmable consumer electronic, network personal computer, minicomputer, mainframe computer and smartcard.

16. The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module, wherein the module is a wired module.

17. The method of claim 16, wherein the module is configured to communicate using one or more wired connections of types selected from the group consisting of: Ethernet, fiber optic connection and Universal Serial Bus connection.

18. The method of claim 16, wherein the module comprises a module of a type selected from the group consisting of: computer, security camera, security monitoring device and networked controller.

Petitioner Samsung Ex-1004, 0470

19. The method of claim 1, wherein the deriving step (c) is performed prior to the generating step (a).

20. The method of claim 1, wherein the generating step (a) is performed before the deriving step (c).

21. The method of claim 1, wherein the embedded integrated circuit card is operably connected to a module and a user accesses a user interface of the module to enter authentication information before the module receives the symmetric key.

22. The method of claim 1, wherein the subscription manager receives the ciphertext from a mobile network operator before the network application sends the first message.

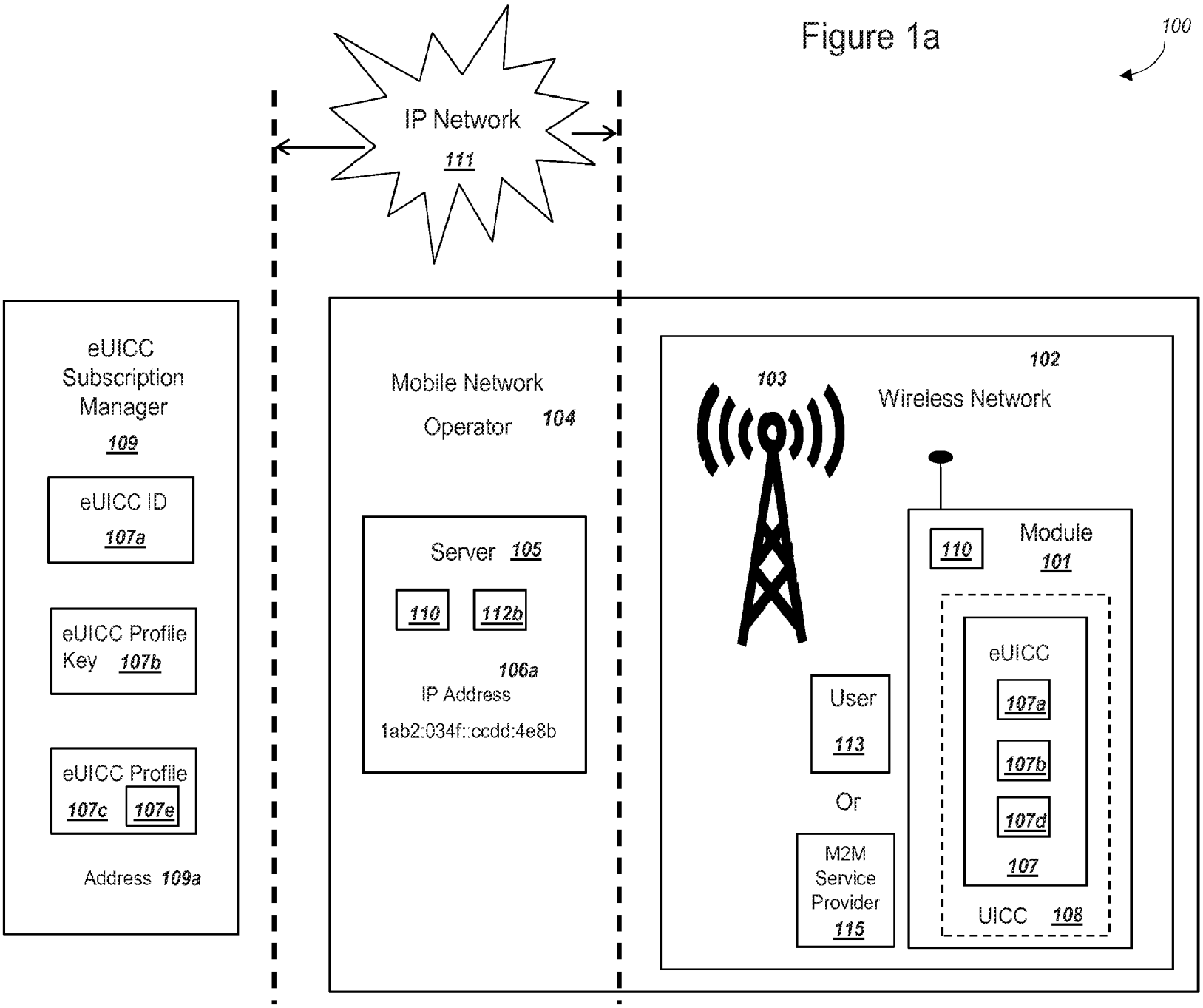
Petitioner Samsung Ex-1004, 0471

ABSTRACT

A module with an embedded universal integrated circuit card (eUICC) can include a profile for the eUICC. The profile can include a first and second shared secret key K for authenticating with a wireless network. The first shared secret key K can be encrypted with a first key, and the second shared secret key K can be encrypted with a second key. The module can (i) receive the first key, (ii) decrypt the first shared secret key K with the first key, and (iii) subsequently authenticate with the wireless network using the plaintext first shared secret key K. The wireless network can authenticate the user of the module using a second factor. The module can then (i) receive the second key, (ii) decrypt the second shared secret key K, and (iii) authenticate with the wireless network using the second shared secret key K. The module can comprise a mobile phone.

Petitioner Samsung Ex-1004, 0472

Figure 1a



Petitioner Samsung Ex-1004, 0473

Figure 1b

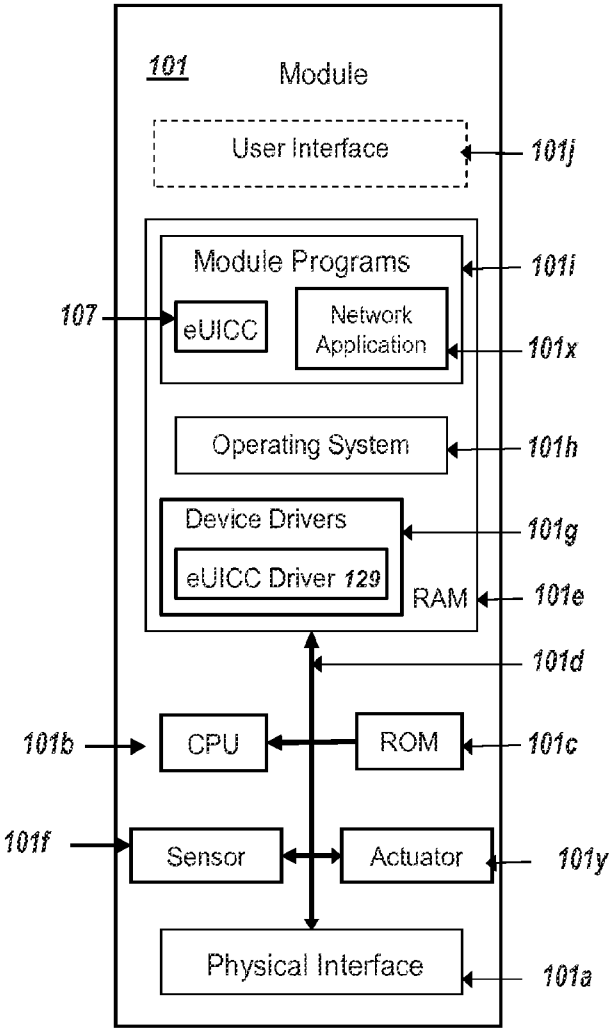
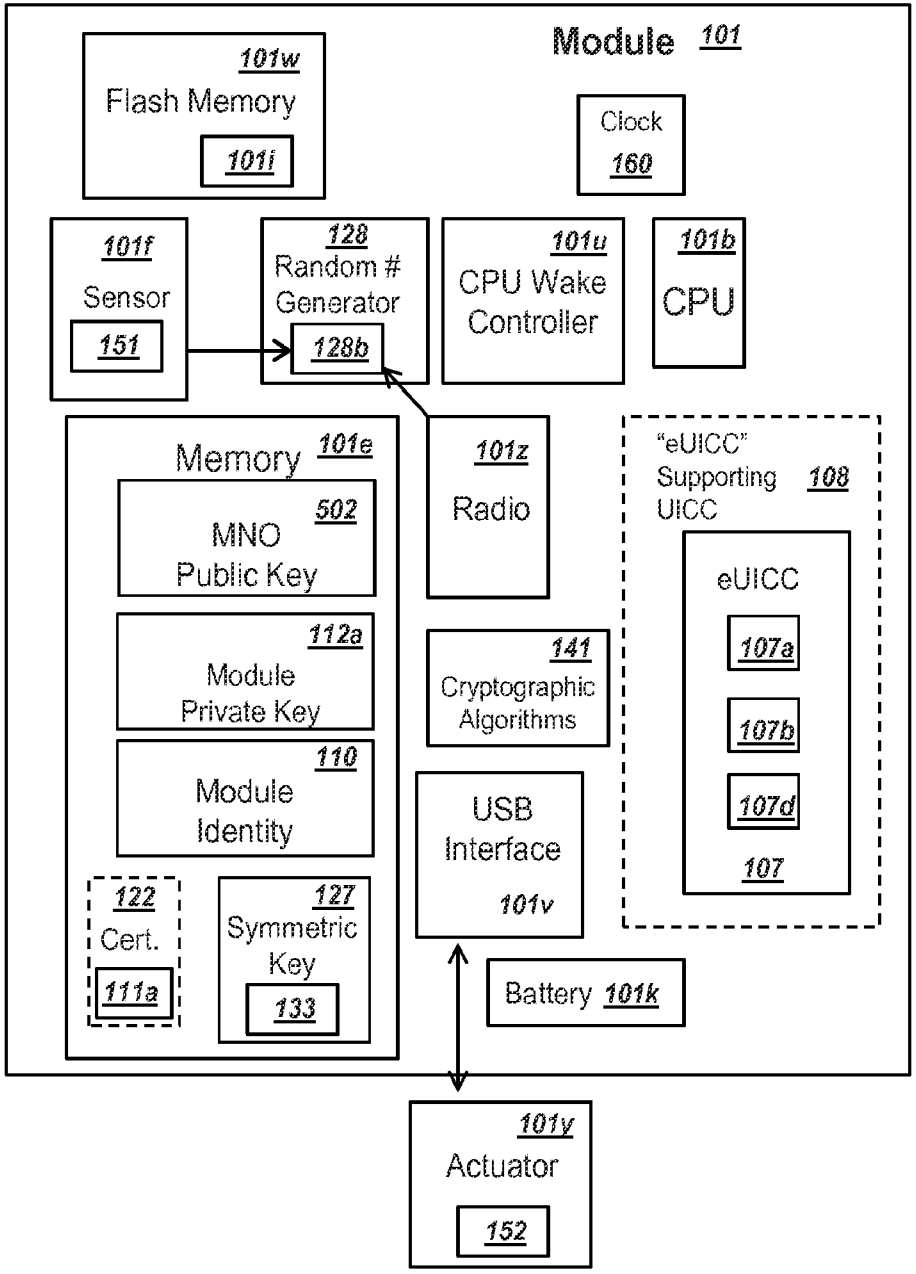


Figure 1c



Petitioner Samsung Ex-1004, 0474

Figure 1d

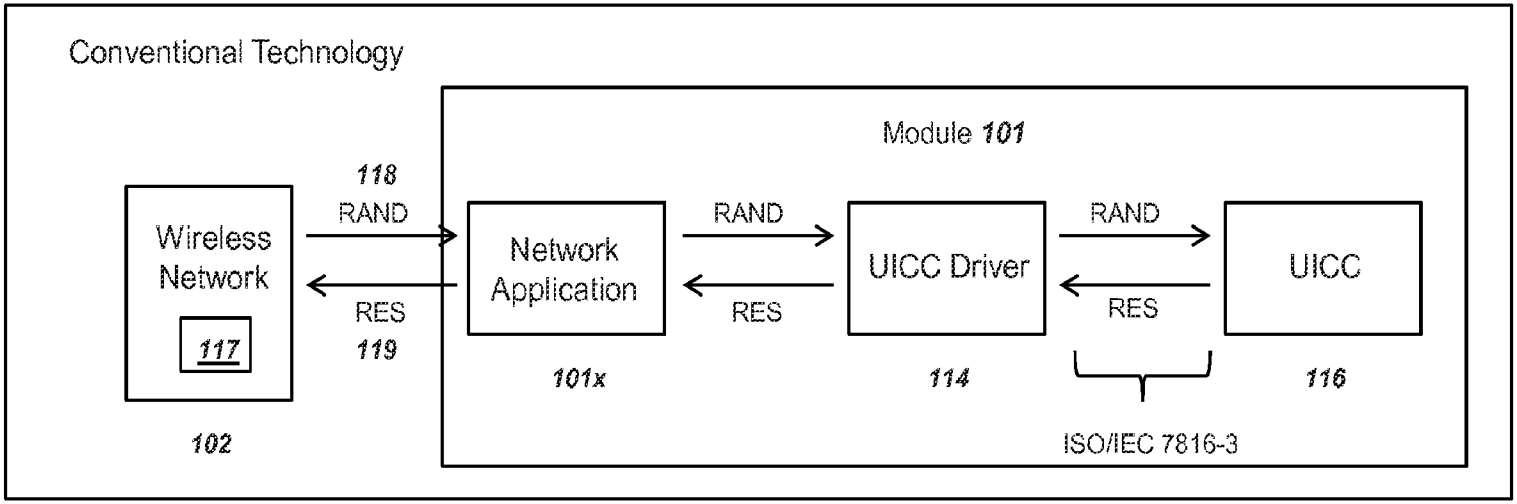
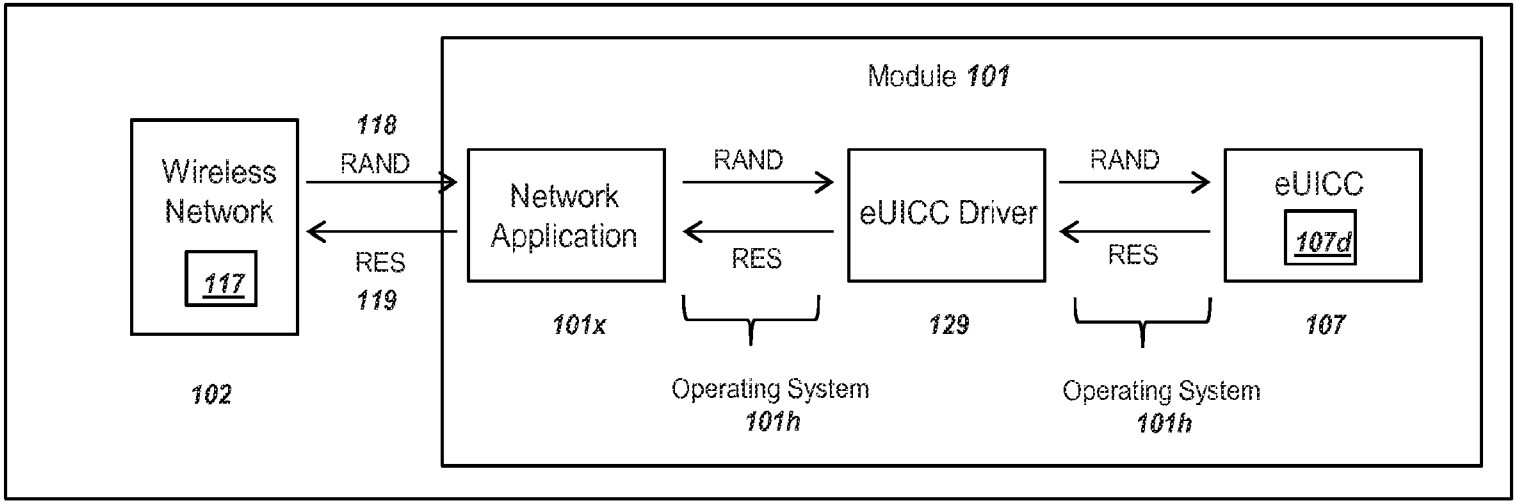
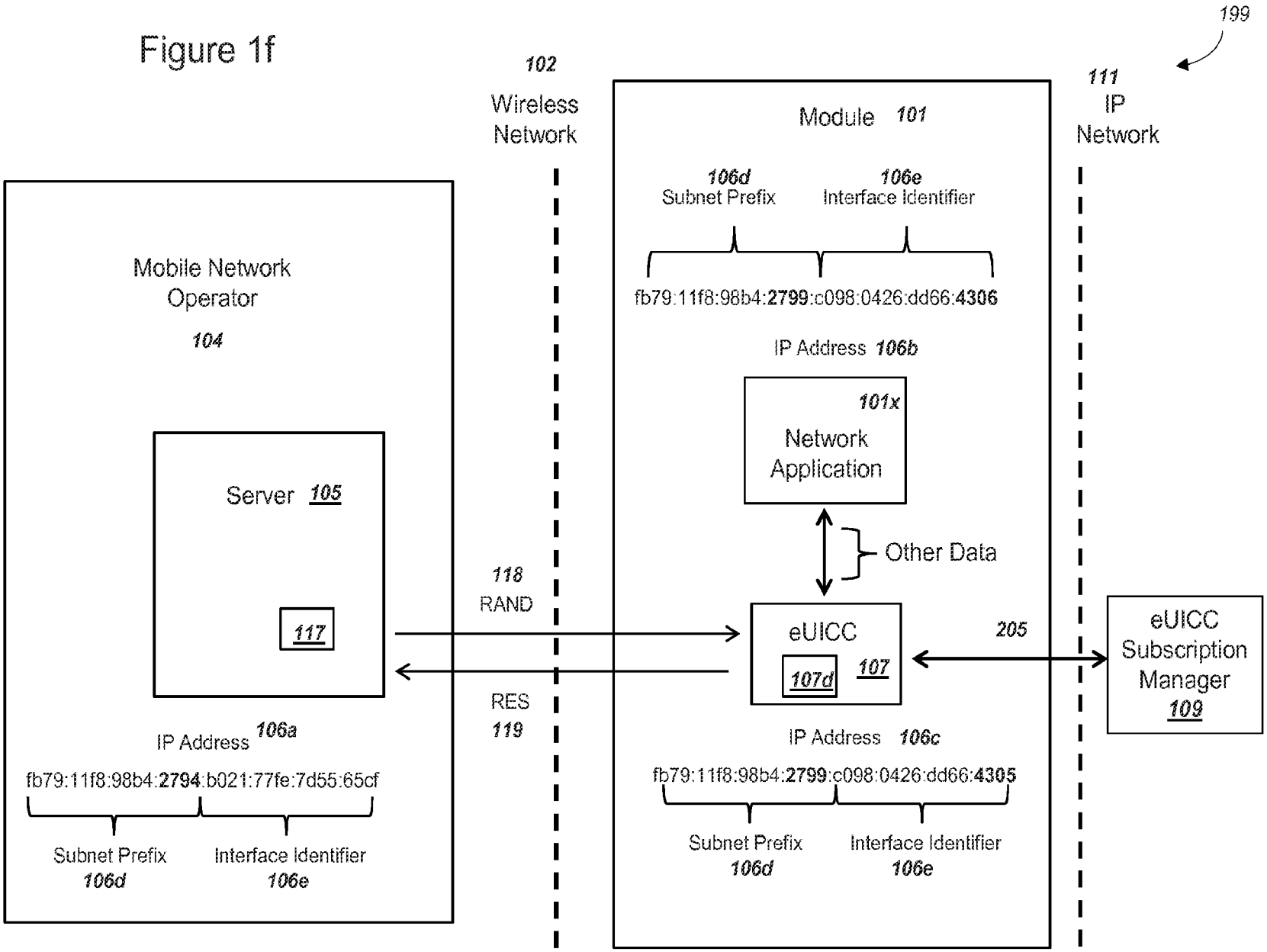


Figure 1e



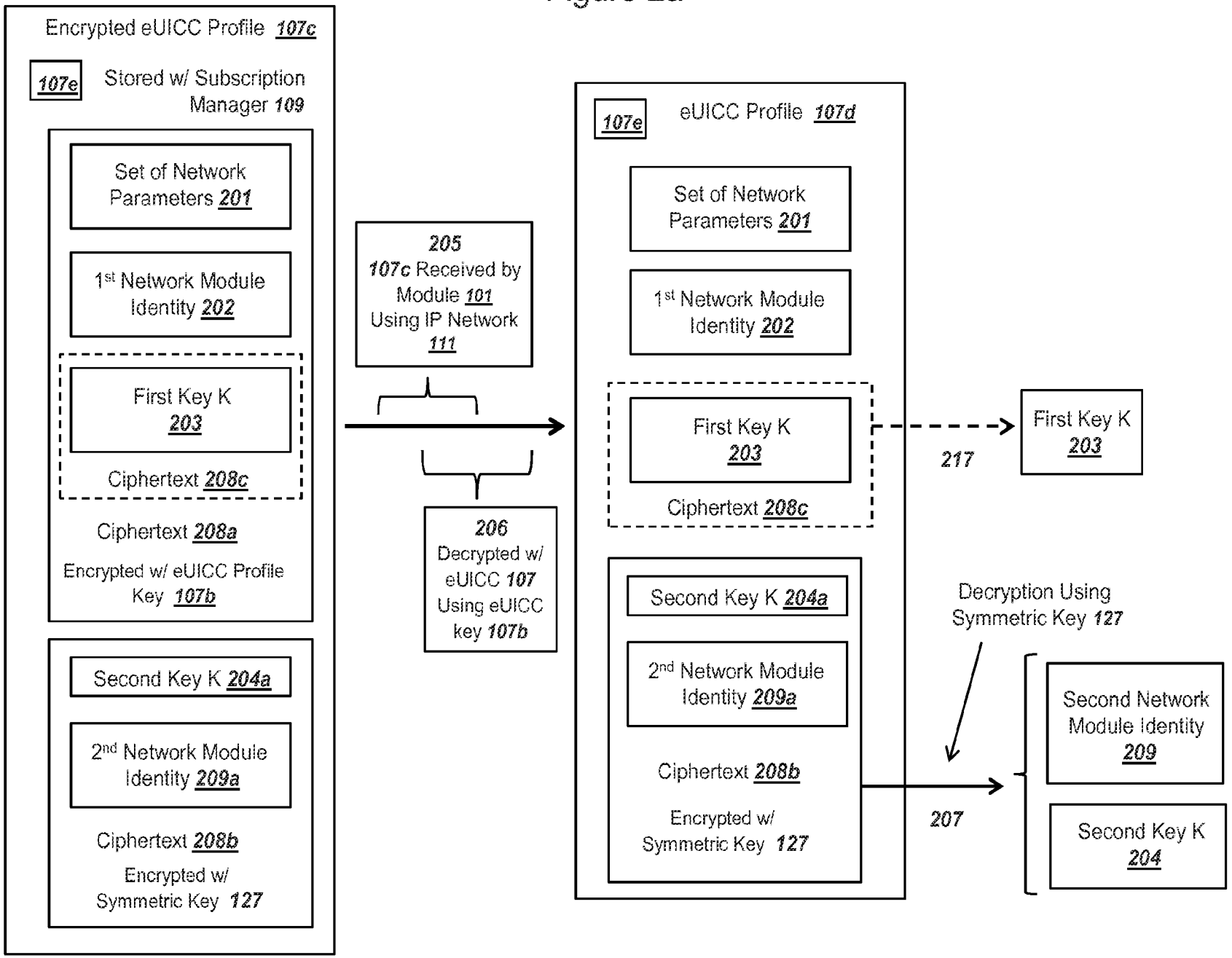
Petitioner Samsung Ex-1004, 0475

Figure 1f



Petitioner Samsung Ex-1004, 0476

Figure 2a



Petitioner Samsung Ex-1004, 0477

Figure 2b

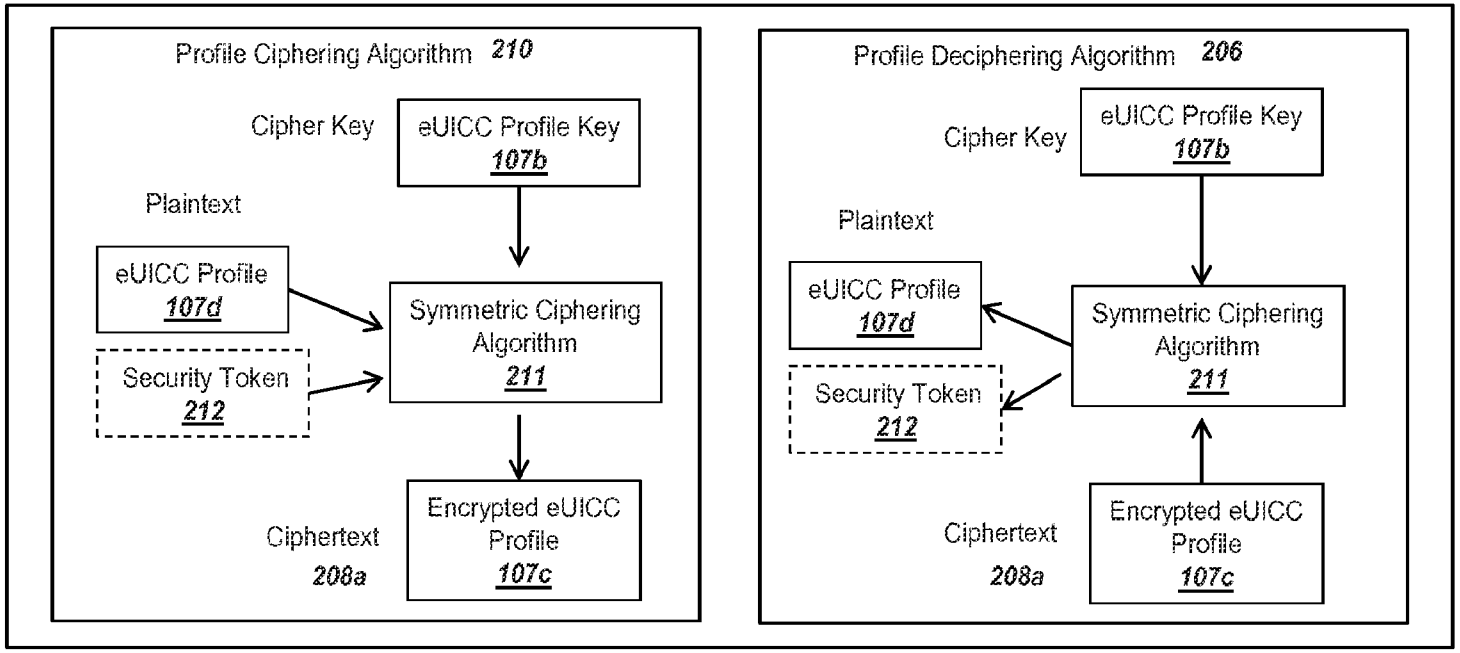
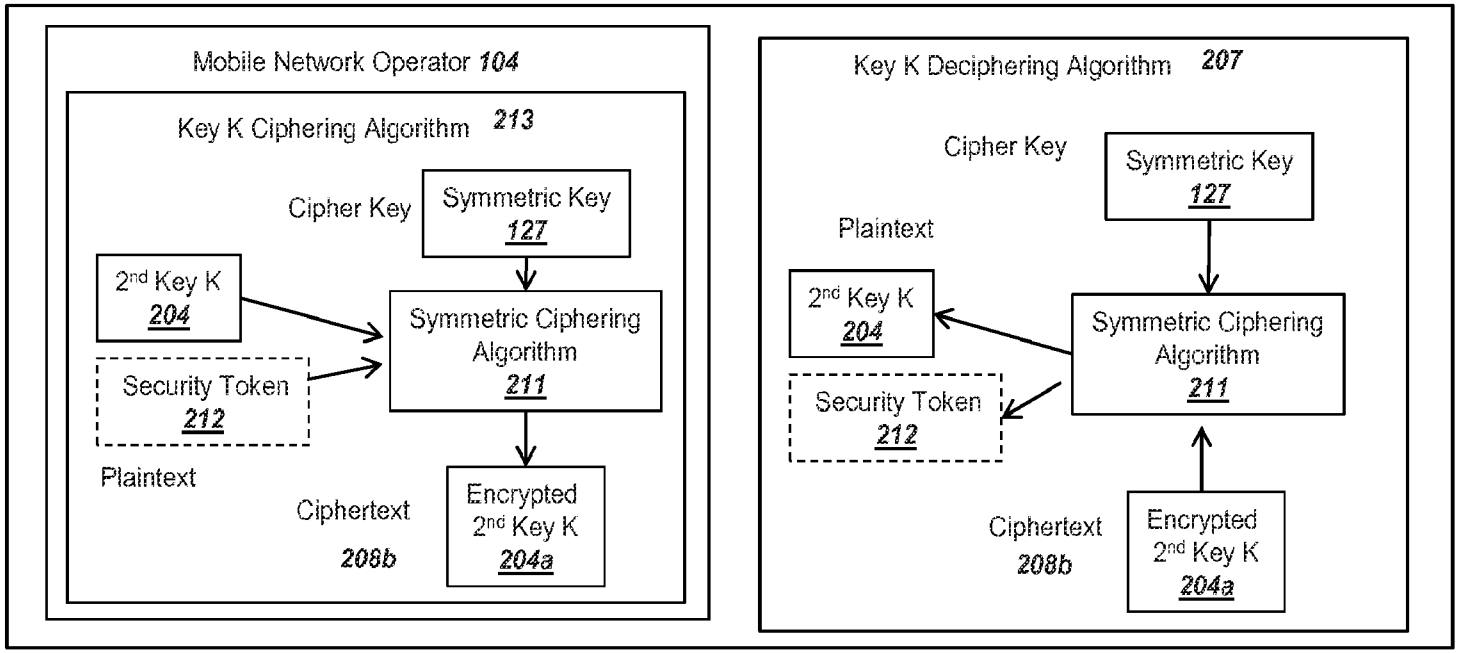


Figure 2c



Petitioner Samsung Ex-1004, 0478

Figure 2d

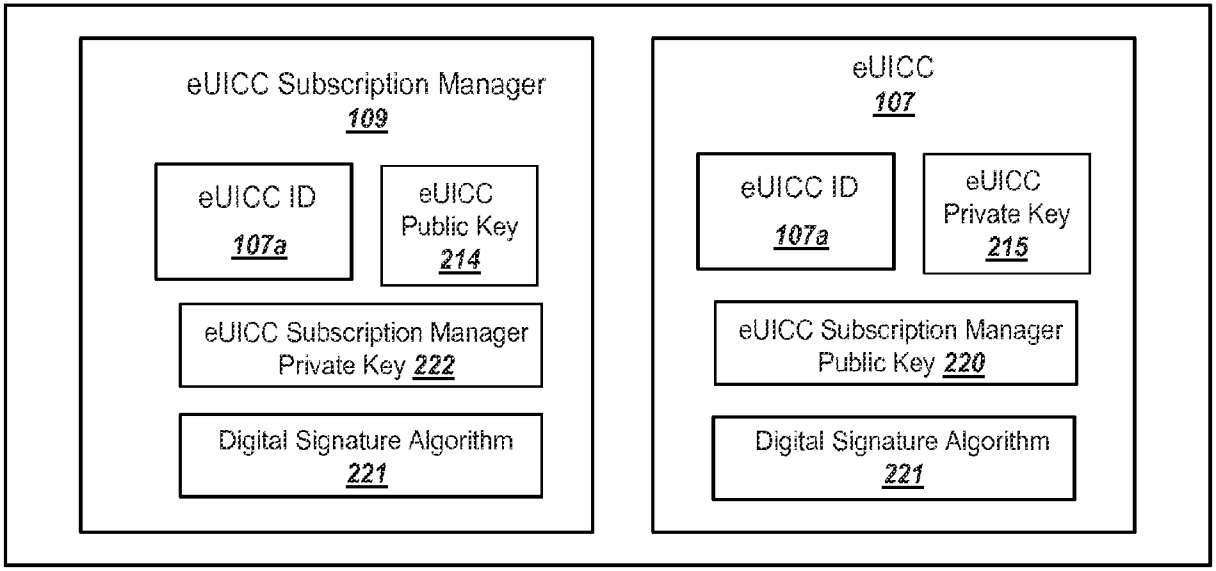
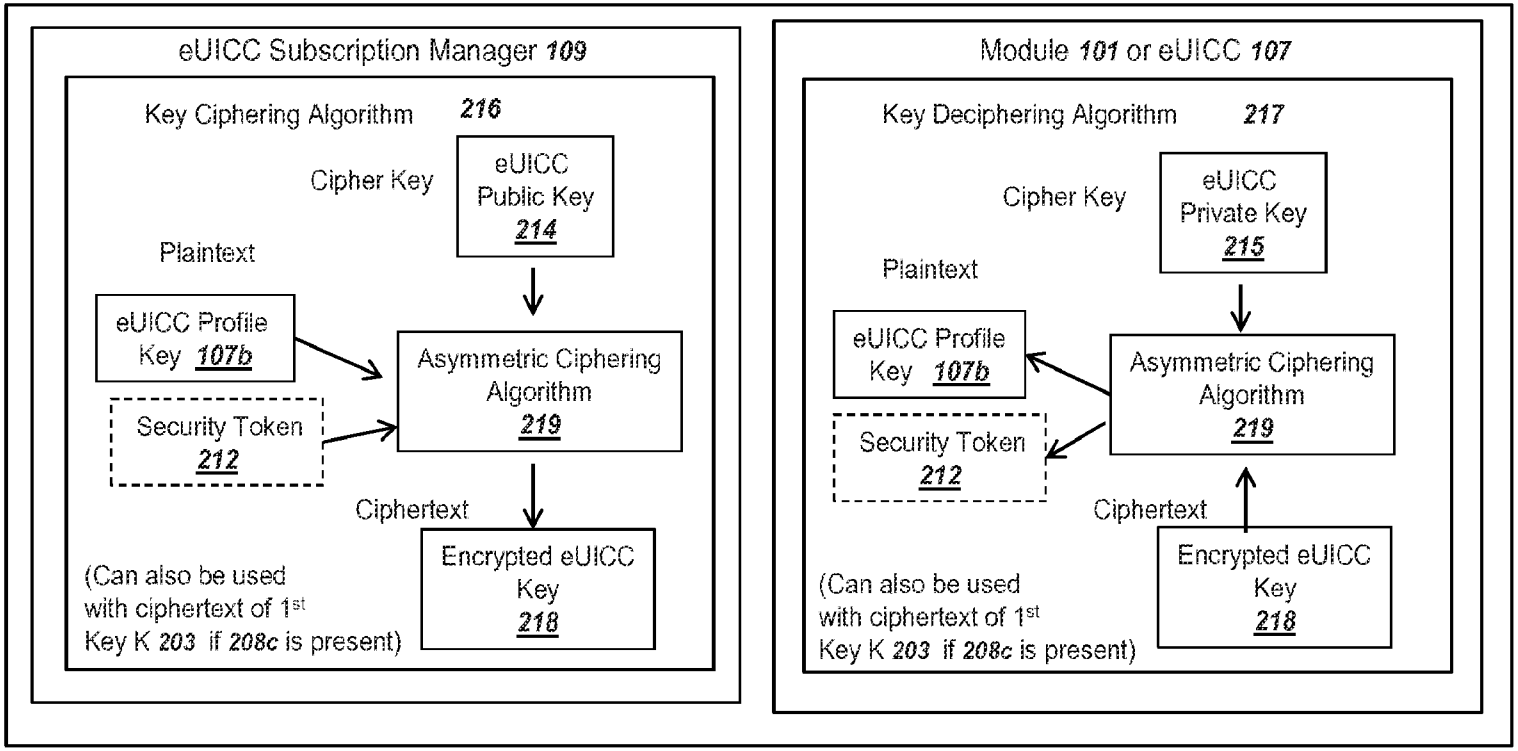
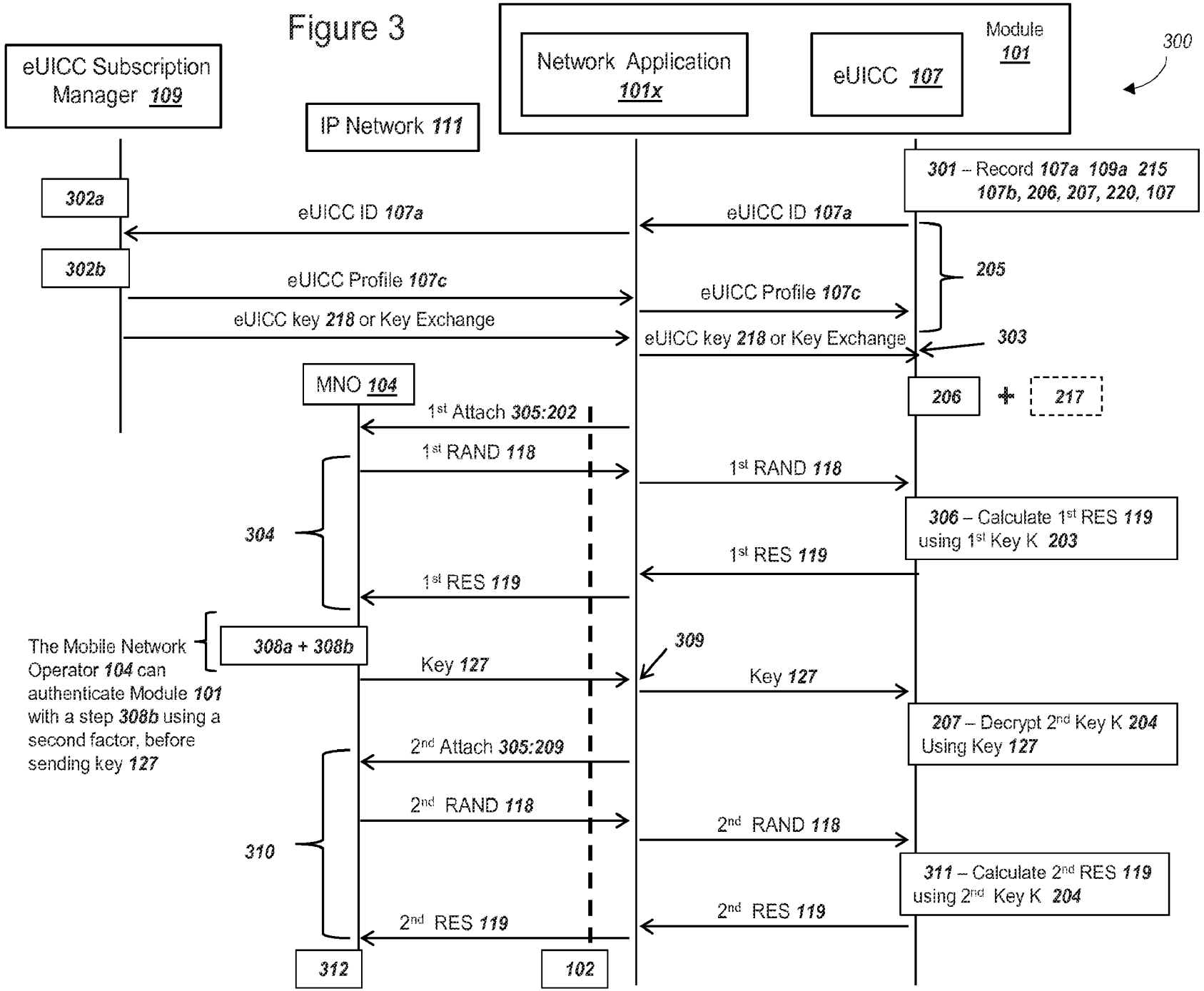


Figure 2e



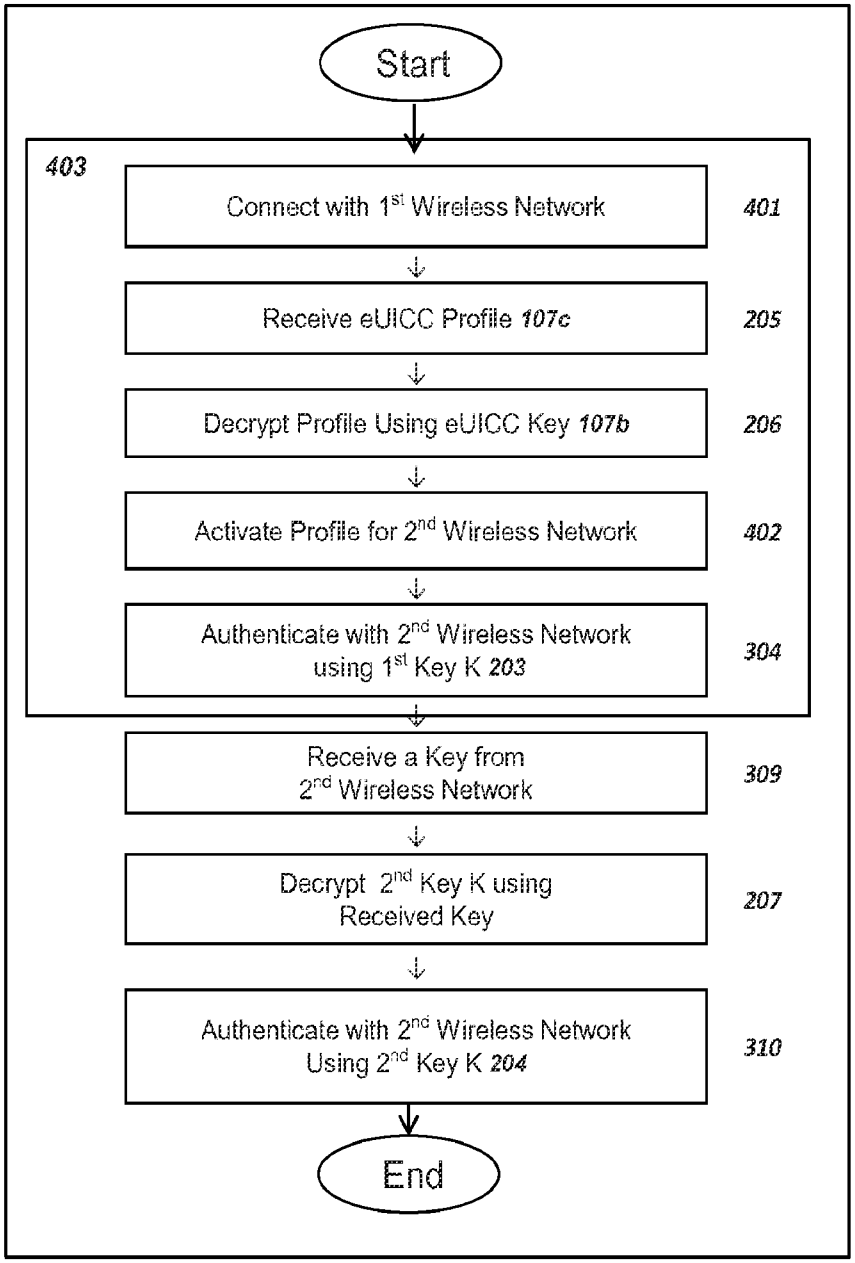
Petitioner Samsung Ex-1004, 0479

Figure 3



Petitioner Samsung Ex-1004, 0480

Figure 4



Petitioner Samsung Ex-1004, 0481

Figure 5a

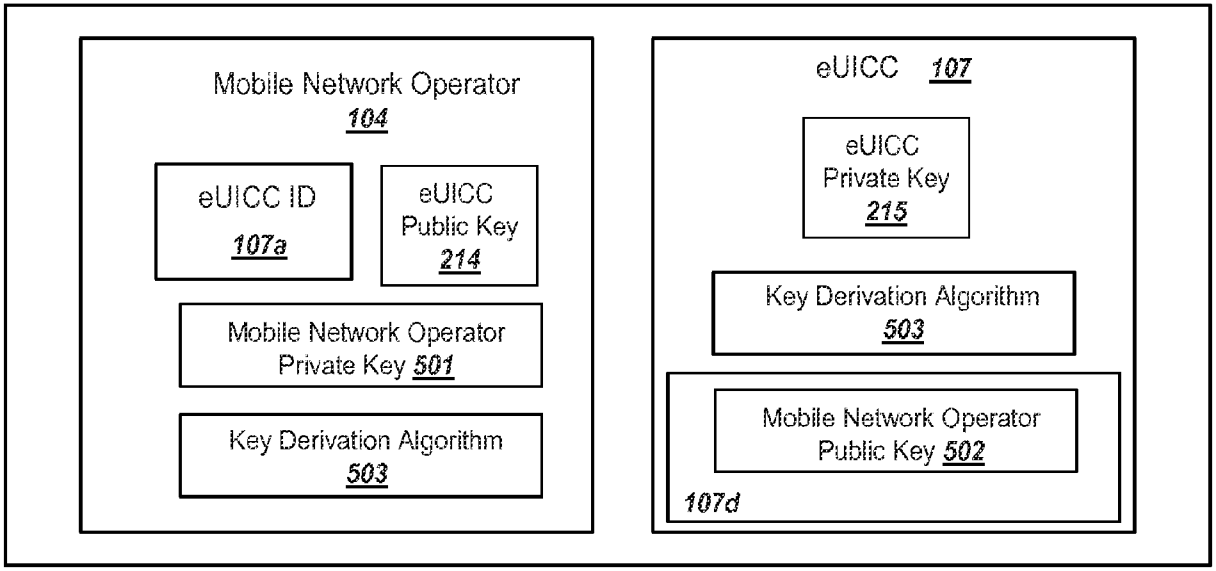
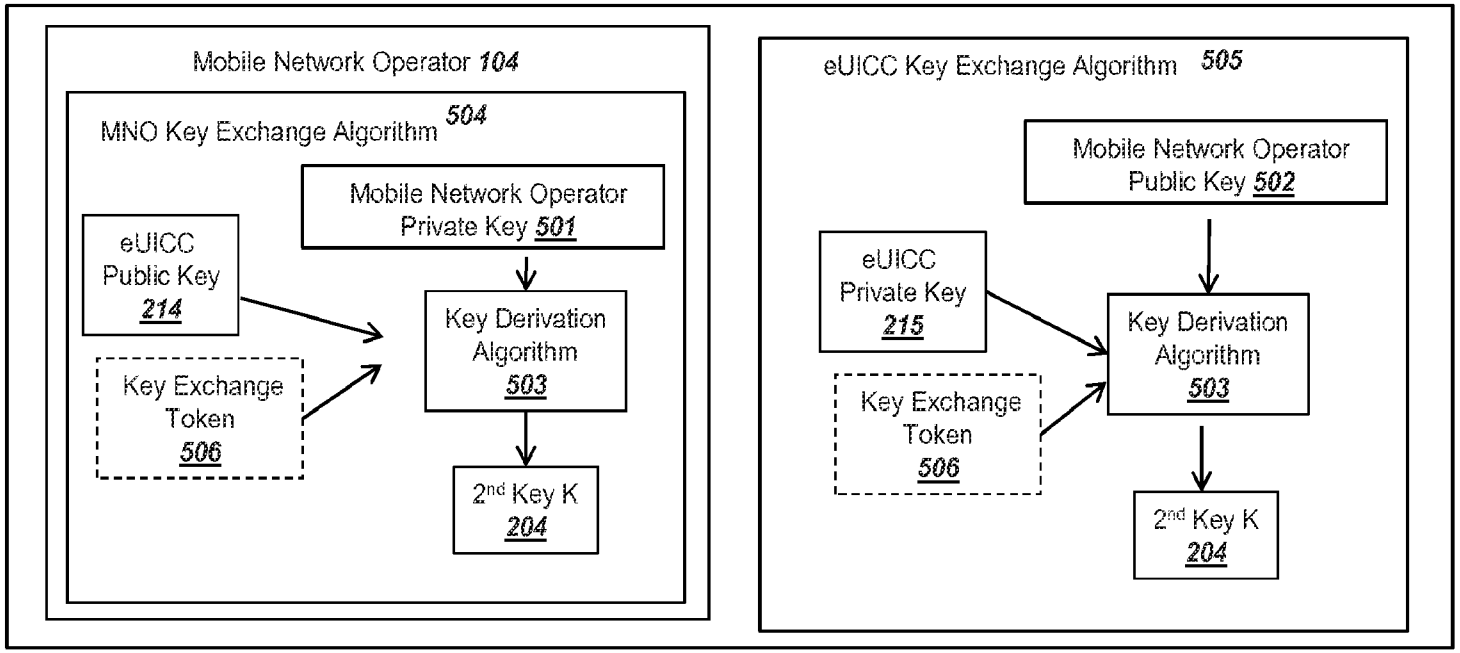
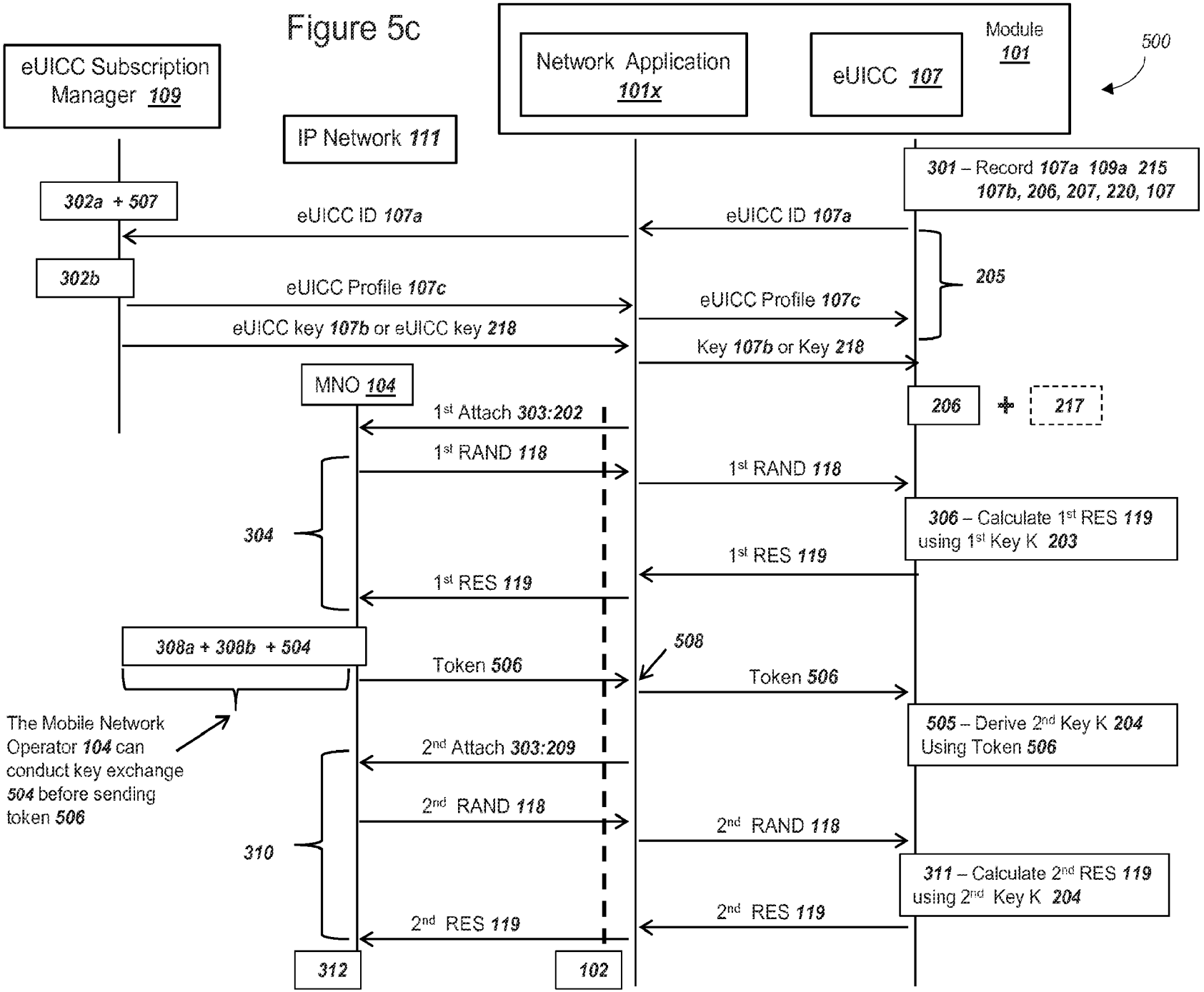


Figure 5b



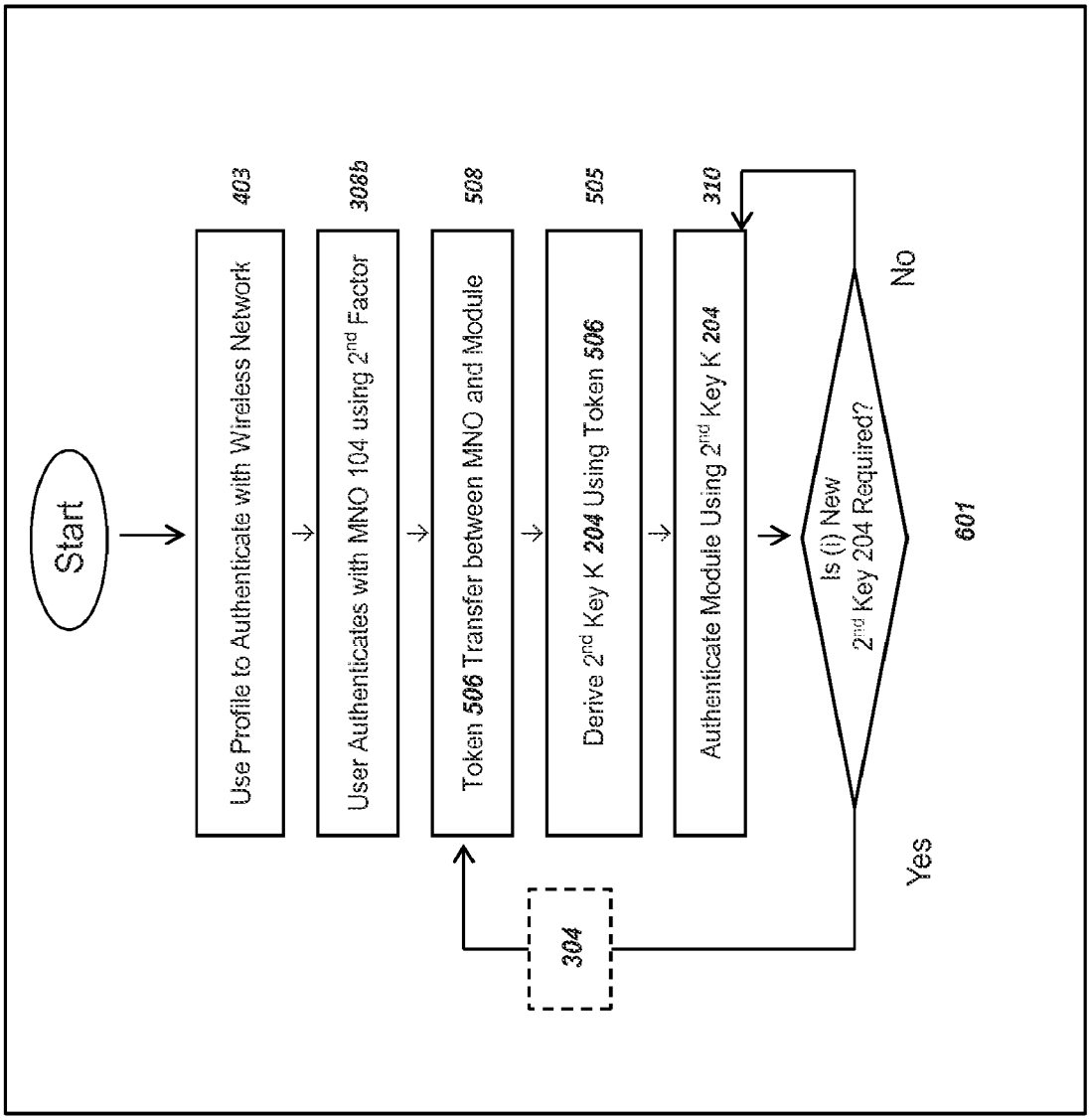
Petitioner Samsung Ex-1004, 0482

Figure 5c



Petitioner Samsung Ex-1004, 0483

Figure 6


Start
Use Profile to Authenticate with Wireless Network
403
User Authenticates with MNO 104 using 2nd Factor
308b
Token 506 Transfer between MNO and Module
508
Derive 2nd Key K 204 Using Token 506
505
Authenticate Module Using 2nd Key K 204
310
Is (i) New 2nd Key 204 Required?
No
Yes
304
601

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	**01/18/2024 05:14:14 PM Z ET**	**63121/0226**

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	63978386	FILING DATE	-
CUSTOMER #	1912	FIRST NAMED INVENTOR	John A. Nix
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Keith Barkaus

Documents

TOTAL DOCUMENTS: 7

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
generatedADS63978386.pdf		6	Application Data Sheet	146 KB
2-PowerofAtty.pdf		2	Power of Attorney	222 KB
3-Parent_Dec.pdf		1	Oath or Declaration filed	129 KB
4-Specification.pdf		134	-	412 KB
4-Specification-SPEC.pdf	(1-129)	129	Specification	398 KB
4-Specification-CLM.pdf	(130-133)	4	Claims	100 KB
4-Specification-ABST.pdf	(134-	1	Abstract	94 KB

	134)		
5-Figs.pdf	12	Drawings-only black and white line drawings	365 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
generatedADS63978386.pdf	72531E06FF2DB6123ABB2ECD43BD140623CB8D218926E833D01ADFD2977103544B78E01660FDD42A2719B3786D1206AF538D3E83A467F7577B68DD088E4A5586
2-PowerofAtty.pdf	535D1E5FC50AE9CF379CE7AC9BF50DEF384ED62904B49A2C62C097378C1E033C7E714A7AFFDDF896974130FAA62A323248EAD24875AA4163913639EAE39492B4
3-Parent_Dec.pdf	08F984090D132484D682191E0883EA4EC380EAF11DA9FA408A63A5B44CD126259DD57794091E6F9D31EC1A5E96C55860A37EDA932FC87DE5FC575AAD508FAC35
4-Specification.pdf	6829DC7AA267D06727E9DBE8252EFB8B8B5FA4F662481DA7B11C1F05951231D2DD9B5ED5F8F395DA9D1AF41540F599F3C774E0A894AD764EDC712B0E74B94A9C
4-Specification-SPEC.pdf	99EEBD41022B7D726786B37924060A8A4870FF1C27D237193AB18BAEEF35DFFBDFBE59683EEA19A528A40E9A54A06D1CC9924FD95EF6639EBE4480B72185 6B4
4-Specification-CLM.pdf	48280CAFFB6095FFF04D99A6CAA2234EF66593245D28E33AF4FB703B8B9CC379BC8E88E6516A7FF804601CD16C83623066A68148895E51ED97B95547D01F6CDF
4-Specification-ABST.pdf	7487794A8A58F537E559394CC76FCA2B6B3F2574569EEDF5C59C2F33E9A375C74DBB84FA1BF34D9377A6E15509504B6746FAA0B0DB1A188B09CFB0676D52D224
5-Figs.pdf	B35D4DE2E007A5C01713FA5B394663BBFF15B89DD055B4031

5628054718ECA17DABF256FEE14D9CC1914DA9ED555B25A6
C8DE952202FD2BB651AE3F03B1CC045

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	Concurrently herewith
First Named Inventor	John A. Nix
Title	An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0226

SIGNATURE of Applicant or Patent Practitioner

Signature	/Keith J. Barkaus/	Date (Optional)	2024-01-18
Name	Keith J. Barkaus	Registration Number	51,431
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 01912

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

NETWORK-1 TECHNOLOGIES, INC.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	Corey M. Horowitz		
Title	Chairman and CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: John A. Nix Date (Optional): June 23, 2015

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR UNITED STATES PATENT

Title: **An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication**

Inventor: John A. Nix
807 Davis St., Unit 409
Evanston, IL 60201
Citizen of the United States of America

Petitioner Samsung Ex-1004, 0491

CROSS-REFERENCE TO RELATED APPLICATIONS

This is a continuation of U.S. Patent Application No. 17/547,990, filed December 10, 2021 , and entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication", which is a continuation of U.S. Patent Application No. 16/453,682, filed June 26, 2019, entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," which is a continuation of U.S. Patent Application No. 16/110,804, filed August 23, 2018, entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," which is a continuation of U.S. Patent Application No. 15/928,848, filed March 22, 2018, entitled "EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION," which is a continuation of U.S. Patent Application No. 14/751,119, filed June 25, 2015, entitled "An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication", now U.S. Patent No. 9,961,060, which is a continuation of U.S. Patent Application No. 14/099,329, filed December 6, 2013, entitled "An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," now U.S. Patent No. 9,100,175, the contents of all of which are incorporated herein by reference in their entirety.

The subject matter of this application is related to the subject matter of U.S. Patent Application Serial No. 14/084,141, filed November 19, 2013 in the name of John Nix, entitled "Key Derivation for a Module using an Embedded Universal Integrated Circuit Card," now U.S. Patent No. 9,319,223, which is hereby incorporated by reference in its entirety.

Petitioner Samsung Ex-1004, 0492

BACKGROUND

Technical Field

The present methods and systems relate to communications for a module, and more particularly, to methods and systems for using an embedded universal integrated circuit card (eUICC), where the methods and systems also support the authentication of a user associated with the eUICC.

Description of Related Art

The combination of "machine-to-machine" (M2M) communications and using low-cost sensors, Internet connections, and processors is a promising and growing field. Among many potential benefits, M2M technologies allow the remote monitoring and/or control of people, assets, or a location where manual monitoring is not economic, or costs can be significantly reduced by using automated monitoring as opposed to manual techniques. Prominent examples today include vending machines, automobiles, alarm systems, and remote sensors. Fast growing markets for M2M applications today include tracking devices for shipping containers or pallets, health applications such as, but not limited to, the remote monitoring of a person's glucose levels or heartbeat, monitoring of industrial equipment deployed in the field, and security systems. Many M2M applications leverage either wired Internet connections or wireless connections, and both types of connections continue to grow rapidly. M2M applications may also be referred to as "the Internet of things".

M2M communications can provide remote control over actuators that may be connected to a M2M device, such as, but not limited to, turning on or off a power switch, locking or unlocking a door, adjusting a speed of a motor, or similar remote control. A decision to change or adjust an actuator associated with an M2M device can utilize one or a series of sensor measurements. An M2M device may also be referred to as a "wireless module" or also simply a

Petitioner Samsung Ex-1004, 0493

module. As one example, if a building or room is too cold, then temperature can be reported to a central server by an M2M device and the server can instruct the M2M device to turn on a switch that activates heat or adjusts a thermostat. As the costs for computer and networking hardware continue to decline, together with the growing ease of obtaining either wired or wireless Internet access for small form-factor devices, the number of economically favorable applications for M2M communications grows.

Many M2M applications can leverage wireless networking technologies. Wireless technologies such as, but not limited to, wireless local area networks and wireless wide area networks have proliferated around the world over the past 15 years, and usage of these wireless networks is also expected to continue to grow. Wireless local area network (LAN) technologies include WiFi and wireless wide area network (WAN) technologies include 3rd Generation Partnership Project's (3GPP) 3rd Generation (3G) Universal Mobile Telecommunications System (UMTS) and 4th Generation (4G) Long-term Evolution (LTE), LTE Advanced, and the Institute of Electrical and Electronics Engineers' (IEEE) 802.16 standard, also known as WiMax. The use of wireless technologies with M2M communications creates new opportunities for the deployment of M2M modules in locations less suitable for fixed-wire Internet access, but also creates a significant new class of problems that need to be solved.

One class of problems for using M2M modules with traditional wireless networks results from basic design considerations for the wireless networks, where many wireless wide-area networking standards were designed and optimized for mobile phones, including smart phones. A core element of traditional wireless WAN technologies such as 3GPP and ETSI standards over the past 20 years has included the use of a subscriber identity module (SIM) card within 2G networks and a related universal integrated circuit card (UICC) for 3G and 4G networks, including LTE networks. ETSI standards for a physical UICC as of 2013 include ETSI TR 102 216. Traditionally, these cards have been supplied by a mobile network operator (MNO) and contain 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. The parameters could

Petitioner Samsung Ex-1004, 0494

include (i) an identity such as an IMSI, (ii) a set of frequencies for a mobile phone to scan in order to locate a beacon signal from the MNO, (iii) a preferred access list of other MNOs in order to support roaming in locations where the MNI associated with the IMSI is not available, and (iv) many other related parameters as well. The physical media and cards in the form of a UICC can be appropriate or suitable for a mobile phone or mobile handset, where an end user can readily replace or "swap out" the physical card as the mobile phone changes geographical locations or due to other preferences for the subscriber or end-user. Distributors of either mobile handsets or mobile phone service can physically insert or change an appropriate UICC for the mobile phones as well.

However, the rapid growth for "machine-to-machine" applications has created significant challenges to the traditional model of utilizing physical media such as a UICC in order to provide data and parameters for a module's connectivity to a MNO. Exemplary reasons for potential difficulties with physical media such as a UICC in M2M applications include (i) the modules may be installed in remote locations that are difficult or expensive to reach after installation, such as, but not limited to, tracking devices on shipping containers that can move globally, (ii) a manufacturer or service provider may prefer for the module to be hermetically sealed for business or technical reasons, including the physical UICC may not be easily tampered with, and (iii) a module (such as a tracking device on a 40 foot shipping container) may move between several different countries, and the lowest costs for Internet or data connectivity through the wireless WAN may be through utilizing different UICC cards from different operators, but the cost of swapping the UICC card could be prohibitive.

Other needs for changing a preferred network or network credentials without physically changing a UICC exist as well. These needs have been one motivation for the industry, including ETSI and 3GPP standards bodies, to consider an embedded UICC, also known as an "eUICC". With an eUICC, the operation of an UICC can be essentially "virtualized", such that the data and algorithms within a UICC can be processed in software and distributed through electronic media (such as, but not limited to, a file transfer or file download). Exemplary

Petitioner Samsung Ex-1004, 0495

benefits and technical considerations for using an eUICC in M2M applications as of November 2013 is outlined in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. Note that this published standard from June 2013, and the standard is primarily in the requirements definition phase, and many of the technical specifications for implementation and operation of an eUICC will be defined in the future.

Although the use of an embedded eUICC can solve many of the issues for distributing and managing physical media such as a UICC, many additional challenges remain. Many open and remaining challenges for a eUICC pertain to securely and electronically transferring a new set of MNO network access credentials (such as an IMSI and network key K) to a module in a secure and efficient manner. A need exists in the art for a module to securely obtain network access credentials. Another need exists in the art for the obtained credentials in a eUICC to be fully compatible with the significant installed and legacy base of networks that use a pre-shared secret key K, where the key K serves as the foundation for authentication and ciphering of data for a mobile phone or user equipment, including modules using conventional technology. A successful solution to these needs for M2M applications in the form of an eUICC can also provide a working solution of the needs for regular mobile phones as well, such that a consumer mobile phone or smartphone could implement and utilize an eUICC in order to eliminate the costs and complexity of dealing with a physical UICC.

A need exists in the art for module and a mobile network operator to securely share a pre-shared secret key K without depending on physical distribution of the key K or electronic distribution of the key K through 3rd parties, even in an encrypted form. A need exists in the art for the decryption of data within an eUICC profile to be under the control of the mobile network operator, because the mobile network operator may not control the distribution or release of profiles from an eUICC subscription manager to a module with an eUICC. As currently contemplated in November of 2013 by eUICC standards discussed above, a pre-shared secret key K and related network access credentials are transmitted to a module from an eUICC

Petitioner Samsung Ex-1004, 0496

subscription manager. The pre-shared secret key K is also known as key K in 4G LTE and related networks and key Ki in 3G networks. The resulting security for the electronically transferred, pre-shared secret key K is no stronger than (i) the encryption on the channel used to transfer key K, and (ii) the security and chain of control for keys used to encrypt the communications channel transferring key K to a module or a mobile phone. A module and mobile network operator (MNO) using an electronically transferred key K for network access credentials is dependent on the communications channel for transferring key K, even though that communications channel may be outside the control of the MNO (such as at a time when key K is transferred using another MNO or a different network). Therefore, a need exists in the art for the MNO to securely and efficiently control the use of an electronically transferred key K within a profile for an eUICC, even though copying and distributing the profile may be outside the control of the MNO.

In addition, over an extended period of time such as several years, a mobile network operator could prefer for the key K to periodically rotate or change for an individual module or mobile phone in order to increase security. The continued and extended use of a single key K for all communications with a module or mobile phone can be a security risk, especially with a large volume of data transferred that could be subject to analysis for cryptographic weaknesses by potential attackers. Additionally, in the future a standard key length for key K may increase from today's current 128 bits to a longer key length such as an exemplary 256 bits. With conventional technology where key K is recorded in physical media such as a UICC, the only feasible way to change key K for a module or mobile phone is to physically distribute a new UICC card, with resulting costs and business complexities. A need exists in the art for a module, including a mobile phone, and a MNO to securely and efficiently support a change in network access credentials, including a key K for the module connecting to the MNO, without requiring a physical replacement of a UICC or equivalent physical media recording a key K.

And other needs exist in the art as well, as the list recited above is not meant to be exhaustive but rather illustrative.

Petitioner Samsung Ex-1004, 0497

SUMMARY

Methods and systems are provided for secure and efficient communication using a module to communicate with a server and a mobile operator network. The module can support "Machine to Machine" (M2M) communications, also known as "the Internet of things". The methods and systems contemplated herein can also support other applications as well, including mobile phone handsets connecting to a wireless network, where the wireless network can be associated with or the radio access portion of a mobile network operator. 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. An objective of the invention is to address the challenges noted above for securing the deployment of modules that can utilize an embedded universal integrated circuit card (eUICC) and/or also PKI algorithms and keys.

The methods and systems contemplated herein can reduce the need for manual intervention with a module in order to automatically and remotely change network access credentials in order for the module to utilize new or different keys in order to connect and authenticate with a wireless network. By using an eUICC, where the eUICC can support both (i) the authentication of a user by the MNO, and (ii) the secure decryption or derivation of the key K under control of the MNO, the value and usefulness of modules can be increased for a user and a mobile operator network. An eUICC can also comprise software and/or firmware components to "virtualize" the operation of a physical UICC, such that (i) the data normally recorded in a physical UICC can be recorded in a file with encryption, and (ii) the steps for using the data in the file can be processed by an eUICC.

In a first embodiment, a mobile network operator can process a set of data for inclusion in a profile for an eUICC. Data within the profile can be equivalent or similar to the data recorded in a physical UICC, including a set of network parameters, a module network identity, and a first key K. The mobile network operator can send the data for a profile to an eUICC

Petitioner Samsung Ex-1004, 0498

subscription manager. A module can include an embedded universal integrated circuit card (eUICC). The eUICC can be processed by an operating system on the module and can be recorded in a nonvolatile memory, such that the eUICC is available after a powered off state. The eUICC can include data such as an eUICC identity, an eUICC profile key, and a symmetric ciphering algorithm. A manufacturer or distributor could record the data for the eUICC before the module is received by a user. The eUICC can communicate in the module with a network application. The network application can communicate with the mobile network operator using a wireless network and a radio within the module. The module can connect with a first network, send the eUICC identity and receive an encrypted profile, and the module can record the encrypted profile in a nonvolatile memory associated with the eUICC. The first network can be a network different than the wireless network for the profile, and the first network could comprise a WiFi network, a LAN connection using a USB interface to the module, or a public land mobile network.

Continuing with this first embodiment, the encrypted profile as received by the module can include a first portion of ciphertext and a second portion of ciphertext. The module using the eUICC can decrypt the first potion of ciphertext using the eUICC profile key and the symmetric ciphering algorithm. The resulting plaintext from the decrypted first portion of ciphertext can include the set of network parameters, the first network module identity, and the first key K. The module using the eUICC can select and activate the profile in order to connect with the wireless network associated with the mobile network operator. The module can conduct a first authentication with the mobile network operator using the first network module identity and the first key K. The module can send an attach request message, including an exemplary radio resource request message with the first network module identity, and the module can receive a random number in the form of a first RAND value.

Continuing with this first embodiment, the module can forward the RAND to the eUICC with the activated profile. The eUICC can input the first RAND and the first key K into a cryptographic algorithm in order to output a response RES value. The eUICC can return the

Petitioner Samsung Ex-1004, 0499

RES value to the module, and the module could forward the RES to the wireless network. The wireless network can compare the received RES with a stored, expected RES (previously calculated using the same first RAND and first key K), and if the two RES values match then the module with the eUICC and profile can be authenticated by the network. The network and the module can take additional steps for the module to have at least limited access to an IP network. With access to the IP network for the module, a user associated with the module can conduct an authentication with the mobile network operator (whereas the mobile network operator may not have control over distribution of the profile with the network access credentials including the first key K up to this point).

Continuing with this first embodiment, the mobile network operator can authenticate or verify a user or M2M service provider associated with the module. The authentication or verification could comprise steps to verify a user, including the user entering information in a web page through the IP connection established with the network in the paragraph above using the first key K. Or the user could place a telephone call to a call center, and the user could verbally confirm identification information or enter DTMF digits. Or, the MNO could authenticate or verify the identity of a user associated with the module by a representative of the MNO visually viewing physical identification of the user such as a drivers license or a passport. If the module is associated with or operated by an M2M service provider, then the MNO could exchange data with the M2M service provider in order to confirm the module with the first key K is authenticated. In either case, where the module is associated with a user or an M2M service provider, the MNO could take steps to authenticate with a second factor, where authentication with the first factor comprised receiving the RES. After successful authentication with the second factor, the MNO can confirm the identity of an entity associated with the module, whereas that identity may not be known before the authentication with the second factor since the distribution of the eUICC profile may be outside the control of the mobile network operator.

Continuing with this first embodiment, after successful authentication with the second factor, the mobile network operator can send a symmetric key to the module. The symmetric key

Petitioner Samsung Ex-1004, 0500

can be encrypted with a key ciphering algorithm. Or, the symmetric key can be (i) plaintext at the application layer, and (ii) encrypted at the data-link layer using the encryption between the module and wireless network after the first authentication above with the first key K. The module can receive the symmetric key (and decrypt the symmetric key if encrypted), and subsequently decrypt the second portion of ciphertext in the eUICC profile. The second portion of ciphertext can include a second network module identity and a second key K. The module can convert the second portion of ciphertext into plaintext using the symmetric ciphering algorithm and the received symmetric key. Note that the decryption of the second portion of ciphertext in the profile without the symmetric key is not feasible, and thus the mobile network operator can retain control over the use of the second key K in the profile for the eUICC, such as not releasing the symmetric key until after a user has successfully completed authentication with the mobile network operator as contemplated in the paragraph above.

After decrypting the second portion of ciphertext, the module with the eUICC can read a plaintext second network module identity and second key K. The second key K can be recorded in a protected, nonvolatile memory. The module can disconnect from the wireless network (where the first session used the first key K), and reconnect with the wireless network using the second network module identity and the second key K. The module with the eUICC can conduct a second authentication using the second key K, including sending the second network module identity, receiving a second RAND value, calculating a second RES value using the second RAND and the second key K, and sending the second RES value. After a successful second authentication, the module can access the IP network and the public Internet through the wireless network, and subsequent authentications with the wireless network can continue to use the second network module identity and the second key K. For embodiments where the module comprises a mobile phone and the user is an individual subscribing to mobile phone services from the mobile network operator, the user can be associated with a telephone number and place/receive phone calls after a successful second authentication.

Petitioner Samsung Ex-1004, 0501

In another embodiment, the eUICC profile key, associated with decrypting the profile from the eUICC subscription manager, may not be recorded in the eUICC before the eUICC sends an eUICC identity to the module, where the module sends the eUICC identity to the eUICC subscription manager through a first network. The eUICC can record an eUICC private key and the eUICC subscription manager could record an eUICC public key. The eUICC subscription manager can (i) encrypt the profile with the eUICC profile key, and then (ii) encrypt the eUICC profile key with an asymmetric ciphering algorithm and the eUICC public key, where the output is an encrypted eUICC profile key. The eUICC can receive the encrypted eUICC profile key from the eUICC subscription manager and decrypt the encrypted eUICC key using the asymmetric ciphering algorithm and the eUICC private key. After reading the plaintext eUICC profile key, the eUICC can decrypt the encrypted profile using the plaintext eUICC profile key, in order to read a plaintext first key K and first network module identity.

In an exemplary embodiment, the first key K is a null value for a profile recorded in the eUICC in a module. The use of a null value or the number zero for a shared secret key K is contemplated in wireless WAN standards and supported by commercial wireless networks in order to support emergency services for a module without a valid UICC. With a null value for the first key K, the MNO and wireless network can provide limited access to the IP network, such that a user of the module with a null or zero value for the first key K could perform steps to authenticate or verify the user with the MNO through the IP network accesses with the first key K as a null value. The data-link layer may not be effectively ciphered due to the use of a null value for the first key K, but the application or transport layer could secure communication from a web browser on the module to a web server for the user to authenticate with the MNO. The secure communication between the web browser and web server can utilize transport layer security (TLS) or similar standards for security at the transport or application layer, even though the data-link or network layer may not be encrypted. After successful authentication via the web browser, the MNO can take steps (discussed in other embodiments) allowing the module with

Petitioner Samsung Ex-1004, 0502

the eUICC to access and use a second key K and a second network module identity for subsequent secured communication between the module and the MNO.

In another embodiment, the second key K can be derived using by both the mobile network operator and the module with the eUICC using a key derivation algorithm. The eUICC could include an eUICC key exchange algorithm and the mobile network operator could include a MNO key exchange algorithm, and the key exchange algorithms can include a key derivation algorithm that accepts input of a token value, a private key, and a public key for the other node. The mobile network operator and the module with the eUICC could communicate the token value used for the key derivation algorithm (including using the connectivity through the wireless network after using the first key K in the profile). The module can record an eUICC private key, and the MNO can have access to the eUICC public key. The key derivation algorithm in the eUICC key exchange algorithm can output a second key K using the token. The MNO can obtain the same value for the second key K. In this manner, both node can derive the same second key K without electronically transferring the second key K, even in encrypted form and thereby increasing the security of a systems with an eUICC.

In an exemplary embodiment can support a module changing a key K used to (i) authenticate with a wireless network and (i) cipher/decipher data with a wireless network. The module can change key K without requiring the manual exchange of a UICC or other physical intervention. The module can use an eUICC profile and change key K while using the same eUICC profile. The module, could also comprise a mobile phone such as, but not limited to, a smart phone. After connecting with a first network, which could comprise a first wireless WAN, wireless LAN, or wired connection, the module can receive a eUICC profile for an eUICC in the module, where the eUICC profile includes a first network module identity and a first key K. The first key K can be a standards-based key K used with wireless networks, and be equivalent to a pre-shared secret key K recorded in physical UICCs for LTE networks.

After authenticating with the wireless network using the first key K, the module and MNO can share a token. The module and MNO can mutually derive a second key K using the

Petitioner Samsung Ex-1004, 0503

token and a key derivation algorithm. The module can disconnect from the wireless network after attaching using the first key K, and then reconnect using the second key K which has now been mutually derived by both the module and the mobile network operator. The module or MNO could determine or evaluate if the use of a new key K is required or preferred, and share a new token for input into the key derivation algorithms to derive a mutually shared new key K. In this manner, a module can change the key K used to authenticate and cipher/decipher data with a wireless network from a first key K to a second key K. This can increase flexibility of the system and reduce costs of physically distributing a new UICC to the module (or electronically sending new eUICC profiles) in order to change a key K.

These as well as other aspects and advantages will become apparent to those of ordinary skill in the art by reading the following detailed description, with reference where appropriate to the accompanying drawings.

Petitioner Samsung Ex-1004, 0504

BRIEF DESCRIPTION OF THE DRAWINGS

Various exemplary embodiments are described herein with reference to the following drawings, wherein like numerals denote like entities.

Figure 1a is a graphical illustration of an exemplary system that includes a module and a mobile network operator, in accordance with exemplary embodiments;

Figure 1b is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments;

Figure 1c is a graphical illustration of components within a module, in accordance with exemplary embodiments;

Figure 1d is a graphical illustration for authenticating with a wireless network using a physical UICC, in accordance with conventional technology;

Figure 1e is a graphical illustration for authenticating with a wireless network using an eUICC, in accordance with exemplary embodiments;

Figure 1f is a graphical illustration of an exemplary system that includes a module, a mobile network operator, and an eUICC in accordance with exemplary embodiments;

Figure 2a is a graphical illustration of an exemplary profile for an eUICC, including encrypted data, decryption steps, and decrypted data for the profile, in accordance with exemplary embodiments;

Figure 2b is a graphical illustration for ciphering and deciphering a profile using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments;

Figure 2c is a graphical illustration for ciphering and deciphering a key K using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments;

Figure 2d is a graphical illustration of a public key and a private key for an eUICC, in accordance with exemplary embodiments;

Petitioner Samsung Ex-1004, 0505

Figure 2e is a graphical illustration for ciphering and deciphering a key for an eUICC using an asymmetric ciphering algorithm using a PKI key pair, in accordance with exemplary embodiments;

Figure 3 is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments;

Figure 4 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments;

Figure 5a is a graphical illustration of a public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments;

Figure 5b is a graphical illustration of deriving a second key K using public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments;

Figure 5c is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments; and,

Figure 6 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments.

Petitioner Samsung Ex-1004, 0506

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS OF THE INVENTION

Figure 1a

Figure 1a is a graphical illustration of an exemplary system that includes a module and a mobile network operator, in accordance with exemplary embodiments. The system 100 includes a module 101 operating within a wireless network 102. System 100 can also include a mobile network operator 104, an IP Network 111, and an eUICC subscription manager 109. Mobile network operator (MNO) 104 can include a server 105. For embodiments where the MNO 104 uses 4G LTE and LTE Advanced networks, server 105 could comprise a home subscriber server (HSS) and/or a mobility management entity (MME). Server 105 could be a server with related functionality as a HSS or MME for a MNO 104 that uses different wireless network standards than those based on 4G LTE. Although not illustrated in Figure 1a, an eUICC subscription manager 109 may also include one or more servers 105, such that a first server 105 could function as an HSS in 4G LTE and LTE Advanced networks and a second server 105 could function as a MME in 4G LTE and LTE Advanced networks.

System 100 is illustrated without specific packet transmissions between module 101 and mobile network operator 104 and eUICC subscription manager 109. Examples of the communications and messages pertaining to the present invention will be illustrated in later Figures. As contemplated herein, machine-to-machine communications may comprise communication between a module 101 and a server 105, such that data can be transferred between the two with minimal manual intervention, although manual intervention can be required to set up system 100 and any occasional manual maintenance required. As contemplated herein, machine-to-machine communications may also be referred to as "the Internet of things" (IoT). Also note that module 101 may comprise a wireless module, such that module 101 can communicate with wireless network 102 using a radio and an antenna. A wireless or a wired configuration for module 101 can be utilized in the present invention.

Petitioner Samsung Ex-1004, 0507

If module 101 operates as a wireless module, module 101 and wireless network 102 can communicate using a base station 103. Module 101 and wireless network 102 can utilize a variety of wireless technologies to communicate, including WiFi, WiMax, a 2nd generation wireless wide area network (WAN) technology such as, but not limited to, General Packet Radio Services (GPRS) or Enhanced Data rates for GSM Evolution (EDGE), 3rd Generation Partnership Project (3GPP) technology such as, but not limited to, 3G, 4G LTE, or 4G LTE Advanced, and other examples exist as well including wireless networks based on WiMAX standards. A wired module 101 can connect to the IP Network 111 via a wired connection such as, but not limited to, an Ethernet, a fiber optic, or a Universal Serial Bus (USB) connection (not shown).

Generally, the communication techniques described herein can be independent of the network technologies utilized at the physical and data-link layers, so long as the underlying network provides access to the IP Network 111 and supports Internet Protocols (IP). The IP Network 111 can be an IPv4 or an IPv6 packet-switched based network that utilizes standards derived from the Internet Engineering Task Force, such as, but not limited to, RFC 786 (User Datagram Protocol), RFC 793 (Transmission Control Protocol), and related protocols. The IP Network 111 can be the public Internet comprising globally routable IP addresses, or a private network that utilizes private IP addresses. IP Network 111 as illustrated in Figure 1a could comprise the globally routable public Internet, or IP Network 111 could also be a private Internet that is (i) not globally routable and (ii) only accessible to authorized modules and servers. As one example of a private IP Network 111, IP Network 111 could use private IP addresses for nodes on the network, and in this case IP Network 107 could be referred to as an intranet or private network. Alternatively, IP Network 111 could be a private network layered on top of the publicly routable Internet via secured and encrypted connections. The specific numbers for IP addresses and port numbers shown in Figure 1a and other figures are illustrative and any valid IP address or port number can be used, including an IPv4 and an IPv6 address. Server 105 within mobile network operator 104 can communicate with the module 101 using IP network 111,

Petitioner Samsung Ex-1004, 0508

where IP network 111 can comprise a private network that utilizes Internet Protocol standards. Module 101 can access the public Internet after authenticating with the server 105 associated with the MNO 104.

When operating in a wireless network configuration, module 101 can access the IP Network 111 via the wireless network 102. In the wireless network configuration, 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. Examples of wireless modules that utilize a wireless WAN such as, but not limited to, 2G and 3G networking technologies include the Motorola® G24-l and Huawei® MC323. Example manufacturers of wireless modules in 2012 include Sierra Wireless® and Telit®. Example leading manufacturers of mobile phones in 2013 include Apple® and Samsung®. In a wired configuration (not shown), module 101 can be a computer, security camera, security monitoring device, networked controller, etc. Module 101 can include a module identity 110, which can comprise a serial number or identity code in order to identify an individual, specific module 101 among a plurality of modules 101. A more detailed depiction of exemplary components of a module 101 is included in Figure 1b and Figure 1c below. Module 101 could also operate as a "smartcard" such that an end user presents module 101 to merchants for payments.

Wireless network 102 may comprise either a wireless local area network (LAN) or a wireless WAN such as a public land mobile network (PLMN). Examples for technologies used in wireless LANs include an 802.11 WLAN, Bluetooth, or Zigbee among other possibilities. Module 101 operating in wireless mode could communicate with a base station 103 of a wireless network 102 using a radio and an antenna. Wireless network 102 could operate as a Mode II device according to FCC Memorandum Opinion and Order (FC-12-36) and related white space regulation documents. If module 101 supports IEEE 802.15.4, then wireless network 102 could be a Zigbee network, an ISA100.11a standards-based network, or a 6LoWPAN network as described by IETF RFC 4944. Other possibilities exist as well for the wireless technology

Petitioner Samsung Ex-1004, 0509

utilized by a wireless network 102 and module 101, operating in a wireless mode, without departing from the scope of the present invention.

System 100 can include an eUICC subscription manager 109, where an eUICC subscription manager 109 can manage the recording and secure distribution of eUICC profiles 107c to a module 101. Example entities that could operate or control an eUICC subscription manager 109 include a manufacturer of module 101, an M2M service provider that manages the operation of module 101, or possibly a mobile network operator 104 could operate the eUICC subscription manager 109. Other entities could operate as an eUICC subscription manager 109 as well. An exemplary eUICC subscription manager 109 is described in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. An eUICC subscription manager 109 can also use a server 105 and record private keys and public keys for the server/subscription manager operation (including exemplary keys depicted and described in connection with Figure 2d below).

In exemplary embodiments, eUICC subscription manager 109 can use an eUICC profile key 107b to cipher portions of an eUICC profile 107c, such that only module 101 with the same eUICC profile key 107b could reasonably decipher the portions of the eUICC profile 107c. In this manner, the eUICC profile 107c can remain reasonably secured. The eUICC subscription manager 109 can share the eUICC profile key 107b in several different ways, including (i) pre-sharing the eUICC profile key 107b, or (ii) the eUICC subscription manager 109 sending the eUICC profile key 107b to the eUICC 107 using an asymmetric ciphering algorithm 219 as depicted and described in connection with Figure 2e below. An eUICC profile 107c can include an eUICC profile identity 107e in order to identify a profile among a plurality of eUICC profiles 107c. An eUICC subscription manager 109 can include an address 109a. The address 109a could comprise a domain name, such that a domain name system (DNS) or secure DNS (DNSSEC) query could resolve the name into an IP address in order for module 101 to communicate with the eUICC subscription manager 109. Or the address 109a could comprise an

Petitioner Samsung Ex-1004, 0510

Internet Protocol (IP) address, and the address 109a could include or be associated with a port number, such as port number 443 for data that utilizes transport layer security.

An eUICC 107 within module 101 can comprise an embedded universal integrated circuit card (eUICC) 107. An eUICC 107 can provide the equivalent functionality as a physical UICC, where definitions for a physical UICC are included in ETSI TR 102 216 and ETSI TS 102 221 V11.0.0, and other examples for the use of a physical UICC in mobile phones and M2M modules exist as well. An eUICC 107 in Figure 1a can support exemplary requirements for an eUICC outlined in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. In other words, an eUICC 107 can operate as a "virtualized" UICC, such that data operations and input/output to a physical UICC can be provided by an eUICC 107. Exemplary details of a conventional, physical UICC for authenticating a module 101 (which can be "virtualized in an eUICC 107) are depicted and described in connection with Figure 1d below. An eUICC 107 can include an eUICC identity 107a, such that an eUICC subscription manager 109 can select and identify the eUICC 107 among a plurality of eUICCs 107. The eUICC 107 can also record an eUICC profile key 107b and an eUICC profile 107d. Profile 107d can represent a profile that is partially decrypted using the eUICC profile key 107b, as depicted and described in connection with Figure 2a below. Additional exemplary details for the operation of an eUICC 107 within module 101 are also provided in Figure 1b, Figure 1c, Figure 1e, and Figure 1f below.

According to an exemplary embodiment, an eUICC 107 can be recorded and operate within a "eUICC supporting" physical universal integrated circuit card (UICC) 108 within module 101. This "eUICC supporting", physical UICC 108 can include a processing unit, RAM memory, ROM memory, EEPROM memory, a bus, and a physical interface (not shown in Figure 1a, but described in Figure 1b). An exemplary processing unit, RAM memory, ROM memory, EEPROM memory, and bus are depicted and described in connection with Figure 1b below. The physical interface for an UICC 108 is depicted and described in connection with Figure 1d below. The "eUICC supporting" physically UICC 108 can perform all of the functions of an

Petitioner Samsung Ex-1004, 0511

eUICC 107, including (i) receiving and recording profiles 107d, (ii) receiving and recording eUICC profile keys 107b, (iii) recording an eUICC identity 107e, (iv) decrypting an eUICC profile 107c into an eUICC profile 107d as depicted and described in connection with Figure 2a below, (v) recording a set of network parameters 201 (in Figure 2a below) for module 101 to connect with wireless network 102, and (vi) recording keys such as a key K for conducting a message digest authentication with wireless network as depicted and described in Figures 1d, Figure 1e, and Figure 3 below. An "eUICC supporting" physical UICC 108 can include a physical electrical interface of ISO/IEC 7816-3 in order to support existing physical slots for UICCs. The use of an "eUICC supporting" physical UICC 108 is optional, and can be omitted. In this case (where "eUICC supporting" physical UICC 108 is omitted), the eUICC 107 can operate as a program within module 101 as depicted and described in connection with Figure 1b below, and the eUICC 107 would not reside within the "eUICC supporting" physical UICC 108.

The physical form-factor for an "eUICC supporting" UICC 108 could be identical to a UICC, and a difference between the two may not even be apparent upon visual inspection without special markings on the card. The physical form-factor for an "eUICC supporting" UICC 108 could comprise a "micro-SIM" or a "nano-SIM" as defined in ETSI TS 102 221 V11.0.0, which is herein incorporated by reference. When the module 101 detects a "eUICC supporting" UICC 107, the module 101 could send received eUICC profiles 107c to the "eUICC supporting" UICC 107, and also select, deselect, activate, and deactivate the different received eUICC profiles 107d recorded in the "eUICC supporting" UICC 108. When a module 101 detects that a regular UICC (i.e. not an "eUICC supporting " UICC 108) has been loaded into a slot for UICCs within the module, the module 101 could access the UICC in a regular manner implemented by mobile phones and modules for connecting to existing wireless networks in 2013, such as LTE or 3G networks. This use of conventional technology for a physical UICC is depicted and described in connection with Figure 1d below.

A module 101 can be associated with a user 113 or an M2M service provider 115. A user 113 could be a subscriber to mobile phone services provided by the mobile network operator

Petitioner Samsung Ex-1004, 0512

104. In this case, the user could be an individual and the module 101 could comprise a mobile phone with a telephone number, an email client, and a web browser (in addition to other, standard functionality for a mobile phone). The user 113 could periodically charge the module 101 (which can comprise a mobile phone), such as typically at night and carry the module 101 during the day in order to place calls and send/receive data. Thus, the user 113 may typically be physically close to a mobile phone as module 101, but an M2M service provider 115 can be associated with module 101 but may not be physically close to module 101. For embodiments where module 101 is associated with M2M communications, such as including a sensor to collect data regarding a monitored unit, the module 101 can be associated with an M2M service provider 115. In this case, the M2M service provider 115 can be a company or a division or department within a larger company that is associated with a plurality of modules 101 for collecting data using sensors and sending the data to a server similar to server 105. The M2M service provider 115 may operate the server similar to server 105 in order to automatically collect data from the plurality of modules 101. The server for the M2M service provider 115 could communicate with module 101 using the IP network 111 and the wireless network 102 when module 101 is connected to the wireless network 102.

Other configurations besides the one illustrated in Figure 1a are possible as well. In many common commercial relationships for the operation of mobile phone service in the United States in 2013, wireless network 102 could represent a portion of the radio access network used by a mobile network operator 104. MNO 104 could outsource portions of the operation and maintenance of a radio access network, such as a wireless network 102, to 3rd parties. In this configuration, wireless network 102 could represent a network operated by a first company specializing in the operation of radio towers and BTS equipment. This first company could be contracted with the mobile network operator 104 in order to support mobile phone service or data services to modules 101.

In addition, server 105 could reside within wireless network 102 in a data center managed by wireless network 102. Wireless network 102 could also operate as an eUICC subscription

Petitioner Samsung Ex-1004, 0513

manager 109. Although a single module 101, server 105, wireless network 102, and mobile network operator 104 are illustrated in Figure 1a, system 100 could comprise a plurality of each of these elements. Module 101 could also record sensor data pertaining to a monitored unit (not shown). Module 101 could be mobile, such as physically attached to a truck or a pallet, and module 101 could connect to a series of different wireless networks 102 or base stations 103 as module 101 moves geographically. Other configurations are possible as well for the elements illustrated in Figure 1a without departing from the scope of the present invention.

Figure 1b

Figure 1b is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments. Figure 1b is illustrated to include many components that can be common within a module 101, and module 101 may also operate in a wireless configuration in order to connect with a wireless network 102. In a wireless configuration, the physical interface 101a of module 101 may support radio-frequency (RF) communications with networks including a wireless network 102 via standards such as, but not limited to, GSM, UMTS, mobile WiMax, CDMA, LTE, LTE Advanced, and/or other mobile-network technologies. In a wireless configuration, the physical interface 101a may also provide connectivity to local networks such as, but not limited to, 802.11 WLAN, Bluetooth, or Zigbee among other possibilities. In a wireless configuration, module 101 could use a physical interface 101a be connected with both a wireless WAN and wireless LAN simultaneously. In a wired configuration, the physical interface 101a can provide connectivity to a wired network such as, but not limited to, through an Ethernet connection or USB connection. As contemplated herein, a physical interface 101a can include a network interface (such as a radio or an Ethernet port), such that module 101 can use the network interface in order to connect with a network and communicate with the network. A network interface can also comprise a physical interface 101a as contemplated herein.

Petitioner Samsung Ex-1004, 0514

The physical interface 101a can include associated hardware to provide the connections such as, but not limited to, radio-frequency (RF) chipsets, a power amplifier, an antenna, cable connectors, etc., and additional exemplary details regarding these components are described below in Figure 1c. Device driver 101g can communicate with the physical interfaces 101a, providing hardware access to higher-level functions on module 101. Device drivers 101g may also be embedded into hardware or combined with the physical interfaces 101a. Module 101 may preferably include an operating system 101h to manage device drivers 101g and hardware resources within module 101. The operating systems described herein can also manage other resources such as, but not limited to, memory and may support multiple software programs operating on module 101 at the same time.

The operating system 101h can include Internet protocol stacks such as, but not limited to, a User Datagram Protocol (UDP) stack, Transmission Control Protocol (TCP) stack, a domain name system (DNS) stack, etc., and the operating system 101h may include timers and schedulers for managing the access of software to hardware resources. The operating system shown of 101h can be appropriate for a low-power device with limited memory and CPU resources (compared to a server 105). An example operating system 101h for module 101 includes Linux, Android® from Google®, Windows® Mobile, or Open AT® from Sierra Wireless®. Additional example operating systems 101h for module 101 include eCos, uC/OS, LiteOs, and Contiki, and other possibilities exist as well without departing from the scope of the present invention.

A module program 101i may be an application programmed in a language such as, but not limited to, C, C++, Java, and/or Python, and could provide functionality to support regular mobile phone functionality. The module program 101i could include a network application 101x, where network application 101x comprises the user equipment protocol for accessing and communicating with the wireless network 102. For embodiments where module 101 connects with a wireless network 102 comprising an LTE network, the network application 101x can receive, process, and send signals with the wireless network 102 for user equipment messages in

Petitioner Samsung Ex-1004, 0515

ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification", which is herein incorporated by reference. In other words, network application 101x can comprise software for accessing and communicating with the wireless network 102. Although network application 101x is depicted in Figure 1b as operating as software within RAM memory 101e, the network application 101x could be included in firmware or a processor or application associated with a radio 101z (described in Figure 1c). Exemplary messages sent and received by a network application 101x are also depicted and described in connection with Figure 3 below.

A module program 101i could also include software for M2M applications such as, but not limited to, remote monitoring of sensors and remote activation of actuators. Module program 101i could also include a software routine, subroutine, linked library, or software module, according to one preferred embodiment. As contemplated herein, a module program 101i can include an application operating within a smartphone, such as, but not limited to, an iPhone® or Android®-based smartphone, and in this case module 101 could comprise a smartphone. The application functioning as a module program 101i could be downloaded from an "app store" associated with the smartphone. A set of device drivers 101g could include an eUICC driver 129, such that a network application 101x or other software or firmware within module 101 communicating with the eUICC 107 could send and receive data with the eUICC driver 129. Additional details regarding an exemplary eUICC driver 129 are depicted and described in connection with Figure 1e below.

Many of the logical steps for operation of module 101 or eUICC 107 can be performed in software and hardware by various combinations of physical interface 101a, device driver 101g, operating system 101h, and a module program 101i. As depicted in Figure 1b, module program 101i can include an eUICC 107 and a network application 101x. When module 101 or eUICC 107 is described herein as performing various actions such as acquiring an IP address, connecting to the wireless network, monitoring a port, transmitting a packet, sending a message, receiving a response, or encrypting or signing data, specifying herein that module 101 or eUICC

Petitioner Samsung Ex-1004, 0516

107 performs an action can refer to software, hardware, and/or firmware operating within module 101 illustrated in Figure 1b or Figure 1c performing the action.

Note that module 101 may also optionally include user interface 101j which may include one or more devices for receiving inputs and/or one or more devices for conveying outputs. User interfaces are known in the art and thus user interfaces are not described in detail here. User interface 101j could comprise a touch screen if module 101 operates as a smartphone or mobile phone. For embodiments where module 101 comprises a module for M2M applications and is associated with an M2M service provider 115, then module 101 can optionally omit a user interface 101j, since no local user 113 input may be required for many M2M applications, although a user interface 101j could be included with module 101. For embodiments where module 101 comprises a mobile phone and is associated with a user 113, the user interface 101j could comprise a touch screen on the front of a mobile phone.

Module 101 may be a computing device that includes computer components for the purposes of collecting data from a sensor 101f or triggering an action by an actuator 101y. Module 101 may include a central processing unit (CPU) 101b, a random access memory (RAM) 101e, and a system bus 101d that couples various system components including the random access memory 101e to the processing unit 101b. The system bus 101d may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures including a data bus. Note that the computer components illustrated for the module 101 in Figure 1b may be selected in order to minimize power consumption and thereby maximize battery life, if module 101 includes a battery and is not attached to external power. In addition, the computer components illustrated for the module 101 in Figure 1b may also be selected in order to optimize the system for both long periods of sleep or idle states relative to active communications and also may be optimized for predominantly uplink (i.e. device to network) communications with small packets or messages. The computer components illustrated for the module 101 in Figure 1b may also be general-

Petitioner Samsung Ex-1004, 0517

purpose computing components, and specialized components may not be required in order to utilize many of the embodiments contemplated herein.

Module 101 may include a read-only memory (ROM) 101c which can contain a boot loader program. Although ROM 101c is illustrated as "read-only memory", ROM 101c could comprise long-term memory storage chipsets or physical units that are designed for writing once and reading many times. As contemplated within the present invention, a read-only address could comprise a ROM 101c memory address or another hardware address for read-only operations accessible via bus 101d. Changing data recorded in a ROM 101c can require a technician have physical access to module 101, such as, but not limited to, removing a cover or part of an enclosure, where the technician can subsequently connect equipment to a circuit board in module 101, including replacing ROM 101c. ROM 101c could also comprise a nonvolatile memory, such that data is stored within ROM 101c even if no electrical power is provided to ROM 101c. Although not illustrated in Figure 1b, but illustrated in Figure 1c below, module 101 could also include a flash memory 101w. Module program 101i, network application 101x, operating system 101h, eUICC 107, or device drivers 101g could be stored in flash memory 101w within module 101 when the module is powered off. These components and/or instructions could be moved from a flash memory 101w (not shown in Figure 1b but shown in Figure 1c) into RAM 101e when the module is powered on by a bootloader program recorded in the ROM 101c. Note that ROM 101c could be optionally omitted or included in a memory unit within CPU 101b (not shown).

Although the exemplary environment described herein employs ROM 101c and RAM 101e, it should be appreciated by those skilled in the art that other types of computer readable media which can store data that is accessible by a module 101, such as, but not limited to, memory cards, subscriber identity module (SIM) cards, local miniaturized hard disks, and the like, may also be used in the exemplary operating environment without departing from the scope of the invention. The memory and associated hardware illustrated in Figure 1b provide nonvolatile storage of computer-executable instructions, data structures, program modules,

Petitioner Samsung Ex-1004, 0518

module program 101i, and other data for computer or module 101. Note the module 101 may include a physical data connection at the physical interface 101a such as, but not limited to, a miniaturized universal serial bus adapter 101v (illustrated in Figure 1c), firewire, optical, or other another port.

The computer executable instructions such as, but not limited to, module program 101i, network application 101x, eUICC 107, operating system 101h, or device driver 101g can be initially loaded into memory such as, but not limited to, ROM 101c or RAM 101e through the physical interface 101a before module 101 is given to an end user, shipped by a manufacturer to a distribution channel, or installed by a technician. In addition, the computer executable instructions such as, but not limited to, module program 101i, network application 101x, operating system 101h or device driver 101g could be transferred wirelessly to module 101. In either case (wired or wireless transfer of computer executable instructions), the computer executable instructions such as module program 101i, network application 101x, operating system 101h, or device driver 101g could be stored remotely on a disk drive, solid state drive, or optical disk (external drives not shown).

A number of program modules may be stored in RAM 101e, ROM 101c, or possibly within CPU 101b, including an operating system 101h, device driver 101g, an http client (not shown), a DNS client, and related software. Further, the module program 101i and/or network application 101x can perform the various actions described in the present invention for the module 101 through instructions the module program 101i and/or network application 101x provide to the CPU 101b. A user may enter commands and information into module 101 through an optional user interface 101j, such as a keypad, keyboard (possibly miniaturized for a mobile phone form-factor), and a pointing device. Pointing devices may include a trackball, an electronic pen, or a touch screen.

The module 101, comprising a computer, may operate in a networked environment using logical connections to one or more remote computers, such as the server 105 illustrated in Figure 1a. Server 105 can also function as a general purpose server to provide files, programs, disk

Petitioner Samsung Ex-1004, 0519

storage, remote memory, and other resources to module 101 usually through a networked connection. Additional remote computers with which module 101 communicates may include another module 101 or mobile device, an M2M node within a capillary network, a personal computer, other servers, a client, a router, a network PC, a peer device, a base station 103, or other common network node. It will be appreciated that the network connections shown throughout the present invention are exemplary and other means of establishing a wireless or wired communications link may be used between mobile devices, computers, servers, corresponding nodes, and similar computers. Although a single module program 101i is depicted in Figure 1b, module 101 could include a plurality of module programs 101i.

The module program 101i, eUICC 107, and network application 101x operating within module 101 illustrated in Figure 1b can provide computer executable instructions to hardware such as CPU 101b through a system bus 101d in order for a module 101 to (i) connect with a wireless network 102, (ii) authenticate with a mobile network operator 104 associated with the wireless network 102, and (iii) send or receive packets with a server 105 or a server associated with an eUICC subscription manager 109. The module program 101i and/or network application 101x can enable the module 101 or eUICC 107 to transmit or send data from the eUICC 107 or module 101. The eUICC 107 or module 101 can send data by recording data in memory such as RAM 101e, where the data can include cryptographic data such as a RAND and RES values, a destination IP:port number, a packet or packet header value, an encryption or ciphering algorithm and key, a digital signature algorithm and key, etc. The data recorded in RAM 101e can be subsequently read by the operating system 101h or the device driver 101g. The operating system 101h or the device driver 101g can write the data to a physical interface 101a using a system bus 101d in order to use a physical interface 101a to send data to the wireless network 102 and IP network 111 using a radio 101z (shown in Figure 1c). Alternatively, the module program 101i and/or network application 101x can write the data directly to the physical interface 101a using the system bus 101d.

Petitioner Samsung Ex-1004, 0520

The module program 101i, eUICC 107, network application 101x, and/or operating system 101h can include steps to process the data recorded in memory such as, but not limited to, encrypting data, selecting a destination address, or decrypting ciphertext data. The data recorded in memory could also include an eUICC profile 107c or eUICC profile 107d, as described in Figure 1a above and Figure 2a below. The eUICC profiles 107d can include instructions and data for connecting with wireless network 102, including network parameters and network access credentials. The module 101 can use the physical interface 101a such as, but not limited to, a radio to transmit or send the data associated with a profile 107d to a base station 103. For those skilled in the art, other steps are possible as well for a module program 101i or operating system 101h to communicate with a wireless network 102 using data associated with an UICC (where an eUICC 107 records data normally associated with a physical UICC) without departing from the scope of the present invention.

Conversely, in order for module 101, network application 101x, or eUICC 107 to receive a packet or message from MNO 104 or wireless network 102, the physical interface 101a can use a radio to receive data from a base station 103. The received data can include information from MNO 104 and may comprise a datagram, a source IP:port number, a packet or header value, an instruction for module 101, an acknowledgement to a packet that module 101 sent, a digital signature, and/or encrypted data. The received data can also include radio resource control (RRC) messages, and related layer 1 and layer 2 access and control messages for module 101 to access the wireless network 102. The operating system 101h or device driver 101g can use a system bus 101d and CPU 101b to record the received data in memory such as RAM 101e, and the module program 101i or operating system 101h may access the memory in order to process the received data and determine the next step for the module 101 after receiving the data. The steps within this paragraph may also describe the steps a module program 101i, eUICC 107, or network application 101x can perform in order to receive a message from wireless network 102 that includes a RAND value. For those skilled in the art, other steps are possible as well for a module program 101i, network application 101x, module 101, and/or eUICC 107 to receive a

Petitioner Samsung Ex-1004, 0521

message from a mobile network operator 104 or wireless network 102 within the scope of the present invention.

Module program 101i can include an eUICC 107, which can provide the functionality or CPU 101b instructions for module 101 to access data normally within a physical UICC, such as network parameters and network access credentials. An eUICC 107 as illustrated in Figure 1a and Figure 1b can be implemented within module 101 in several different ways, including (i) as depicted in Figure 1b a module program 101i stored in RAM 101e during operation, but also recorded in a nonvolatile memory, such as, but not limited to, either flash memory 101w (described in Figure 1c) or ROM 101c at other times than normal operation (such as during periods of power off), (ii) firmware within CPU 101b or another specialized processing unit within module 101, (iii) an "eUICC supporting" physical UICC 108 within module 101 that contains the eUICC 107, or (iv) a specialized circuit within a surface mount package that is soldered directly onto a circuit board of the module 101, including an 8-lead small outline non-leaded (SON-8) package. For the embodiment where an eUICC 107 comprises a module program 101i, the eUICC 107 could be loaded and installed within nonvolatile memory 101w in module 101 using the steps and procedures described for a module program 101i in Figure 1b. Other possibilities exist as well for the physical implementation of an eUICC 107 within a module 101 without departing from the scope of the present invention. An eUICC 107 may also be referred to as an "electronic UICC", an "electronic SIM" (eSIM), or an "embedded SIM" (also eSIM).

For embodiments where an eUICC 107 can be loaded into a RAM 101e or flash 101w memory, a CPU 101b could designate the RAM 101e or flash 101w memory containing the instructions or data for an eUICC 107 to be a protected memory. When (i) loaded with appropriate data (such as, but not limited to a eUICC profile 107d described in Figure 2a below), and (ii) a profile for a MNO 104 is selected and activated, then an eUICC 107 can provide the equivalent functionality of a physical UICC. The eUICC 107, using an activated eUICC profile 107d, can provide the module 101 with (i) network access credentials 202 and 203, and (ii)

Petitioner Samsung Ex-1004, 0522

network parameters 201 in order to connect with wireless network 102. The eUICC 107, using an activated eUICC profile 107d, can record a first key K 203 (described in Figures 2a and 3 below) and also a first network module identity 202. The eUICC 107 can support standard steps by module 101 for network authentication contemplated in 3GPP TS 33.401 V12.9.0 and related standards, including inputting a RAND value into the eUICC 107 and outputting a RES value.

Moreover, those skilled in the art will appreciate that the present invention may be implemented in other computer system configurations, including hand-held devices, netbooks, portable computers, multiprocessor systems, microprocessor based or programmable consumer electronics, network personal computers, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments, where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices. In addition, the terms "mobile node", "mobile station", "mobile device", "M2M module", "M2M device", "networked sensor", "industrial controller", or "user equipment" can also refer to module 101 or its functional capabilities. Other possibilities exist as well for the configuration or combination of components illustrated in Figure 1b without departing from the scope of the present invention.

Figure 1c

Figure 1c is a graphical illustration of components within a module, in accordance with exemplary embodiments. Figure 1c is illustrated to show a combination of components useful for leveraging the efficient and secure communication techniques described in the present invention. In addition to the components illustrated in Figure 1b above, module 101 can include a an eUICC 107, a battery 101k, a MNO public key 502, a wireless module private key 112a, a connection to an actuator 101y, a USB interface 101v, a CPU wake controller 101u, a flash memory 101w, a symmetric key 127, a random number generator 128, cryptographic algorithms 141, a radio 101z, and other components illustrated in Figure 1c. Not all of the components

Petitioner Samsung Ex-1004, 0523

illustrated in Figure 1c are required for many exemplary embodiments, and some of the components illustrated in Figure 1c may also be optionally omitted in some exemplary embodiments.

The CPU 101b can comprise a general purpose processor appropriate for the low power consumption requirements of a module 101, and may also function as a microcontroller. CPU 101b could be a processor with an ARM® core, or possibly an ATOM® core or processors, and other possibilities exist as well. The CPU 101b can include registers, a cache memory, and arithmetic logic units. Clock 160 can comprise a crystal oscillator generating sine or square wave outputs at a frequency to drive a system bus 101d, CPU 101b, and RAM 101e, in addition to other functionality. In exemplary embodiments, clock 160 can comprise a temperature-compensated crystal oscillator (TCXO), a voltage-controlled crystal oscillator (VCXO), or a voltage-controlled temperature-compensated crystal oscillator (VCTCXO), and other possibilities exist as well. Clock 160 could include circuits and logic to keep time while module 101 is both in an active state and a dormant state.

Sensor 101f could be a device to collect environmental data or data regarding (i) a monitored unit for M2M applications or (ii) user 113 for applications where module 101 comprises a mobile phone and user 113 is an individual person such as a mobile phone subscriber. Sensor 101f could collect data such as, but not limited to, temperature, humidity, pressure, visible light levels, radiation, shock and/or vibration, voltage, current, weight, pH levels, orientation/motion, or the presence of specific chemicals. Sensor 101f could also be a microphone. Sensor 101f could be a magnetic strip reader for credit cards and similar cards, or an antenna for either near-field RF communications, such as, but not limited to, reading an RF identity tag. An antenna for a sensor 101f could also collect longer-range RF signals, such as, but not limited to, reading long-range radio frequency identity tags. Sensor 101f could also collect biometric data such as, but not limited to, heart rate, glucose levels, body temperature, or other health measurements for a user 113. The sensor 101f can provide data to the CPU 101b in the form of analog or digital data, which can be communicated via a system bus 101d or physical

Petitioner Samsung Ex-1004, 0524

interface 101a and other electrical interfaces are possible as well. A sensor measurement can comprise the analog or digital data collected by CPU 101b from sensor 101f.

A sensor measurement from sensor 101f can include processing of the analog or digital data input CPU 101b by sensor 101f, such as, but not limited to, averaging over time, using mathematic formulas to convert the raw data from sensor 101f into a usable form. Module 101 may also collect sensor data or sensor values using a sensor 101f and CPU 101b, where the data or values are derived from electrical signals output by a sensor 101f. A sensor measurement can comprise the sensor data or sensor values. If module 101 comprises a "point of presence" payment terminal, then a sensor measurement could comprise data read from a payment card. As contemplated herein, the terms "sensor measurement" and "sensor data" can be used interchangeably, and can also be considered functionally equivalent. Although a single sensor 101f is shown in Figure 1c, a module 101 could include multiple sensors. Each of the multiple sensors 101f could include a sensor identity 151, which could comprise a number or string to identify the sensor 101f. A sensor 101f could be external to module 101, and also a plurality of sensors 101f may be used and they also can connect to module 101 when module 101 uses radio 101z as a base station for a WiFi network.

Actuator 101y could be a device to control a parameter or state for a monitored unit in M2M applications for module 101, such as, but not limited to, changing a voltage or current, activating a switch or relay, turning on or off a microphone or speaker, activating or deactivating a light, and other examples are well known in the art. Actuator 101y could also be a speaker. Actuator 101y could be controlled by module 101 via a digital or analog output from CPU 101b, which could also be transmitted or sent via system bus 101d or a physical interface 101a. Although actuator 101y is illustrated as external to wireless module 101 in Figure 1c, actuator 101y could also be internal to module 101, and module 101 could include multiple actuators 101y. A module 101 could include multiple actuators 101y each with an actuator identity 152. Sensors and actuators are well known to those of ordinary skill in the art, and thus are not described in additional detail herein.

Petitioner Samsung Ex-1004, 0525

Module 101 can include a Universal Serial Bus (USB) interface 101v. In accordance with an exemplary embodiment, module 101 can comprise a wireless module and include a radio 101z. Note that the use of a radio 101z is not required for module 101, which could also obtain a connection to the IP Network 111 via a wired line such as Ethernet. Although not illustrated, radio 101z could include antennas for reception and transmission of RF signals, and even multiple antennas could be used. Although a single radio 101z is illustrated in module 101, module 101 could also contain multiple radios 101z. Radio 101z can support wireless LAN standards such as, but not limited to, WiFi, Bluetooth, and Zigbee, or similar wireless LAN standards. Note that module 101 may also operate as a base station in a wireless LAN, such as, but not limited to, an 802.11 base station. When module 101 operates a wireless LAN, radio 101z can function as either a client/node and/or a base station 103 to support communication from other wireless nodes in physical proximity, such as, but not limited to, other nodes within an exemplary 50 meters. The other wireless nodes could comprise a sensor 101f and/or actuator 101y, and in this case a sensor could be referred to as a "networked sensor" and an actuator could be referred to as a "networked actuator".

In accordance with exemplary embodiments, module 101 can store module private key 112a, MNO public key 502, and module identity 110, and a symmetric key 127 in memory/RAM 101e during operation, such as when CPU 101b is active and the module 101 is connected to a network such as a wireless network 102 during data transmissions. Module private key 112a preferably is recorded in nonvolatile memory such as, but not limited to, flash memory 101w, so that module 101 has access to its private key 112a after the private key has been derived or loaded, including times when a battery 101k has been fully drained or removed from module 101 (if module 101 does not utilize a persistent power source such as land-line power). Symmetric key 127 can be a secure, shared private key for use with symmetric encryption or symmetric ciphering algorithms 211 (in Figure 2c below). Symmetric key 127 may also include an expiration time 133, such that symmetric key 127 may only be used by module 101 and/or eUICC 107 during a limited period of time, such symmetric key 127 remaining only valid for a

Petitioner Samsung Ex-1004, 0526

day, or a week, or during a session (where the session comprises multiple messages and/or responses between a module 101 and a wireless network 102), etc.

Module identity 110 is preferably a unique identifier of module 101, and could comprise a number or string such as, but not limited to, a serial number, an international mobile subscriber identity number (IMSI), international mobile equipment identity (IMEI), or an Ethernet media access control (MAC) address. According to an exemplary embodiment, module identity 110 can also comprise a serial number or string that is written into hardware of module 101 upon manufacturing or distribution of module 101 (also depicted and described in connection with a step 511 in Figure 5b below). In this case, module identity 110 could be recorded in a read only memory 101c, where read only memory 101c could not be easily erased or otherwise tampered with. Read only memory 101c could also comprise a protected memory and the address for accessing the module identity 101 within the ROM 101c could comprise a protected address.

A protected address can comprise an address accessible to a CPU 101b and readable by CPU 101b where the data within the protected address is not modified, changed, or updated by a CPU 101b under normal operating conditions. Also note that the protected address can comprise one form of a nonvolatile memory, where a memory records data. In exemplary embodiments module identity 110 may preferably be permanently or persistently associated with the physical hardware of module 101, which can be helpful for the security procedures contemplated herein. Module identity 110 can function as a basic identifier for services from mobile network operator 104, eUICC subscription manager 109, wireless network 102, M2M service provider 115, or server 105 in order to properly identify module 101 among a plurality of modules. Module private key 112a and an associated module public key 112b could be unique to module 101 and uniquely associated with module identity 110, according to a preferred embodiment.

MNO public key 502 in module 101 could be obtained from downloading the key over the IP Network 111, or optionally also written into nonvolatile memory of module 101 upon manufacture or distribution. MNO public key 502 could be obtained using a domain name or Internet address that is recorded in nonvolatile memory upon the configuration of module 101,

Petitioner Samsung Ex-1004, 0527

such as, but not limited to, during installation or distribution, and module 101 could fetch the MNO public key 502 upon connecting to a wireless network 102 or other connection to the IP Network 111. Additional elements besides those depicted in Figure 1c could also be recorded in volatile memory 101e, which could comprise a RAM 101e. For example, cryptographic algorithms 141 could also be recorded in RAM 101e as well. Note that values and related data can also be recorded in both RAM 101e and nonvolatile memory 101w at the same time, such that data in nonvolatile memory 101w allows module 101 to access the data after a shutdown state, but moving the same data into RAM 101e during an active state allows module 101 to more quickly perform operations using a CPU 101b. Other possibilities exist as well for the storage location of various values and data elements illustrated in Figure 1c without departing from the scope of the present invention.

Module 101 may also contain cryptographic algorithms 141, which may comprise a suite of algorithms or subroutines that can be utilized for (i) deriving a pair of keys comprising a public key and a private key, (ii) encrypting data using public keys, (iii) decrypting data using private keys, (iv) processing secure hash signatures using private keys, and (v) verifying secure hash signatures using public keys, and related software, firmware, or subroutines for implementing a cryptographic system, including symmetric ciphering algorithms. Cryptographic algorithms 141 could utilize publicly available software libraries within tools such as, but not limited to, OpenSSL maintained by The OpenSSL Project (http://www.openssl.org/), libgcrypt maintained by The Free Software Foundation (http://www.gnu.org/software/libgcrypt/), and similar libraries such as, but not limited to, libmcrypt and Crypto++. Note that cryptographic algorithms 141 could also use proprietary cryptographic libraries as well. In addition to implementing asymmetric encryption/ciphering, such as, but not limited to, used with RSA and ECC cryptography, cryptographic algorithms 141 can provide symmetric ciphering where a shared private key is utilized to both encrypt and decrypt, such as, but not limited to, with the Advanced Encryption Standard (AES) cipher suite.

Petitioner Samsung Ex-1004, 0528

As illustrated in Figure 1c, module 101 may also contain a random number generator 128. Random number generator 128 may contain a seed 128b. The creation of random numbers with a high degree of entropy may be important the use of cryptographic algorithms 141. 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 101f 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). Note that values or data for each of the elements listed in the previous sentence could be utilized in a "module random seed file" instead of or in addition to a state. The use of a "module random seed file" with a random number generator 128 is also depicted and described in connection with Figure 1d of U.S. Patent Application Serial No. 14/084,141, filed November 19, 2013 in the name of John Nix, which is hereby incorporated by reference in its entirety.

Figure 1d

Figure 1d is a graphical illustration for authenticating with a wireless network using a physical UICC, in accordance with conventional technology. Figure 1d illustrates the components and interfaces for using a physical UICC in order to a module 101 conduct an authentication with a wireless network 102 according to wireless WAN standards which use a pre-shared secret key K recorded in the physical UICC 116. The wireless network could be an LTE, LTE Advanced, or a 3G network, and also based on related standards. With a 3G network, the pre-shared secret key K is also known as "Ki". The module 101 can include a network application 101x, a UICC driver 114, and a physical interface supporting the ISO/IEC 7816-3 electrical standards, such as the third edition published on November 1, 2006. The physical UICC 116 can be a smart card in the form factor of a mini-SIM, micro-SIM, or nano-SIM, connected to the physical interface such as ISO/IEC 7816-3 and related electrical standards. The physical interface can include six electrical contacts known as C1 through C6, where C1 provides a power supply to the physical UICC 116, C2 provides a reset signal input, C3 provides

Petitioner Samsung Ex-1004, 0529

a clock signal input, etc. The network application 101x can comprise software or firmware for the module 101 to communicate with the wireless network 102 using the standards that include layer 2 messages between module 101 and wireless network 102 such as, but not limited to, radio resource control (RRC) messages, security mode commands, ciphering, and authentication. The network application 101x can communicate with a radio 101z (described in Figure 1c) using the system bus 101d.

A network application 101x in a Figure 1d can be similar or equivalent to a network application 101x depicted and described in connection with Figure 1b. The UICC driver 114 can comprise a driver within a set of drivers 101g within module 101, where drivers 101g are also depicted and described in connection with Figure 1b. A physical UICC 116 can support other and additional functionality for a module 101 than the authentication functionality depicted in Figure 1b, such as, but not limited to, (i) recording a set of network parameters equivalent to a set of network parameters 201 in Figure 2a below in order to module 101 to identify and select a wireless network 102, (ii) recording an address book with a list of phone numbers for user 113, (iii) recording a list of recent SMS messages and telephone numbers dialed, and/or (iv) recording and implementing a personal identification number (PIN) in order for a user 113 to authenticate and access the module 101 with the UICC 116, and other functionality of a physical UICC 116 is possible as well. The physical UICC 116 can also include (i) an IP Multimedia Services Identity Module (ISIM) application and data and/or a (ii) Universal Subscriber Identity Module (USIM) application for the module 101 to utilize when communicating with the wireless network 102.

After power-up of the module 101 from a powered off state, the module 101 can use the UICC driver 114 to read data from the physical UICC 116 such as a set of network parameters 203 (depicted in Figure 2a below) as well as an IMSI or equivalent value as a network module identity. The set of network parameters 203 or IMSI in a physical UICC 116 may not be encrypted (or associated with an eUICC profile 107d) and the set of network parameters can be directly read by the UICC driver 114. The module 101 can use the set of network parameters to tune a radio 101z to particular frequencies for the wireless network 102 and search for a beacon

Petitioner Samsung Ex-1004, 0530

signal from a base station 103. The beacon signal can include codes such as a mobile country code (MCC) and mobile network code (MNC) that can match values in either the network parameters or IMSI. Upon finding and selecting a base station 103, the module 101 can send a random access channel (RACH) message and subsequently an identity value recorded in the physical UICC 116 such as an IMSI, temporary mobile subscriber identity (TMSI), a globally unique temporary identity (GTUI), or a similar value to identify the module 101 using the physical UICC 116 with the wireless network 102.

In order to authenticate a module 101 with the wireless network 102, the wireless network 102 can record a set of authentication tokens or vectors associated with a network identity sent by the module 101, such as a GTUI value. An authentication vector 117 for the module's 101 network identity can comprise a vector or set of values that includes a random number (RAND) 118, response (RES) 119, a network authentication token (AUTN), and a sequence number. The value AUTN and sequence number is not shown in Figure 1d and subsequent figures such as Figure 1e and Figure 3, but the value AUTN and sequence number can be used by module 101 with a physical UICC 116 or eUICC 107 in order to authenticate the wireless network 102. The sequence number can prevent replay attacks and the AUTN value can comprise a digital signature or message digest value the physical UICC 116 or eUICC 107 can also calculate using the RAND 118 value in order for the module 101 to authenticate the wireless network 102. The values for the authentication vector 117 that includes a RAND 118 and a RES 119 can be calculated by a home subscriber server (HSS) for the mobile network operator 104 associated with the wireless network 102 and provided by the mobile network operator 104 to servers associated with the wireless network 102. An exemplary format for the use of a RAND 118 with a response RES 119 is described in ETSI standard TR 131 900 v.10.0.0 and related documents. Other possibilities exist as well for the format, structure, and data elements within an authentication vector 117 without departing from the scope of the present invention.

In order to conduct an authentication of module 101, after receiving a RACH message and the network module identity such as an IMSI, TMSI, or GTUI value, the wireless network

Petitioner Samsung Ex-1004, 0531

102 can send a RAND 118 from the authentication vector 117. The module 101 can receive the RAND 118 value using the network application 101x and the radio 101z. The network application 101x can send the RAND 118 value to the UICC driver 114, and the UICC driver 114 can send the RAND 118 value through the physical interface such as ISO/IEC 7816-3 to the physical UICC 116. After receiving the exemplary RAND 118 message, in order to conduct an authentication, module 101 using a physical UICC 116 could take steps to demonstrate to a wireless network 102 that the physical UICC 106 records the same pre-shared secret key K for the network module identity as recorded by a mobile network operator 104 associated with the wireless network 102. Physical UICC 116 can properly respond to the RAND 118 using message digest algorithms by calculating a secure hash value RES 119 using the RAND 118 and the recorded secret key K. The physical UICC 116 could use algorithms specified in ETSI TS 135 205 – 209, as well as subsequent and related standards, in order for the physical UICC 116 to calculate a secure hash value such as a RES 119. The calculation and processing of a RES 119 using a RAND 118 and a secret key K is also depicted and described in connection with steps 306 and 311 of Figure 3. Other possibilities exist as well for a physical UICC 116 or an eUICC 107 to calculate a RES 119 value using a RAND 118 and a secret key K without departing from the scope of the present invention.

After the calculation of a RES 119 value in response to the RAND 118, the physical UICC 116 can send the RES 119 to the UICC driver 114 through the physical interface such as ISO/IEC 7816-3. The device driver 114 can send the RES 119 value to the network application 101x and the network application 101x can send the RES 119 value to the wireless network 102 using a radio 101z and the base station 103. The wireless network 102 can take steps to compare the received RES 119 with a recorded RES 119 value in the authentication vector 117. If the received RES 119 matches the recorded RES 119 in the authentication vector 117 then the module 101 with the physical UICC 116 can be considered authenticated. The authentication of module 101 by wireless network 102 is also depicted and described in connection with a step 308a of Figure 3. After successful authentication, the module 101 and wireless network 102 can

Petitioner Samsung Ex-1004, 0532

then take subsequent steps for a module 101 to have access to the IP network 111 including the public Internet, as well as configuring services such as voice and SMS.

Figure 1e

Figure 1e is a graphical illustration for authenticating with a wireless network using an eUICC, in accordance with exemplary embodiments. A module 101 with an eUICC 107 can perform the equivalent steps for authentication with a wireless network 102, such that a module 101 can use an eUICC 107 instead of a physical UICC 116. The wireless network 102 can perform the same steps as (i) recording an authentication vector 117 from a mobile network operator 104 associated with the wireless network 102, (ii) receiving a RACH message and a network module identity such as a GTUI or TMSI from the module 101, (iii) sending values from the authentication vector 117 including a RAND 118, and (iv) receiving a RES 119 and comparing the received RES 119 with a recorded RES 119 in the authentication vector 117 in order to authenticate the module 101 using an eUICC 107 instead of a physical UICC 116. In other words, the use of an eUICC 107 by module 101 can be transparent to a wireless network 102, such that a module 101 with an eUICC 107 instead of a physical UICC 116 can be fully "backward compatible" with standards, software, and infrastructure deployed on a wireless network 102.

A module 101 in Figure 1e can include a network application 101x, an eUICC driver 129, an eUICC 107, and an operating system 101h. The network application 101x can be equivalent or similar to a network application 101x depicted and described in connection with Figure 1d and Figure 1b above. The use of an eUICC 107 instead of a physical UICC 116 within module 101 can also be transparent to network application 101x, via the use of eUICC driver 129. In other words, in exemplary embodiments, the same or equivalent network application 101x can be used for either (i) a module 101 with a physical UICC 116 or (ii) a module 101 with an eUICC 107, since the eUICC driver 129 can perform the identical input and output functions as a UICC driver 114 when communicating with the network application 101x. The use of an eUICC driver

Petitioner Samsung Ex-1004, 0533

129 is also depicted and described in connection with Figure 1b above. The eUICC driver 129 can communicate with the network application 101x using the operating system 101h. The internal communication between network application 101x and eUICC driver 129 using an operating system 101h could comprise sharing memory 101e, such that network application 101x writes messages such as, but not limited to, an exemplary RAND 118 value into the shared memory 101e and eUICC driver 129 reads the values from the shared memory 101e. In another embodiment, the internal communication between network application 101x and eUICC driver 129 using an operating system 101h could comprise using loopback UDP ports within operating system 101h, such that network application 101x sends a UDP datagram with the RAND 118 value using a first UPD loopback port, and the eUICC driver 129 receives the UDP datagram with the RAND 118 value using a second UDP loopback port. Similar steps could be taken as well for an eUICC driver 129 to send data such as a RES 119 to the network application 101x using the operating system 101h.

As illustrated in Figure 1e, eUICC driver 129 can also communicate with the eUICC 107 using the operating system 101h. Two differences between conventional technology illustrated in Figure 1d and the exemplary embodiment illustrated in Figure 1e include (i) the eUICC driver 129 communicates with the eUICC 107 using operating system 101h instead of a physical interface such as ISO/IEC 7816-3 and related electrical standards, and (ii) the eUICC 107 can operate as a separate program or application within memory 101e or memory 101w instead of a physically separate application operating on a physical UICC 116. The eUICC driver 129 can communicate with the eUICC 107 using the equivalent steps and procedures for an network application 101x to communicate with an eUICC driver 129 described in the paragraph above, including using shared memory or sending UDP loopback messages on internal UDP loopback ports. Other possibilities for the communication between eUICC driver 129 and eUICC 107 exist as well without departing from the scope of the present invention. In addition, although eUICC driver 129 and eUICC 107 are depicted in Figure 1e and Figure 1b as separate elements, programs, and/or processes for a module 101, the eUICC driver 129 could be optionally

Petitioner Samsung Ex-1004, 0534

combined with an eUICC 107 such that the network application 101x can communicate directly with the eUICC 107 using the operating system 101h.

The eUICC 107 can include an eUICC profile 107d which can contain the same information used by a physical UICC 116 in Figure 1d above, including a set of network parameters, a network module identity, and a key K. In other words, the data recorded in a eUICC 107 in the form of a profile 107d can allow and support the eUICC 107 in Figure 1e to operate in an equivalent manner as a physical UICC in Figure 1d for the authentication steps illustrated in Figure 1d and Figure 1e. Although not illustrated in Figure 1e, the eUICC 107 could also perform the similar or equivalent functions of a physical UICC including (i) recording a set of network parameters equivalent to a set of network parameters 201 in Figure 2a below in order to module 101 to identify and select a wireless network 102, (ii) recording an address book with a list of phone numbers for user 113, (iii) recording a list of recent SMS messages and telephone numbers dialed, and/or (iv) recording and implementing a personal identification number (PIN) in order for a user 113 to authenticate and access the module 101 with the eUICC 107. Other functionality of an eUICC 107 for a module 101 is possible as well without departing from the scope of the present invention.

As illustrated in Figure 1e, the network application 101x in module 101 can receive a RAND 118 value from wireless network 102 in order to authenticate the module 101. The network application 101x can send the RAND 118 value to the eUICC driver 129. The eUICC 107 can read a RAND 118 value from the network application 101x using the eUICC driver 129. After receiving the exemplary RAND 118 message, in order to conduct an authentication, module 101 using an eUICC 107 could take steps to demonstrate to a wireless network 102 that the module 101 records the same pre-shared secret key K for the network module identity as recorded by a mobile network operator 104 associated with the wireless network 102. eUICC 107 can properly respond to the RAND 118 using message digest algorithms by calculating a secure hash value RES 119 using the RAND 118 and the recorded secret key K from the profile 107d. The eUICC 107 could use algorithms specified in ETSI TS 135 205 – 209, as well as

Petitioner Samsung Ex-1004, 0535

subsequent and related standards, in order for the eUICC 107 to calculate a secure hash value such as a RES 119. The calculation and processing of a RES 119 using a RAND 118 and a secret key K for an eUICC 107 is also depicted and described in connection with steps 306 and 311 of Figure 3. Other possibilities exist as well for an eUICC 107 to calculate a RES 119 value using a RAND 118 and a secret key K, without departing from the scope of the present invention. As illustrated in Figure 1e, the eUICC 107 can send the RES 119 to the eUICC driver 129, and the eUICC driver 129 can send the RES 119 to the network application 101x. The network application 101x can then send the RES 119 to the wireless network 102, and the wireless network 102 could perform a step 308a as depicted and described in connection with Figure 3 in order to authenticate the module 101 using the eUICC 107 and profile 107d.

Figure 1f

Figure 1f is a graphical illustration of an exemplary system that includes a module, a mobile network operator, and an eUICC in accordance with exemplary embodiments. System 199 in Figure 1f can include a mobile network operator 104 and a module 101. The mobile network operator 104 can communicate with the module 101 using a wireless network 102, and the wireless network 102 could comprise the radio access portion of the mobile network operator 104, such as a collection of base stations 103 using licensed radio spectrum such as, but not limited to, the 700 Mhz band for LTE, and other possibilities exist as well for the wireless network 102. The mobile network operator 104 can include a server 105 with an IP address 106a. The server 105 with MNO 104 in Figure 1f can comprise a Mobility Management Entity (MME) in LTE networks, or equivalent functionality to receive authentication requests from modules 101 with other wireless wide-area networking technology. The MME can support radio bearer activation/deactivation processes for the module 101 and authenticating the module 101 by recording an authentication vector 117, where the authentication vector 117 can be received from an HSS.

Petitioner Samsung Ex-1004, 0536

The server 105 can comprise a server as depicted and described in connection with server 105 in Figure 1k and Figure 1m of U.S. Patent Application Serial No. 14/084,141, filed November 19, 2013 in the name of John Nix, which is hereby incorporated by reference in its entirety. The IP address 106a can include a subnet prefix 106d and an interface identifier 106e. The IP address 106a can comprise an IPv6 address, where the subnet prefix 106d comprises the first 64 bits of a 128 bit IPv6 address, and the interface identifier 106e can comprise the last 64 bits of a 128 bit IPv6 address as shown in Figure 1f. Other nodes connected to the wireless network 102 can also include IPv6 addresses with different values for the subnet prefix 106d and the interface identifier 106e. A module 101 can include both a network application 101x and an eUICC 107, where a network application 101x is depicted and described in connection with Figure 1b and an eUICC 107 is depicted and described in connection with Figure 1a, Figure 1b, Figure 1c, and Figure 1e.

In an exemplary embodiment, different elements within module 101 can be associated with different IP addresses. The network application 101x can be associated with an IP address 106b and the eUICC 107 can be associated with an IP address 106c. The wireless network 102 could assign the module 101 the subnet prefix 106d used by module 101 with wireless network 102, and an operating system 101h could assign the interface identifier 106e used by the network application 101x and the eUICC 107. Other possibilities exist as well for the source of IP addresses in a system 199, but an end result can comprise the eUICC 107 having a unique IPv6 address 106c such that a server 105 such as an MME can communicate with the eUICC 107 directly by sending a packet with a RAND 118 value from server 105 address 106a to eUICC 107 address 106c.

Although not illustrated in Figure 1f, the exemplary IP addresses for server 105 and eUICC 107 can be associated with port numbers, such that server 105 can use a first port number with the IP address 106a when sending a RAND 118, and eUICC 107 could use a second port number with the IP address 106c when receiving the RAND 118. Server 105 can use a third port number when receiving a RES 119, and eUICC 107 could use a fourth port number when

Petitioner Samsung Ex-1004, 0537

sending the RES 119. The first and third port numbers could be the same value or number, and the second and fourth port numbers could be the same value or number. In an exemplary embodiment, the RAND 118 and RES 119 in system 199 can be formatted according to the UDP Lite protocol, as specified in IETF RFC 3828, which is also incorporated by reference herein. The term "UDP Lite" described in the present invention may also refer to any connectionless protocol supported on IP Network 111 and wireless network 102 where checksums may be partially disabled, thereby supporting the transfer of bit errors within a datagram.

As illustrated in Figure 1f, an eUICC 107 operating in module 101 could be an application with a unique IPv6 address 106c, and the network application 101x utilize a different IPv6 address 106b. The two IP addresses could be on the same subnet 106d used by a module 101, and the network application 101x could communicate with the eUICC 107 locally within module 101 using the two different IPv6 addresses 106b and 106c. The network application 101x could communicate with the eUICC 107 locally for exemplary "other data" depicted in Figure 1f, which could comprise the storing of an address book in the eUICC 107, reading a set of network parameters by the network application 101x from the eUICC 107 with the eUICC profile 107d, etc. In an exemplary embodiment, the eUICC 107 could communicate with the mobile network operator 104 for authentication, thus potentially bypassing the network application 101x for separate handling of RAND 118 and RES 119 values depicted in Figure 1e above. The authentication messages comprising a RAND 118 and a RES 119 could be communicated between the eUICC 107 with IP address 106c to the mobile network operator 104 with IP address 106a without the use of a network application 101x.

The eUICC 107, with an associated IP address 106c could also communicate with the eUICC subscription manager 109 by sending a packet from IP address 106c to an IP address of a server associated with the eUICC subscription manager, such as the exemplary data for a step 205 depicted and described in connection with Figure 2a and Figure 3 below. Note that the eUICC 107 with the IP address 106c can communicate with the eUICC subscription manager 109 without the wireless network 102, but rather through an IP network 111. The connectivity

Petitioner Samsung Ex-1004, 0538

for the IP network 111 could be provided by a different wireless network 102 than the wireless network 102 associated with the MNO 104. Although the use of a specific, unique IP address 106c for eUICC 107 is illustrated in Figure 1f, an eUICC 107 does not require a separate IP address 106c in other embodiments, and the eUICC 107 could share an IP address 106b with a network application 101x or other processes or elements within module 101.

Figure 2a

Figure 2a is a graphical illustration of an exemplary profile for an eUICC, including encrypted data, decryption steps, and decrypted data for the profile, in accordance with exemplary embodiments. Two exemplary forms of an eUICC profile are illustrated in Figure 2a: an encrypted eUICC profile 107c and an eUICC profile 107d. As contemplated herein, an eUICC profile, such as the exemplary eUICC profile 107c and 107d, can be similar to profiles for an eUICC contemplated in ETSI specification TS 103 383 v12.2.0 and related standards, but with differences to the currently published standards, as described below. An eUICC profile 107d can comprise the data from an encrypted eUICC profile 107c, where (i) a first portion of the data, comprising ciphertext 208a, has been decrypted, and (ii) a second portion of the encrypted eUICC profile 107c, comprising ciphertext 208b remains encrypted. Thus, an encrypted eUICC profile 107c can include a first portion, or ciphertext 208a and a second portion, or ciphertext 208b as depicted in Figure 2a. As contemplated herein, an encrypted eUICC profile 107c can be referred to as "profile 107c", and the eUICC profile 107d can be referred to as "profile 107d". Both profile 107c and profile 107d can include a profile identity 107e. Profile identity 107e can comprise a number or string such that various elements illustrated in Figure 1a can properly refer to, select, and or identity a profile 107c or profile 107d, including elements such as a mobile network operator 104, eUICC subscription manager 109, module 101, and/or an eUICC 107.

A profile 107c or profile 107d in exemplary systems herein, including systems 100, 300, and 500 can comprise several different possible embodiments. The profiles could be recorded in

Petitioner Samsung Ex-1004, 0539

a file or data set, and stored in nonvolatile memory associated with an eUICC 107, such as, but not limited to, a flash memory 101w. 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. An application layer protocol such as transport layer security (TLS) and additional ciphering at the data-link layer could be utilized as well, in addition to sending and receiving the data for a profile 107c as ciphertext 208a and 208b. The exemplary forms for a profile 107c and 107d in Figure 2a can represent data for a file recorded in a module, such as, but not limited to, (i) storing in a volatile memory 101e when the profiles 107c or 107d are being processed or accessed by a CPU 101b, or (ii) storing in an nonvolatile memory such as flash memory 101w when the profile 107c and 107d are stored long term, including times when a battery 101k may be removed from module 101.

Note that profile 107c with at least two distinct portions, comprising ciphertext 208a and ciphertext 208b, could be recorded in separate segments or in distinct location within module 101 or with an eUICC subscription manager 109, and the two or multiple portions together can comprise a profile 107c. In other words, the portions of ciphertext 208a and 208b (and other data in a profile 107c or profile 107d) can be recorded in different locations while comprising a profile 107c. Other possibilities exist as well for the structure and recording of the exemplary data for a profile 107c and 107d without departing from the scope of the present invention. Although the label "Stored w/ Subscription Manager 109" is depicted with an encrypted eUICC profile 107c, the encrypted eUICC profile 107c can also be stored as the format depicted in Figure 2a within a module 101 or an eUICC 107, until at least a step 206 is performed to decrypt the first ciphertext 208a, as described in this Figure 2a and Figure 3 below.

A first portion of profile 107c can include ciphertext 208a, where ciphertext 208a can include a set of network parameters 201, a first network module identity 202, and a first key K 203. Ciphertext 208a can include these elements in a ciphered string or file, such that a third party would not feasibly be able to ready the plaintext within ciphertext 208a without a key such as eUICC profile key 107b. Ciphertext 208a can comprise the set of network parameters 201,

Petitioner Samsung Ex-1004, 0540

the first network module identity 202, and the first key K 203 as plaintext ciphered with a eUICC profile key 107b, as depicted and described in connection with Figure 2b below. The set of network parameters 201 could comprise a list of values and settings for a module 101 to utilize in connecting with a mobile network operator 104. The set of network parameters 201 could include a list of numbers or strings for values such as (i) allowed frequencies or frequency bands to scan, (ii) preferred access lists for roaming onto other wireless networks, (iii) criteria for a module 101 to select base stations 103 in idle mode, (iv) support for emergency services, (v) supported languages or character encoding, (vi) codes to search for in beacons broadcast by a wireless network 102, (vii) parameters for a radio 101z to use when connecting to a wireless network 102, (viii) names or addresses for a server 105 associated with a MNO 104 in order for a module 101 to send data, etc.

A first network module identity 202 within a ciphertext 208a in profile 107c can comprise a subscriber identity or related identifier of module 101 when connected to a MNO 104 through a wireless network 102. In an exemplary embodiment, the first network module identity 202 can comprise an international mobile subscriber identity (IMSI), a globally unique temporary identity (GTUI), a media access control (MAC) address, a temporary mobile subscriber identity (TMSI) or a similar number or string to identify a module 101 with wireless network 102. Note that a network module identity such as the first network module identity 202 can be different than a module identity 110, such that a network module identity can be assigned by a mobile network operator 104, while a module identity 110 can be assigned by manufacturer. In other words, a network module identity such as the first network module identity 202 can change over time for a module 101, while the module identity 110 can remain the same. The eUICC identity 107a can also remain the same value or number while a network module identity changes.

A first key K 203 within a ciphertext 208a in profile 107c can comprise a standards-based shared secret key K for use in wireless WAN networks based on ETSI, 3GPP, and related standards. As currently specified in ETSI/3GPP standards for LTE and LTE Advanced

Petitioner Samsung Ex-1004, 0541

networks, the shared secret key K, (i) recorded in a SIM or UICC, and a MNO 104 HSS, and (ii) described in 3GPP TS 33.401 V12.9.0 and related standards, comprises a pseudo-random number with a length of 128 bits. The length of key K for standards-based wireless networks 102 may be extended in the future. The use of shared secret key K for authentication of a module 101, and also for ciphering and data integrity, with a wireless network 102 that implements ETSI and/or 3GPP standards is also defined in the specifications ETSI TS 135 205 – 209 and related standards. Both the first key K 203 and the second key K 204 can comprise a shared secret key K as described in 3GPP TS 33.401 V12.9.0 figure 6.2-1 and related standards. A mobile network operator 104 using the function of an authentication center, possibly within a home subscriber server (HSS) can generate or process authentication vectors 117 comprising an random number (RAND), an authentication token (AUTN), a response (RES), and a sequence number using the first key K 203 recorded in a eUCC profile 107c or 107d for the first network module identity 202. Likewise, authentication vectors 117 can be generated by a HSS and sent to a MME for the second network module identity 209a with the second key K 204.

In exemplary embodiments, the first key K 203 depicted in Figure 2a is also depicted and described as operating as a standards-based shared secret key K in Figure 3 below at a step 306. Using the properties of a standards-based key K, a module 101 or an eUICC 107 can use the first key K 203 and a first random number RAND 118 received to process or calculate a first response RES 119. Step 306 with a first key K 203 can comprise an authentication for a module 101 (comprising a "mobile phone", "mobile station", or "user equipment") within standards such as 3GPP TS 33.401 V12.9.0 and related standards using a shared secret key K. As contemplated herein, the use of the term "random number" can comprise a pseudo-random number with a high degree of information entropy that may not be purely mathematically random, but can be considered a random number and referred to as a random number for the purposes herein.

In an exemplary embodiment, as described in Figure 2e and step 302a of Figure 3 below, the first key K 203 can be optionally recorded in ciphertext 208a with an additional layer of encryption, such that the first key K 203 is recorded as a ciphertext 208c within ciphertext 208a.

Petitioner Samsung Ex-1004, 0542

In other words, upon conversion of ciphertext 208a into plaintext using a profile deciphering algorithm 206, the first key K 203 can retain an additional layer of encryption as ciphertext 208c with other data in a profile 107d that may be plaintext. This optional additional layer of encryption for the first key K 203 is also depicted within the profile 107d, where ciphertext 208c optionally remains in profile 107d after the conversion of ciphertext 208a into plaintext using a step 206. As described below, the optionally additional layer of encryption for ciphertext 208c with the first key K 203 can be (i) processed into plaintext first key K 203 (ii) after a subsequent deciphering with an asymmetric ciphering algorithm 219 as illustrated in Figure 2e.

Note that the additional layer of encryption for the first key K 203, in the form of using a ciphertext 208c, can be optionally omitted and the first key K 203 could be plaintext after the conversion of the first portion of profile 107c as ciphertext 208a into plaintext in a profile 107d using a step 206. Thus, the dashed lines around the first key K 203 as a ciphertext 208c indicate the use of ciphertext 208c is optional, depending on the security requirements for an MNO 104 when distributing electronically the first key K 203. In another embodiment as described in Figure 3, the fist key K 203 can comprise a null value, such as the value for a key K in order to support emergency services if module 101 has no valid UICC, and in this case the use of additional encryption via ciphertext 208c can be omitted for a first key K 203. In a related embodiment, the first key K 203 can be omitted entirely from a profile 107c and profile 107d, and the eUICC 107 can subsequently use a null value for the first key K 203.

A second portion of profile 107c can include ciphertext 208b, where ciphertext 208b can include a second key K 204a and a second network module identity 209a. Ciphertext 208b can be ciphered with a symmetric key 127, where the ciphering and deciphering of a portion of ciphertext 208b is depicted and described in connection with Figure 2c below. In an exemplary embodiment, the second network module identity 209a can comprise an international mobile subscriber identity (IMSI), a globally unique temporary identity (GTUI), a media access control (MAC) address, or similar number or string to identify a module 101. In exemplary embodiments, the second network module identity 209a can be a different number or value than

Petitioner Samsung Ex-1004, 0543

the first network module identity 202. Although the second network module identity 209a is illustrated in Figure 2a as internal to ciphertext 208b, the second module identity 209a could be external to ciphertext 208b, such as, but not limited to, the second network module identity 209a being within a profile 107c or profile 107d and external to ciphertext 208b. In other words, in exemplary embodiments, the second network module identity 209a may optionally not be ciphered with the symmetric key 127, while the second key K 204a can be ciphered with the symmetric key 127. As contemplated herein, the term second network identity 209a comprises an encrypted second network identity 209a, where the second network identity 209 is the plaintext version of the encrypted second network identity 209a. Likewise, the term second key K 204a comprises an encrypted second key K 204a, where the second key K 204 is the plaintext version of the encrypted second key K 204a.

In another exemplary embodiment, the second network module identity 209 can comprise the same number or value as the first network module identity 202, or the second network module identity 209 can be optionally omitted. In this case, if (A) the second network module identity 209 comprises the same number or value as the first network module identity 202, or the second network module identity 209 is optionally omitted, then (B) the mobile network operator 104 can preferably support the use of two different shared secret keys K (i.e. first key K 203 and second key K 204) for the same network module identity 202. However, given the current functionality of an HSS and related infrastructure for wireless networks 102, the use of two different network module identities (i.e. the first network module identity 202 and the second network module identity 209) with two different shared secret keys K (i.e. first key K 203 and second key K 204, respectively) may be more compatible or suitable for deployed and operational HSS infrastructure.

A second key K 204a (as an encrypted form of plaintext second key K 204) within a ciphertext 208b in profile 107c can comprise a standards-based shared secret key K for use in wireless WAN networks based on ETSI, 3GPP, and related standards. The use of a second key K 204a (in an unencrypted form of second key K 204) can be equivalent to a first key k 203, but

Petitioner Samsung Ex-1004, 0544

comprise a different random number. The second key K 204 can comprise a random number that is 128 bits in length in order to support 4G networks such as LTE that are widely deployed in 2013, although the length of either first key K 203 or second key K 204 may be a longer number in the future, such an exemplary 256 bits and other possibilities exist as well for the key length. A second key K 204 can also be used with standards-based authentication with a wireless network 102, where the second key K 204 in Figure 2a is also depicted and described as operating as a standards-based shared secret key K in Figure 3 below at a step 311.

The list of exemplary data for encrypted eUICC profile 107c and an eUICC profile 107d comprises an exemplary set, and the profiles could also include additional data to the exemplary data illustrated in Figure 2a. The additional data for a profile 107c or 107d could include (i) a set of cryptographic parameters for eUICC 107, (ii) a set of cryptographic algorithms, such as the exemplary cryptographic algorithms described within ETSI TS 135 205 – 209 and related standards, (iii) a name or address for an eUICC subscription manager 109 associated with the profile 107c, (iv) a name or address for a server 105 associated with a mobile network operator 104, (v) a digital signature of the profile 107d processed with a private key from either eUICC subscription manager 109 or MNO 104, (vi) a date or timestamp for processing the profile 107c or 107d, (vii) and similar or related values for a module 101 and/or eUICC 107 to utilize the profiles. This exemplary additional data which is not depicted in Figure 2a could be included within or external to any of ciphertext 208a and ciphertext 208b.

Note that the profile identity 107e may preferably be external to ciphertext 208a and ciphertext 208b, in order that module 101 and/or eUICC 107 can take steps to identify a profile 107c or 107d. In addition, although a single profile 107c and profile 107d are illustrated in Figure 2a, a module 101 and/or an eUICC 107 could include a plurality of profiles 107c and/or 107d, where each of the plurality of profiles could comprise different data associated with different wireless networks 102. In an exemplary embodiment, more than one profile 107c or profile 107d could be associated with the same wireless network 102, such that a mobile network operator 104 can prefer for the same module 101 to utilize different network access credentials

Petitioner Samsung Ex-1004, 0545

over time, such that the same module 101 could use a different key K and a different network module identity with the same wireless network 102 or mobile network operator 104 over time. Different profiles 107c or 107d can also be identified by the use of a different profile identity 107e. Each profile 107c can be associated with an eUICC profile key 107b as an encryption key (shown in Figure 2b below), although multiple profiles 107c could also share the same eUICC profile key 107b.

A module 101 can receive a profile 107c using a step 205. A profile 107c can be recorded with an eUICC subscription manager 109 before being received by a module 101. As depicted in Figure 2a, a module 101 can receive the profile 107c at a step 205 using the IP network 111. The use of a step 205 by a module 101 is depicted and described in connection with Figure 3 below. The module 101 can receive the profile 107c using a network that is different than wireless network 102 associated with the network access credentials comprising the first key K 203 and the first network module identity 202. In an exemplary embodiment, module 101 can receive the profile 107c in a step 205 using an initial wireless network 102, where module 101 connects with and authenticates with the initial wireless network 102 using an initial eUICC profile 107d different than the eUICC profile 107d depicted in Figure 2a. Or, module 101 could receive a profile 107c using a wireless LAN network or a wired connection via a physical interface 101a such as a USB interface 101v. In another exemplary embodiment, module 101 can receive the profile 107c from a manufacturer, distributor, end user, or technician taking steps to load the profile 107c into a nonvolatile memory within module 101 or eUICC 107. Upon receipt of a profile 107c by module 101, the module 101 can record or store the profile 107c with an eUICC 107.

A module 101 can use an eUICC 107 to decrypt the first portion or ciphertext 208a in a profile 107c using a step 206. Before a step 206, a module 101 can receive an eUICC profile key 107b, where the eUICC profile key 107b can comprise a symmetric ciphering key. The use of a step 206 by module 101 and/or eUICC 107 is also depicted and described in connection with Figure 2b and Figure 3 below. Note that both eUICC subscription manager 109 and module 101

Petitioner Samsung Ex-1004, 0546

can record profile 107c with ciphertext 208a for a period of time, and the step 206 can be taken (i) after receiving eUICC profile key 107b and (ii) before module 101 authenticates with a wireless network 102 using the eUICC profile 107c. A step 206 can covert the ciphertext 208a into plaintext, such that an eUICC 107 can read the values in order to authenticate with a wireless network 102 using the first key K 203. By encrypting the first network module identity 202 and the first key K 203, these network access credentials can remain secure, such that a profile 107c can be transferred in normal physical media (such as disks, drives, or files transferred electronically) or in communications channels outside the control of a mobile network operator 104 and/or eUICC subscription manager 109.

As depicted in Figure 2a, after a step 206 to convert profile 107c into profile 107d, where the ciphertext 208a is decrypted using the eUICC profile key 107b, the ciphertext 208b with the second key K 204a can remain encrypted and thus the second key K can continue to remain secure within a profile 107d. In addition, although ciphertext 208b is depicted in a profile 107c as external to, or separate from, ciphertext 208a, ciphertext 208b could optionally be included within ciphertext 208a. In this case, where ciphertext 208b is within ciphertext 208a for a profile 107c, the result of a step 206 to generate a profile 107d can remain the same, where the ciphertext 208a can be decrypted by step 206 and ciphertext 208b remains encrypted in the resulting profile 107d from a step 206.

A module 101 can use an eUICC 107 to decrypt the second portion or ciphertext 208b in a profile 107d using a step 207. Before a step 207, a module 101 can take the previous steps 205 and 206 in order to record a profile 107d with an eUICC 107. Before a step 207, module 101 can receive a symmetric key 127, where the symmetric key 127 can comprise a symmetric ciphering key. In exemplary embodiments, module 101 can receive the symmetric key 127 from a mobile network operator 104 after a user associated with module 101 performs a separate authentication step 308b as depicted and described in connection with Figure 3 and Figure 4 below. By a mobile network operator 104 only sending symmetric key 127 after the second authentication step 308b, the second key K 204 can remain secured, while a user is allowed to access the

Petitioner Samsung Ex-1004, 0547

wireless network 102 (perhaps temporarily or with other constraints such as limiting access to the Internet but allowing emergency calls) using the first key K 203.

In this manner and by using a second, separate authentication step 308b before sending symmetric key 127, the decryption of network access credentials such as the second key K 204 can remain in the control of a mobile network operator 104, thereby increasing the security of exemplary systems illustrated herein, such as systems 100, 300, and 500. By ciphering the second key K 204 with symmetric key 127, security over conventional technology for an eUICC can be increased for both a user and a mobile network operator. With conventional technology for an eUICC, where only the first key K 203 is used for authentication and ciphering of data between module 101 and wireless network 102, the decryption of the first key K 203 can be outside the control of a mobile network operator 104. With conventional technology contemplated for an eUICC, an end user outside the control or a contractual relationship with mobile network operator 104, including possibly fraudulent users or imposters of valid users, could (i) take steps to obtain a plaintext first key K 203 and associated plaintext first network module identity 202 and (ii) use the credentials to fraudulently access the wireless network 102. In contrast and as contemplated herein, the symmetric key 127 to decrypt the second key K 204a can preferably be only made available to users who authenticate with mobile network operator using a step 308b as described below (or an equivalent step or related commercial arrangements between a user and a mobile network operator 104).

In exemplary embodiments, use of two sets of network access credentials comprising at least the first key K 203 and the second key K 204 allows a user with an eUICC profile 107c to connect to the wireless network 102 using the first key K 203, such that the module 101 can have connectivity to the mobile network operator 104 via the wireless network 102 (and also IP network 111) in order to conduct separate authentication steps 308b. The security steps for a mobile network operator 104 to control the decryption of the first key K 203 can be lowered (thus making the distribution of profile 107c simpler, less costly, and less complex), while a

Petitioner Samsung Ex-1004, 0548

mobile network operator 104 can retain full control over the decryption of the second key K 204a into a usable second key K 204 associated with the second network module identity 209.

The use of a step 207 by module 101 with an eUICC is also depicted and described in connection with Figure 2c and Figure 3 below. A module 101 can record profile 107d with ciphertext 208b for a period of time, and the step 207 can be taken (i) after recording profile 107d, and (ii) before module 101 authenticates with a wireless network 102 using the second key K 204. A step 207 can covert the ciphertext 208b into plaintext, such that an eUICC 107 can read the values in order to authenticate with a wireless network 102 using the second key K 204.

A step 207 can convert the encrypted second key K 204a into a plaintext key K 204. As illustrated in Figure 2a, a step 207 can also convert the encrypted network module identity 209a into a plaintext network module identity 209 as well. As discussed above in this Figure 2a, the network module 209 can be optionally omitted from a step 207, such that the plaintext network module identity 209 could be recorded in a profile 107d, and the plaintext network module identity 209 could be included in the first portion, or ciphertext 208a, in a profile 107c. In another embodiment, the second network module identity 209 can be received by module 101 from wireless network 102 after the module authenticates using the first key K 203. Although not illustrated in Figure 2a, an eUICC 107 can continue to record the plaintext network module identity 209 and plaintext second key K 204 in an eUICC profile after the second key K 204 is decrypted using the symmetric key 127. The module 101 can record the second key K 204 in a protected memory address within ROM 101c or nonvolatile memory 101w.

For embodiments where the first key K 203 is recorded within a ciphertext 208c in a profile 107d after a step 206, the first key K 203 can be converted from ciphertext 208c into a plaintext first key K 203 using a key deciphering step 217 as depicted and described in connection with Figure 2e below. The key deciphering step 217 could use an asymmetric ciphering algorithm 219 with input of (i) ciphertext 208c and (ii) the eUICC private key 215 in order to output the plaintext first key K 203. As described above, the use of a ciphertext 208c can be optionally omitted, and the first key K 203 could be recorded as plaintext in a profile

Petitioner Samsung Ex-1004, 0549

107d. In this case, a step 217 for data in profile 107d can be omitted, and thus step 217 with ciphertext 209c is depicted in Figure 2a with a dashed line.

Although the first key K 203 and the second key K 204a are depicted in Figure 2a as recorded within an eUICC profile 107c or eUICC profile 107d, the first key K 203 and the second key K 204a can be (i) recorded in a nonvolatile memory of module 101, such as, but not limited to, a flash memory 101w, and (ii) without the use of an eUICC 107. In other words, embodiments contemplated herein can be used without an eUICC 107, such that (i) a module 101 can use a first key K 203 to authenticated with a wireless network 102, (ii) after authentication with the first key K 203, the module can receive a symmetric key 127 to decrypt the second key K 204a into second key K 204, and (iii) the module can authenticate with the wireless network 102 using the second key K 204. In other words, an eUICC 107 can be omitted and a module 101 can perform the same steps for (i) receiving encrypted network access credentials and (ii) decrypting the encrypted network access credentials without requiring the use of an eUICC 107.

In embodiments where a module 101 does not include an eUICC 107, the module can record the first key K 203 and the encrypted second key K 204a in a file or memory address without requiring the use of a profile 107c and 107d. For example, the first key K 203 could be recorded in a regular, physical UICC, and the second key K 204a could also be recorded in a regular, physical UICC as well. The regular, physical UICC could (i) receive the symmetric key 127 and decrypt the second key K 204a, and (ii) subsequently record the decrypted second key K 204. The module 101 and UICC could use the decrypted second key K 204 to authenticate with the wireless network 102 where the first key K 203 was previously used. Other possibilities exist as well for a module 101 to (i) use a first key K 203 and an encrypted second key K 204a without departing from the scope of the present invention.

Figure 2b

Figure 2b is a graphical illustration for ciphering and deciphering a profile using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments.

Petitioner Samsung Ex-1004, 0550

An eUICC profile 107d can be (i) ciphered using a profile ciphering algorithm 210 and (ii) deciphered with a profile deciphering algorithm 206. Both the profile ciphering algorithm 210 and the profile deciphering algorithm 206 can include a symmetric ciphering algorithm 211 and the use of an eUICC profile key 107b. An eUICC subscription manager 109, or another node outside a module 101 as illustrated in Figure 1a, can use a profile ciphering algorithm 210 to encrypt an eUICC profile 107c. The processing and computational steps for performing a profile ciphering algorithm 210 could be conducted on a server associated with the eUICC subscription manager 109. The server associated with the eUICC subscription manager 109 can be similar to a server 105 illustrated in Figure 1a, with the difference being the server associated with the eUICC subscription manager 109 can be co-located, associated with, or under the operational control of an eUICC subscription manager 109. Data for an eUICC profile 107d used in a profile ciphering algorithm 210 can comprise the exemplary data illustrated for a profile 107d in Figure 2a above, and an eUICC subscription manager 109 could receive the data for the profile 107d from a mobile network operator 104. The mobile network operator 104 could process, generate, or derive the exemplary values in a profile 107d that can include the network parameters 201, the first network module identity 202, the first key K 203, and the ciphertext 208b. As contemplated herein, the MNO 104 could also function as a eUICC subscription manager 109, and thus in embodiments the profile 107d could be generated by a MNO 104 as well.

Symmetric ciphering algorithm 211 in a profile ciphering algorithm 210 can utilize a key such as an eUICC profile key 107b to encrypt or cipher data. Examples of symmetric ciphers for a symmetric ciphering algorithm 210 include (i) an Advanced Encryption Standard (AES) cipher, as specified in Federal Information Processing Standards (FIPS) Publication 197, and (ii) Triple Data Encryption Standard (Triple DES), as described in NIST Special Publication 800-67 Revision 1, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (Revised January 2012)". Other symmetric ciphers and/or combinations of symmetric ciphers can be utilized as well for a symmetric ciphering algorithm 210 without departing from the scope of the present invention. In general, a symmetric ciphering algorithm 211 in a profile ciphering

Petitioner Samsung Ex-1004, 0551

algorithm 210 (and other steps for symmetric ciphering contemplated herein) can accept input of plaintext and a key, and using the two sets of input data, the symmetric ciphering algorithm 211 can perform multiple rounds of mixing, substituting, rotating, and/or perform XOR functions with the input in order to produce a ciphertext output. Although not illustrated in Figure 2b and Figure 2c, a set of cryptographic parameters can also be input into symmetric ciphering algorithms 211 in order to specify parameters or configurations of the symmetric ciphering algorithm 211, such as, but not limited to, the selection of 128, 192, or 256 bits with AES.

A cipher key used with a symmetric ciphering algorithm 211, such as, but not limited to, the exemplary eUICC profile key 107b can comprise a random or pseudo-random number, with an appropriate length or number of bits for the symmetric ciphering algorithm 211. The exemplary eUICC profile key 107b for use in a profile ciphering algorithm 210 could be shared between an eUICC subscription manager 109 and an eUICC 107 in a module 101 in several different ways. The eUICC profile key 107b could be recorded in or with the eUICC 107 upon manufacturing of module 101. The eUICC profile key 107b could be securely received by a module 101 using a wireless network 102 from the eUICC subscription manager 109 before the module 101 performs a step that includes a profile deciphering algorithm 206. An encrypted eUICC profile key 107b could be received by module 101 and then decrypted by module 101 using an asymmetric ciphering algorithm 219 as depicted and described in connection with Figure 2e below. The eUICC profile key 107b could also be derived by a module 101 and an eUICC subscription manager 109 (or another server performing the steps in a profile ciphering algorithm 210) using a key exchange such as, but not limited to, a Diffie-Hellman key exchange or an Elliptic Curve Diffie-Hellman key exchange.

Other possibilities exist as well for a module 101 and an eUICC subscription manager 109 (or another server performing the steps in a profile ciphering algorithm 210) to securely share a eUICC profile key 107b without departing from the scope of the present invention. In addition, although a single eUICC profile key 107b is illustrated in Figure 2b, an eUICC subscription manager 109 and an eUICC 107 could use multiple eUICC profile keys 107b,

Petitioner Samsung Ex-1004, 0552

including embodiments where a first encrypted eUICC profile 107c is associated with a first eUICC profile key 107b and a second encrypted eUICC profile 107c is associated with a second eUICC profile key 107b. Further, each encrypted eUICC profile 107c could be uniquely associated with a different eUICC profile key 107b. Each of the different eUICC profile keys 107b could be securely transferred between the eUICC 107 and the eUICC subscription manager 109 using either (i) asymmetric ciphering 219 as illustrated in Figure 2e below, or (ii) a key exchange, as depicted and described in connection with step 303 of Figure 3 below.

With a profile ciphering algorithm 210, the symmetric ciphering algorithm 211 can accept input of (i) the eUICC profile key 107b, and (ii) and an eUICC profile 107d plus an optional security token 212, in order to output an encrypted eUICC profile 107c. The encrypted eUICC profile 107c can be reasonably secured, such that deciphering the profile 107c without the eUICC profile key 107b would be infeasible. After ciphering with a symmetric ciphering algorithm 211, deciphering the ciphertext without the cipher key would require extensive dedicated computational resources such as hundreds of servers or more for many years or longer. The optional security token 212 can include a string or number in order to enhance the security of the ciphertext output by a symmetric ciphering algorithm 211. The optional security token 211 could comprise a random number or other value, such that the input and output of a symmetric ciphering algorithm 211 is properly padded, where the length of input and output are appropriate for the symmetric ciphering algorithm.

Although the input of eUICC profile 107d is depicted in Figure 2b with a label of "plaintext", the eUICC profile 107d in a profile ciphering algorithm 210, the "plaintext" eUICC profile 107d can include encrypted data such as ciphertext 208b, where ciphertext 208b can include encrypted data ciphered with a different key than eUICC profile key 107b. In other words, a profile 107c can include multiple layers of ciphering, where different layers use different cipher keys, and the exemplary a profile ciphering algorithm 210 with the eUICC profile key 107b can be used to encrypt the ciphertext 208a illustrated in Figure 2a above. As

Petitioner Samsung Ex-1004, 0553

noted above with Figure 2a, ciphertext 208b can be either (i) included inside ciphertext 208a, or (ii) remain external to ciphertext 208a.

After a server associated with an eUICC subscription manager 109 generates the output of an encrypted profile 107c from a profile ciphering algorithm 210, the encrypted profile 107c can be transferred to module 101 through either unsecured channels, or channels that are not under the full control of an eUICC subscription manager 109 or a mobile network operator 104 associated with the profile 107c. The module 101 can receive the profile 107c through an IP network 111, including using the public Internet, or a manufacturer, distributor, technician, or end user could load the profile 107c into the module (such as, but not limited to, using a USB interface 101v). This initial loading of profile 107c by a manufacturer, distributor, technician, or end user may be required for the first use or startup of a module 101, but then module 101 may preferably receive additional or subsequent profiles 107c at later times using IP network 111 and other automated, electronic means using a network including a wireless network 102.

A module 101 or an eUICC 107 within module 101 can process the encrypted profile 107c using a profile deciphering algorithm 206 as depicted in Figure 2b and also depicted and described in Figure 2a. Note that the module 101 or eUICC 107 could record the encrypted profile 107c for a period of time, and take the steps to decrypt the profile 107c in a profile deciphering algorithm 206 after receiving the eUICC profile key 107b associated with the profile 107c. Or the eUICC profile key 107b could be recorded in a module 101 or with an eUICC 107 before profile 107c is received, and the steps for a profile deciphering algorithm 206 could be performed after the receipt of an instruction from an eUICC subscription manager 109 or at a specified time or under specified conditions (such as a module 101 needing or preferring to connect to a wireless network 102 for the first time). An exemplary use and sequence for a profile deciphering algorithm 206 is depicted and described in connection with Figure 3 below. Other possibilities exist as well for the time that a module 101 or an eUICC 107 can process a profile deciphering algorithm 206 without departing from the scope of the present invention. As

Petitioner Samsung Ex-1004, 0554

contemplated herein, the use of the term "step 206" can refer to the use of a profile deciphering algorithm 206, and a "step 207" can refer to the use of a key K deciphering algorithm 207, etc.

A profile deciphering algorithm 206 can include a symmetric ciphering algorithm 211. The symmetric ciphering algorithm 211 can be equivalent to or the same as the symmetric ciphering algorithm 211 in a profile ciphering algorithm 210 operated by a server and as described above. The symmetric ciphering algorithm 211 can accept input of the eUICC profile key 107b as a cipher key. The module 101 or eUICC 107 could securely receive the eUICC profile key 107b using the steps described above in connection with a profile ciphering algorithm 210. An exemplary transfer or key exchange for module 101 to receive eUICC profile key 107b is also described in Figure 2e and Figure 3 below. The symmetric ciphering algorithm 211 in a profile deciphering algorithm 206 can also accept input of the encrypted eUICC profile 107c, which could comprise ciphertext 208a.

The symmetric ciphering algorithm 211 in a profile deciphering algorithm 206 can decrypt the ciphertext 208a in order to output the profile 107d, where the ciphertext 208a is converted to plaintext. Ciphertext 208b in a profile 107c can remain encrypted using the symmetric key 127 after a profile deciphering algorithm 206. In other words, the profile deciphering algorithm 206 can convert a portion of the profile 107c into plaintext, where the portion comprises ciphertext 208a. As depicted in Figure 2a above, exemplary plaintext in a profile 107d resulting from a profile deciphering algorithm 206 can include a first network module identity 202 and the first key K 203. The resulting plaintext from a profile deciphering algorithm 206 can also optionally include a security token 212. Security token 212 could comprise the string or value also optionally input into the symmetric ciphering algorithm 211 in a profile ciphering algorithm 210. The security token 212 can include a padding value to make the length of the security token 212 and profile 107d a desired value for the symmetric ciphering algorithm 211 or other requirements such as making the encrypted profile 107c a desired length.

Figure 2c

Petitioner Samsung Ex-1004, 0555

Figure 2c is a graphical illustration for ciphering and deciphering a key K using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments. A second key K 204a can be (i) ciphered using a key K ciphering algorithm 213 and (ii) deciphered with a key K deciphering algorithm 207. Both the key K ciphering algorithm 213 and the key K deciphering algorithm 207 can include a symmetric ciphering algorithm 211 and the use of a symmetric key 127. A mobile network operator 104 can use a key K ciphering algorithm 213 to encrypt the second key K 204a. The processing and computational steps for performing a key K ciphering algorithm 213 could be conducted on a server associated with the mobile network operator 104 such as a server 105 illustrated in Figure 1a. Other possibilities exist as well for the location or association of a computer to process a key K ciphering algorithm 213 without departing from the scope of the present invention.

A key K ciphering algorithm 213 can include a symmetric ciphering algorithm 211. The symmetric ciphering algorithm 211 can similar to the symmetric ciphering algorithm 211 as depicted and described in connection with Figure 2b above. A symmetric ciphering algorithm 211 can include a collection of different symmetric ciphers, such that a first symmetric cipher comprising the AES cipher could be used in a Figure 2b, while a different symmetric cipher could be used in a Figure 2c. Or, the same algorithm within symmetric ciphering algorithm 211 can be used in a symmetric ciphering algorithm 211 in Figure 2b and Figure 2c. The symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 can accept input of a symmetric key 127 and plaintext in the form of a second key K 204. The second key K 204 could represent a random number, such as, but not limited to, an exemplary 128 random number currently used as a shared secret key K in standard LTE networks and a different length for second key K 204 could be used as well. The second key K 204 could be derived or processed by the function of an authentication center with a home subscriber server (HSS). Although not illustrated in Figure 2c, but as illustrated in Figure 2a, the plaintext as input into a symmetric ciphering algorithm 211 can also include a second network module identity 209. The input into a symmetric ciphering algorithm 211 for a key K ciphering algorithm 213 can also include a number, value, or string for

Petitioner Samsung Ex-1004, 0556

a security token 212. The use of a security token 212 is depicted and described in connection with Figure 2b above. Thus, a mobile network operator 104 could also use a key K ciphering algorithm 213 to encrypt other data in addition to a second key K 204.

The symmetric key 127 input into a symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 can comprise a random number processed or generated by a server 105, where the server 105 is associated with a mobile network operator 104. The server processing or deriving a symmetric key 127 can comprise or be associated with an HSS for an LTE or LTE advanced network. As illustrated in Figure 2c, the symmetric key 127 can comprise a cipher key for the symmetric ciphering algorithm 211. A cipher key used with a symmetric ciphering algorithm 211, such as, but not limited to, the exemplary symmetric key 127 can comprise a random or pseudo-random number, with an appropriate length or number of bits for the symmetric ciphering algorithm 211 in a key K ciphering algorithm 213. Using the input of the symmetric key 127 and the plaintext second key K 204, the symmetric ciphering algorithm 211 could output an encrypted second key K 204a. As illustrated in Figure 2c and Figure 2a above, the encrypted second key K 204a could be included in ciphertext 208b. The symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 may also optionally include a security token 212, as illustrated.

After processing the ciphertext 208b, the mobile network operator 104 can either (i) include the ciphertext 208b in a profile 107d and send the profile 107d to an eUICC subscription manager 109, or (ii) send the ciphertext 208b directly an eUICC subscription manager 109 for the eUICC subscription manager 109 to include the ciphertext 208b in a profile 107d. Ciphertext 208b could be recorded in or with an eUICC profile 107d, where an eUICC subscription manager 109, or another server associated with an eUICC subscription manager 109 can subsequently encrypt the eUICC profile 107d using a profile ciphering algorithm 210 depicted and described in connection with Figure 2b above. Other possibilities exist as well for the timing an sequence of steps for transferring and recording a ciphertext 208b output from a key K ciphering algorithm 213 without departing from the scope of the present invention. After profile

Petitioner Samsung Ex-1004, 0557

107d with ciphertext 208b has been created, the profile 107d can be ciphered with a profile ciphering algorithm 210 to create an encrypted profile 107c, as illustrated in Figure 2b above.

The exemplary symmetric key 127 for use in a key K ciphering algorithm 213 could be shared between a module 101 with an eUICC 107 and the mobile network operator 104 in several different ways. The symmetric key 127 could be sent from the mobile network operator 104 (possibly using a server 105) to a module 101 after (i) the module properly authenticates with the mobile network operator 104 and/or a wireless network 102 associated with the MNO 104 using the first key K 203, and (ii) a user 113 associated with the module 101 authenticates with the MNO 104. Note that if MNO 104 sends the symmetric key 127 to module 101 after module 101 uses the first key K 203 to authenticate, then the ciphering or encryption of the channel used to send the symmetric key K 127 can be within the control of MNO 104 (whereas the communications channel and ciphering keys used to send encrypted profile 107c may be outside the control of MNO 104). The symmetric key K 127 could also be derived by a module 101 and an MNO 104 using a key exchange, where the symmetric key K 127 could be derived using a RAND 118 value received by the module 101 after authenticating with the first key K 203, where the module 101 and/or eUICC 107 derives the symmetric key K 127 using the RAND 118 value and the first key K 203. Other possibilities exist as well for a module 101 and a mobile network operator 104 to securely share a symmetric key 127 without departing from the scope of the present invention.

A module 101 or an eUICC 107 within module 101 can process the ciphertext 208b using a key K deciphering algorithm 207 as depicted in Figure 2c. Note that the module 101 or eUICC 107 could record the ciphertext 208b for a period of time, and take the steps to decrypt the ciphertext 208b with a key K deciphering algorithm 207 after receiving or deriving the symmetric key 127. Or the symmetric key 127 could be recorded in a module 101 or with an eUICC 107 before ciphertext 208b is decrypted, and the steps for a key K deciphering algorithm 207 could be performed after the receipt of an instruction from the MNO 104 to decrypt the second key K 204a. An exemplary use and sequence for a key K deciphering algorithm 207 is

Petitioner Samsung Ex-1004, 0558

depicted and described in connection with Figure 3 below. Other possibilities exist as well for the time that a module 101 or an eUICC 107 can process a key K deciphering algorithm 207 without departing from the scope of the present invention.

A key K deciphering algorithm 207 can include a symmetric ciphering algorithm 211. The symmetric ciphering algorithm 211 can be equivalent to or the same as the symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 performed by an MNO 104 and as described in this Figure 2c above. The symmetric ciphering algorithm 211 can accept input of the symmetric key 127 as a cipher key. The module 101 or eUICC 107 could securely receive or derived the symmetric key 127 using the steps described above in connection with a key K ciphering algorithm 213. The symmetric ciphering algorithm 211 in a key K deciphering algorithm 207 can also accept input of the encrypted key K 204a, which could comprise ciphertext 208b. Additional data, such as, but not limited to a second module identity 209a could optionally be included within ciphertext 208b.

The symmetric ciphering algorithm 211 in a key K deciphering algorithm 207 can decrypt the ciphertext 208b in order to output the plaintext second key K 204, such that the ciphertext 208b is converted to plaintext. The resulting plaintext from a key K deciphering algorithm 207 can also optionally include a security token 212. Security token 212 could comprise the string or value also optionally input into the symmetric ciphering algorithm 211 in a key K ciphering algorithm 213. The security token 212 can include a padding value to make the length of the security token 212 and second key K 204a a desired value for the symmetric ciphering algorithm 211 or other requirements such as making the ciphertext 208b a desired length.

Figure 2d

Figure 2d is a graphical illustration of a public key and a private key for an eUICC, in accordance with exemplary embodiments. An eUICC 107 within a module 101 can include an eUICC private key 215, which can be associated with an eUICC public key 214. The eUICC

Petitioner Samsung Ex-1004, 0559

private key 215 and eUICC public key 214 can comprise a public key infrastructure (PKI) key pair for eUICC 107. The eUICC subscription manager 109 can record the eUICC public key 214 along with an eUICC identity 107a, such that the eUICC subscription manager 109 can properly associate one of a plurality of eUICC public keys 214 with the proper eUICC 107. Although not illustrated in Figure 2d, an eUICC subscription manager 109 could record the eUICC public key 214 and an associated eUICC identity 107a in a database. The use of an eUICC ID 107a is also depicted and described in connection with Figure 3 below.

The eUICC private key 215 and eUICC public key 214 could be processed using RSA algorithms or elliptic curve cryptography (ECC) algorithms, and other possibilities exist as well for the format of PKI keys without departing from the scope of the present invention. An ECC key length of 283 bits provides security similar to an RSA key length of approximately 2048 bits, and in an exemplary embodiment the eUICC key pair can utilize an ECC algorithm, although an RSA algorithm or other algorithms for PKI keys could also be utilized by an eUICC 107. The eUICC private key 215 can be processed or derived using a random number. eUICC public key 214 can comprise a key recorded in an X.509 certificate that also includes a module identity 110 and/or eUICC identity 107a, although the use of an X.509 certificate with an eUICC public key 214 is not required. The eUICC public key 214 in the form of an X.509 certificate can optionally be signed by a certificate authority. The keys can support standards such as, but not limited to, the International Organization for Standardization (ISO) ISO/IEC 9594 series of standards (herein incorporated by reference) and the Internet Engineering Task Force (IETF) RFC 5280 titled "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (herein incorporated by reference), including future updates to these standards.

Several possibilities exist for the source of an eUICC private key 215 and eUICC public key 214. The eUICC private key 215 and eUICC public key 214 be generated using standard software tools such as, but not limited to, Openssl, libmcrypt, and/or and Crypto++, and other tools to generate public and private keys exist as well. Public and private keys as contemplated

Petitioner Samsung Ex-1004, 0560

herein could be recorded in a file such as, but not limited to, a *.pem file (Privacy-enhanced Electronic Mail), a file formatted according to Basic Encoding Rules (BER), Canonical Encoding Rules (CER), or Distinguished Encoding Rules (DER), or as text or binary file. Other formats for public and private keys may be utilized as well, including proprietary formats. A module 101 could derive the PKI key pair using a set of cryptographic algorithms and a key pair generation algorithm. 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.

A manufacturer of module 101 or an eUICC subscription manager 109 could also derive the eUICC private key 215 and eUICC public key 214 in a server, and load the eUICC private key 215 into a nonvolatile memory of module 101 before distribution of the module 101. The manufacturer of module 101 could send or make available the eUICC public key 214 to an eUICC subscription manager 109. The module 101 could send record the eUICC public key 214 and 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.

Although Figure 2d illustrates an eUICC private key 215 and eUICC public key 214, a module 101 could use a PKI key pair associated with module 101 instead of being associated with an eUICC 107 in order to use an asymmetric ciphering algorithm as depicted in Figure 2e below. In other words, a module 101 and an eUICC subscription manager 109 could use a module private key 112a and a module public key 112b in order to obtain the same functionality of an eUICC private key 215 and an eUICC public key 214. A module private key 112a and a module public key 112b for a module 101 could have the same properties and characteristics for an eUICC private key 215 and an eUICC public key 214 as described herein. Other possibilities exist as well for the source or use of a PKI key pair for an eUICC private key 215 and eUICC public key 214 without departing from the scope of the present invention.

Petitioner Samsung Ex-1004, 0561

In exemplary embodiments, both the eUICC subscription manager 109 and the eUICC 107 can include a set of digital signature algorithms 221, in order to sign and verify messages between (i) an eUICC 107 and eUICC subscription manager 109, and (ii) eUICC subscription manger 109 and MNO 104. Digital signature algorithms 221 can also verify signatures such as, but not limited to, comparing that (i) a first secure hash value received from a sending node matches (ii) a second secure hash value calculated using a recorded public key associated with the sending node. Digital signature algorithms 221 can utilize algorithms in National Institute of Standards (NIST) "FIPS 186-4: Digital Signature Standard", or IETF RFC 6979 titled "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)". The use of ECDSA algorithm within a set of digital signature algorithms 221 may be preferred if keys such as, but not limited to, eUICC private key 215 and eUICC public key 214 are based on elliptic curve cryptography. Digital signature algorithms 221 could also include an RSA digital signature algorithm (DSA) for use with RSA-based public and private keys. Other PKI standards or proprietary techniques for securely generating digital signatures and verifying digital signatures may be utilized as well in digital signature algorithms 221. As depicted and described in connection with Figure 3 below, a digital signature algorithm 221 can be used in a step 205 in order to authenticate an eUICC 107 operating in a module 101 with an eUICC subscription manager 109.

As illustrated in Figure 2d, the eUICC subscription manager 109 may also be associated with an eUICC subscription manager public key 220 and an eUICC subscription manager private key 222, and the two keys can comprise a PKI key pair for the eUICC subscription manager 109. The eUICC subscription manager public key 220 and an eUICC subscription manager private key 222 can be formatted and processed by algorithms equivalent or similar to the algorithms and format for the eUICC public key 214 and the eUICC private key 215 described in this Figure 2d above. The eUICC subscription manager public key 220 can optionally be signed by a certificate authority. An eUICC 107 can use the digital signature algorithms 221 and the eUICC subscription manager public key 220 to verify a digital signature from the eUICC subscription

Petitioner Samsung Ex-1004, 0562

manager 109. Although not illustrated in Figure 2d, the eUICC 107 or module 101 could also record a public key associated with the mobile network operator 104, and use the public key associated with the mobile network operator 104 to verify a digital signature from the mobile network operator 104 using the digital signature algorithms 221.

Figure 2e

Figure 2e is a graphical illustration for ciphering and deciphering a key for an eUICC using an asymmetric ciphering algorithm using a PKI key pair, in accordance with exemplary embodiments. An eUICC subscription manager 109 could process or calculate a key ciphering algorithm 216 and a module 101 or eUICC 107 could process or calculate a key deciphering algorithm 217. The eUICC key ciphering algorithm 216 can use an asymmetric ciphering algorithm 219 with an input of (i) an eUICC public key 214 as a cipher key and (ii) the eUICC profile key 107b as plaintext in order to output ciphertext of an encrypted eUICC key 218. The plaintext eUICC profile key 107b can comprise a random number of appropriate length for processing a profile ciphering algorithm 210 and profile deciphering algorithm 206 as depicted and described in connection with Figure 2b above. As illustrated in Figure 2e, the input into a key ciphering algorithm 216 could also include an optional security token 212, where a security token 212 is depicted and described in connection with Figure 2b above.

An asymmetric ciphering algorithm 219 within a key ciphering algorithm 216 and a key deciphering algorithm 217 an comprise an algorithm for utilizing public key infrastructure (PKI) techniques to both (i) encrypt plaintext with a public key and (ii) decrypt plaintext with a private key. Example algorithms within asymmetric ciphering algorithm 219 include an RSA algorithm and an elliptic curve cryptography (ECC) algorithm, and other asymmetric ciphering algorithms could be utilized as well. The use and application of RSA algorithms and cryptography are described within IETF RFC 3447 titled "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", herein incorporated by reference, among other published standards for the use of RSA algorithms. The use of an RSA algorithm in an

Petitioner Samsung Ex-1004, 0563

asymmetric ciphering algorithm 219 for encryption and decryption, can also be processed according to the description of the RSA algorithm according to the Wikipedia entry for "RSA (algorithm)" as of September 9, 2013, which is incorporated by reference herein. The use and application of an ECC algorithm for asymmetric ciphering algorithm 219 can conform with algorithms within IETF RFC 6090 titled "Fundamental Elliptic Curve Cryptography Algorithms" (herein incorporated by reference), among other published standards using ECC. Asymmetric ciphering algorithm 219 can also utilize elliptic curve cryptography algorithms for the Wikipedia entry for "Elliptic curve cryptography" as of September 9, 2013, which is incorporated by reference herein.

ECC algorithms (with corresponding ECC-based PKI keys) may utilized for asymmetric ciphering algorithm 219 according to exemplary preferred embodiments in order to maintain high security with smaller key lengths, compared to RSA, thereby helping to comparably reduce the message lengths, radio frequency spectrum utilization, and processing power required by module 101. RSA algorithms (with corresponding RSA-base PKI keys) for asymmetric ciphering algorithm 219 may be utilized in other embodiments in order to maintain compatibility with deployed or legacy software and systems that supports RSA based keys and algorithms.

After an eUICC subscription manager 109 uses a eUICC key ciphering algorithm 216 to convert a plaintext eUICC profile key 107b into a ciphertext as an encrypted eUICC key 218, the eUICC subscription manager can send the ciphertext to the module 101. The eUICC subscription manager could send the ciphertext as an encrypted eUICC key 218 to module 101 using an IP network 111, and the IP network 111 could comprise the public Internet. In this manner, the module 101 can securely receive the encrypted eUICC key 218 in order to perform, process, or calculate a key deciphering algorithm 217. Third parties with access to the encrypted eUICC key 218 would not feasibly be able to read the plaintext eUICC profile key 107b, even with access to the eUICC public key 214. The module 101 could receive the encrypted eUICC key 218 along with an eUICC profile identity 107e in order to determine a profile 107c associated with the encrypted eUICC key 218, where a subsequent step (after deciphering the

Petitioner Samsung Ex-1004, 0564

encrypted eUICC key 218) could comprise a profile deciphering algorithm 206. The module 101 could receive the encrypted eUICC key 218 either before or after receiving the profile 107c.

After receiving the encrypted eUICC key 218, the module 101 or eUICC 107 could decrypt the encrypted eUICC key 218 using a key deciphering algorithm 217. A key deciphering algorithm 217 can include a asymmetric ciphering algorithm 219. The asymmetric ciphering algorithm 219 can be equivalent to or the same as the asymmetric ciphering algorithm 219 in a key ciphering algorithm 216 operated or processed by an eUICC subscription manager 109 as described in this Figure 2e above. The asymmetric ciphering algorithm 219 in a key deciphering algorithm 217 can accept input of the eUICC private key 215 as a cipher key. The asymmetric ciphering algorithm 219 in a key deciphering algorithm 217 can also accept input of the encrypted eUICC key 218 as a ciphertext. The key deciphering algorithm 217 can use an asymmetric ciphering algorithm 219 with an input of (i) an eUICC private key 215 as a cipher key and (ii) the encrypted eUICC key 218 as ciphertext in order to output plaintext of an eUICC profile key 107b. As illustrated in Figure 2e, the plaintext could also optionally include a security token 212. After processing a plaintext eUICC profile key 107b from a key deciphering algorithm 217, module 101 or eUICC 107 could use the plaintext eUICC profile key 107b in order to perform a profile deciphering algorithm 206 as illustrated in Figure 2b.

Although exemplary embodiments can include the use of a key ciphering algorithm 216 and a key deciphering algorithm 217 in order to securely transfer the eUICC profile key 107b from an eUICC subscription manager 109 to a module 101, a key ciphering algorithm 216 and a key deciphering algorithm 217 can be omitted in other exemplary embodiments. For example, if the eUICC subscription manager and module 101 or eUICC 107 support the use of a secure key exchange such as Diffie-Hellman or ECDH, then the eUICC profile key 107b could be mutually derived by the two nodes and the encrypted eUICC key 218 would not need to be transferred through an IP network 111 between the two nodes.

In another embodiment, as depicted in Figure 2e, the key ciphering algorithm 216 and key deciphering algorithm 217 may also be used with ciphertext 208c with an encrypted first key

Petitioner Samsung Ex-1004, 0565

K 203 and a plaintext of the first key K 203, if a profile 107d includes ciphertext 208c with encrypted first key K 203. In this case, a mobile network operator 104 could perform the key ciphering algorithm 216 with input of (i) the plaintext first key K 203 and (ii) the eUICC public key 214 in order to output ciphertext 208c. The ciphertext 208c can include the encrypted first key K 203, although the ciphertext 208c could also include other data such as the network parameters 201. The MNO 104 could send the ciphertext 208c (with the encrypted first key K) to the eUICC subscription manager 109 in a step 302b in Figure 3 for inclusion in the profile 107d and profile 107c. As depicted in Figure 2e, a module 101 or eUICC 107 could perform the key deciphering algorithm 217 on the ciphertext 208c with the first encrypted key K 203 in order to obtain the plaintext first key K 203. In this manner, the first key K 203 is not shared as plaintext with any entities besides the MNO 104 and a module 101 with the eUICC 107. In other words, a MNO 104 can use a key ciphering algorithm 216 to prevent the sharing of a plaintext first key K 203 with an eUICC subscription manager 109.

In addition, although Figure 2e illustrates an eUICC subscription manager as performing the eUICC key ciphering algorithm 216 and the module 101 or eUICC 107 as performing the eUICC key deciphering algorithm 217, an alternative embodiment contemplates that the eUICC subscription manager 109 performs the eUICC key deciphering algorithm 217 and the module 101 or eUICC 107 performs the eUICC key ciphering algorithm 216. In this alternative embodiment, the module 101 can (i) derive the eUICC profile key 107b, and (ii) send the ciphertext comprising the encrypted eUICC key 218 to the eUICC subscription manager 109. In this alternative embodiment, the module 101 can (i) use the eUICC subscription manager public key 220 to cipher the derived eUICC profile key 107b, (ii) send the encrypted eUICC profile key 107b to the eUICC subscription manager 109, and (iii) the eUICC subscription manager 109 can decrypt the encrypted eUICC profile key 107b using the eUICC subscription manager private key 222. In this alternative embodiment, the eUICC subscription manager 109 could (i) use the eUICC key deciphering algorithm 217 to decrypt the encrypted eUICC key 218 received from

Petitioner Samsung Ex-1004, 0566

the module 101, and then (ii) subsequent encrypt the profile 107d into a profile 107c using a profile ciphering algorithm 210 as depicted and described in connection with Figure 2b above.

Figure 3

Figure 3 is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments. System 300 can include an eUICC subscription manager 109, an IP network 111, a mobile network operator 104, a module 101. A module 101 can include a network application 101x and an eUICC 107. The network application 101x can perform the operations for communicating with the wireless network 102 (i) at the data-link layer using standards for PLMN networks such as, but not limited to exemplary radio resource control standards within ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification", which is herein incorporated by reference, and (ii) at the network layer using Internet Protocol. Other standards for communication at the data-link layer between a network application 101x and a mobile network operator 104 can be utilized as well without departing from the scope of the present invention. The (i) mobile device 101, using the network application 101x, and (ii) the mobile network operator 104 can send and receive data using the wireless network 102 depicted and described in connection with Figure 1a. Although a single module 101 is illustrated in system 300 in Figure 3, a system 300 could include a plurality of modules 101.

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 network application 101x and the eUICC 107 can send and receive data locally within the module 101 using an eUICC driver 128 as depicted and described in connection with Figure 1b and Figure 1e. The module 101, using a network application 101x, can send and receive data with the eUICC subscription manager 109 using the IP network 111. As illustrated in Figure 3, the

Petitioner Samsung Ex-1004, 0567

module 101 can send and receive data with the eUICC subscription manager 109 in a step 205 using an initial network.

The initial network could comprise a different wireless network 102 than a wireless network 102 (i) for the mobile network operator 104, and (ii) used for a first authentication 304 and a second authentication 310. In other words, module 101 can send and receive data for an eUICC profile 107c through a initial network that is different than the wireless network 102 associated with the mobile network operator 104. The network application 101x could support different standards for wireless networking technologies, such that the different wireless network 102 used to access the eUICC subscription manager 109 could comprise exemplary networks such as WiFi or LTE Advanced, and the network application 101x could use LTE to communicated with the mobile network operator 104. Other possibilities exist as well for the network application 101x to support communication with a variety of different networks without departing from the scope of the present invention.

The left side of network application 101x in Figure 3 for communication with the mobile network operator 104 can comprise communication through a radio 101z with the wireless network 102, and the right side of network application 101x can comprise internal communication within module 101 as described in the paragraph above and also Figure 1e above. The internal communication between network application 101x and eUICC 107 using an operating system 101h could comprise either (i) sharing memory 101e, where module 101 writes data such as, but not limited to, an exemplary RAND 118 value and eUICC 107 reads the values from the shared memory 101e, or (ii) using loopback UDP ports within operating system 101h, such that network application 101x sends a UDP datagram with the RAND 118 value using a first UPD loopback port, and the eUICC 107 receives the UDP datagram with the RAND 118 value using a second UDP loopback port. For an operating system 101h within module 101 using IPv4 addresses, the addresses used for the UDP loopback ports could comprise addresses in the range of the 127.0.0.0/8 address block. For an operating system 101h within module 101 using IPv6 addresses, the addresses used for the UDP loopback ports could comprise an ::1

Petitioner Samsung Ex-1004, 0568

address. In another embodiment illustrated in Figure 1f above, the eUICC 107 can communicate with the MNO 104 directly for embodiments where the eUICC 107 includes an IP address 106c.

At a step 301, a module 101 can record an eUICC identity 107a, an address 109a of an eUICC subscription manager 109, and an eUICC private key 215 associated with the eUICC 107. A manufacturer, distributor, technician, end user, or installer of module 101 could record the data for a step 301 in module 101, or the data could be downloaded or accessed separately via an IP network 111, including the public Internet. Other data could be included in a step 301 as well, such as, but not limited to, the software or firmware comprising the eUICC 107, an eUICC profile key 107b, an eUICC public key 214, an eUICC subscription manager public key 220, an eUICC driver 128, an initial profile 107d or 107c, and policy rules for allowing access to the profiles, and other additional data could be included in a step 301 as well. Additional optional data for recording with an eUICC 107 in a step 301 are depicted on the second line of step 301 in Figure 3.

In an exemplary embodiment, a manufacturer of module 101 records the exemplary data for an eUICC 107 in a step 301, such that a module 101 can being operations and connecting to an initial wireless network 102 upon power-up in order to establish initial communications, including allowing the communication with the eUICC subscription manager 109 through the initial wireless network 102. As noted above in this Figure 3, an initial wireless network 102 used for the eUICC 107 to access the eUICC subscription manager 109 can be different than the wireless network 102 used to access the mobile network operator 104. The address 109a of an eUICC subscription manager 109 could comprise either an IP address or a domain name, and in an exemplary embodiment the address 109a comprises a domain name and the module 101 can query for the IP address associated with the domain name for address 109a via either a domain name system (DNS) query or a secured DNS query (DNSSEC). A module 101 can connect with an initial wireless network 102 (different than the depicted wireless network 102 in Figure 3) after a step 301 in order to communicate with an eUICC subscription manager 109.

Petitioner Samsung Ex-1004, 0569

At a step 302a, an eUICC subscription manager 109 could record data for the eUICC 107. The data could include (i) an eUICC identity 107a, (ii) a profile 107c, (iii) an eUICC public key 214, (iv) an eUICC subscription manager public key 220 and private key 222, (v) an eUICC profile key 107b with an associated eUICC profile identity 107e, (vii) a module identity 110 (for embodiments where the module identity 110 for the eUICC 107 is known before the eUICC 107 sends and receives data with the eUICC subscription manager 109), (viii) and parameters for a symmetric ciphering algorithm 211 and an asymmetric ciphering algorithm 219 used by the eUICC 107. The parameters for a symmetric ciphering algorithm 211 and an asymmetric ciphering algorithm 219 used by the eUICC 107 could specify the ciphers used, such as (i) selecting an exemplary 128 or 192 bit keys for use with an AES cipher for a symmetric ciphering algorithm 211 used with a eUICC 107 and eUICC identity 107a, and (ii) selecting an exemplary elliptic curve or RSA algorithm for use with an asymmetric ciphering algorithm 219. The eUICC subscription manager 109 could also record related data for the operation of eUICC 107 with eUICC subscription manager 109 in a step 302a.

At a step 302a, the eUICC subscription manager 109 could receive the profile 107d from the mobile network operator 104, and an exemplary profile 107d is depicted and described in connection with Figure 2a. Or, eUICC subscription manager 109 could receive a subset of data for the exemplary profile 107d from the MNO 104 in a step 302a without receiving the entire profile 107d. As one example, the MNO 104 may not know the eUICC profile identity 107e for the eUICC profile 107d, and thus the MNO 104 may not send the complete profile 107d but the MNO 104 could send data for the profile 107d to the eUICC subscription manager 109 in a step 302a. In an exemplary embodiment, the eUICC subscription manager 109 could receive a subset of data for the profile 107d using the IP network 111 over a secured link or connection to the MNO 104. The profile 107d in a step 302a could include both ciphertext 208b and plaintext of a set of network parameters 201, a first network module identity 202, and a first key K 203. As depicted and described in connection with Figure 2a, the ciphertext 208b could comprise an encrypted second key K 204a. The ciphertext 208b could also include the second network

Petitioner Samsung Ex-1004, 0570

module identity 209a. In an exemplary embodiment, the plaintext first key K 203 could be optionally omitted from being received from an MNO 104 in a step 302a, and the eUICC subscription manager 109 can receive the first key K 203 in the form of a ciphertext 208c below in a step 302b. The eUICC subscription manager 109 could use a server or a plurality of servers similar to a server 105 in order to take the processing and communication steps described herein for an eUICC subscription manager 109 in this step 302a and also additional steps for an eUICC subscription manager 109 described throughout Figure 3.

After a module 101 powers up and established connectivity with the IP network 111, an eUICC 107 operating in a module 101 could then perform a step 205 in order to receive an eUICC profile 107c using the IP network 111. The use and operation of a step 205 is also depicted and described in connection with Figure 2a above. In a step 205, an eUICC 107 could send an eUICC identity 107a to the eUICC subscription manager 109. The module 101 could use a network application 101x to send the eUICC identity 107a, such as the network application 101x writing data with the eUICC identity 107a to a physical interface 101a, and the physical interface 101a could include a radio 101z. Or, using the exemplary embodiment illustrated in Figure 1f above, the eUICC 107 could be associated with an IP address 106c, and the eUICC 107 could send the eUICC identity 107a to the eUICC subscription manager 109 without using a separate network application 101x associated with the wireless network 102. During a step 205 for a module 101 or eUICC 107, an eUICC subscription manager 109 could receive the eUICC identity 107a and perform a step 302b. In an exemplary embodiment, both a module identity 110 and an eUICC identity 107a could be sent by an eUICC 107 or a module 101 in a step 205. Or, the eUICC identity 107a could comprise a module identity 110, and the module identity 110 could be sent in a step 205. Other possibilities exist as well for identifying a module 101 or an eUICC 107 with an eUICC subscription manager 109 without departing from the scope of the present invention.

In an exemplary embodiment, a message with the eUICC identity 107a in a step 205 could include a digital signature, where the digital signature is processed using (i) the eUICC

Petitioner Samsung Ex-1004, 0571

private key 215 recorded in a step 301 and (ii) a digital signature algorithm 221. The message with the eUICC identity 107a and a digital signature in a step 205 could preferably include a random number or string, including a nonce or a "number used once" such as, but not limited to, an exemplary security token 212 in order to prevent replay attacks.

An eUICC subscription manager 109 can take several actions in a step 302b after receiving an identity for the eUICC 107 or module 101. A first action in a step 302b could comprise authenticating an eUICC 107 or a module 101 based on the eUICC identity 107a received in the message. In a step 302b, eUICC subscription manager 109 can authenticate the message with eUICC identity 107a according to message digest, or using the eUICC profile key 107b which could be recorded in the eUICC 107 in a step 301 above. In addition, the eUICC subscription manager could authenticate using a digital signature algorithm 221, where the message with the eUICC identity 107a could include a digital signature, as described in the paragraph above.

Both the eUICC 107 and the eUICC subscription manager 109 could use the eUICC profile key 107b as a cipher key with a symmetric ciphering algorithm 211 to encrypt/decrypt data sent with the eUICC identity 107a, where the successful encryption and decryption of data with eUICC identity 107a using the eUICC profile key 107b on both ends could be confirmation that the eUICC 107 or module 101 is authenticated, since both parties would only be able to mutually successfully encrypt and decrypt by sharing the same eUICC profile key 107b. In another embodiment, the eUICC profile key 107b could be used as a private key with a digital signature algorithm 211 (instead of the eUICC private key 215), in order for the eUICC 107 with the eUICC 107a to be authenticated. For embodiments where the module 101 with the eUICC 107 sends a digital signature with the eUICC identity 107a, the eUICC subscription manager 109 could use the eUICC identity 107a to select the eUICC public key 214 or eUICC profile key 107b from a database. In this manner, the eUICC subscription manager 109 could communicate with a plurality of eUICCs 107 and select the appropriate keys using the eUICC identity 107a.

Petitioner Samsung Ex-1004, 0572

A second action in a step 302b could comprise the eUICC subscription manager 109 authenticating with an eUICC 107 or a module 101. The eUICC subscription manager 109 could also authenticate with an eUICC 107 at a step 302b within a step 205, such that eUICC 107 can confirm an identity of the eUICC subscription manager 109, using any of the same or equivalent steps described in the paragraph above for an eUICC 107 to authenticate with an eUICC subscription manager 109. The eUICC subscription manager 109 could send the eUICC 107 a digital signature processed using a digital signature algorithm 221 and the eUICC subscription manager private key 222. The eUICC 107 could verify the digital signature using a eUICC subscription manager public key 220 (which could be recorded with an eUICC 107 in a step 301). The eUICC 107 could also receive data encrypted with a eUICC profile key 107b, and successful decryption of the data by the eUICC 107 using a symmetric ciphering algorithm 211 could confirm the eUICC subscription manager 109 also holds the eUICC profile key 107b. Note that a system 300 could include multiple eUICC keys 107b, such that a first eUICC profile key 107b is used with a step 301 and step 205 in Figure 3, and a second eUICC profile key 107b could be used with a subsequent step 206 below. Other possibilities exist as well for an eUICC 107 and an eUICC subscription manager 109 to perform a 2-way authentication in a step 205 and a step 302b in Figure 3 without departing from the scope of the present invention.

In another exemplary embodiment, where data received from an MNO 104 does not include a plaintext first key K 203 for inclusion in a profile 107d, for a third action in a step 302b, the eUICC subscription manager 109 could send the eUICC identity 107a (or the module identity 110) and the eUICC public key 214 to the MNO 104. In this embodiment, the MNO 104 could also use the key ciphering algorithm 216 depicted and described in connection with Figure 2e above in order to encrypt the first key K 203 with the eUICC public key 214. The output of an MNO 104 using a key ciphering algorithm 216 could comprise a ciphertext 208c of an encrypted first key K 203. Thus, at a step 302b for the embodiment described in this paragraph, the eUICC subscription manager 109 could receive the first key K 203 for a profile 107d as ciphertext 208c (instead of a plaintext first key K 203 for profile 107d in Figure 2a), In this

Petitioner Samsung Ex-1004, 0573

manner, the first key K 203 in a profile 107d could be recorded as ciphertext 208c, which is also depicted and described as an optional format for the first key K 203 in Figure 2a and Figure 2e.

In an exemplary embodiment, the MNO 104 can send the ciphertext 208c only after a user 113 conducts a separate authentication step 308b below. In other words, a step 308b could also be used concurrently with a step 302b, where the step 302b includes the receipt of an encrypted first key K 203 in a ciphertext 208c. In this manner, the MNO 104 can retain control over the release of an encrypted first key K 203, such that the first key K 203 in a ciphertext 208c is only received by an eUICC subscription manager 109 in a step 302 or a eUICC 107 in a step 205 after a user 113 (associated with the module 101 with the eUICC 107) authenticates with the MNO 104. In this embodiment, a separate authentication step 308b below can be optionally omitted, and the use of an encrypted second key K 204a in ciphertext 208b can also be omitted. In this embodiment, a user 113 of the module 101 can access the wireless network 102 of the mobile network operator 104 using the first key K 203 which has been (i) encrypted by the mobile network operator 104 using a key ciphering algorithm 216 in a step 302b, and (ii) only available to module 101 or eUICC 107 (or eUICC subscription manager 109) after a user 113 conducts an authentication step 308b with MNO 104.

After the eUICC subscription manager 109 receives and/or processes all the data for a profile 107d, including subsets of data from a MNO 104 described for this step 302b above, a fourth action in a step 302b could comprise the eUICC subscription manager 109 ciphering a profile 107d using a profile ciphering algorithm 210, in order to convert profile 107d with plaintext into a profile 107c with ciphertext. Some elements in a profile 107c could remain plaintext as well, such as the exemplary profile identity 107e. The eUICC subscription manager 109 could use an eUICC profile key 107b, where the eUICC profile key 107b in a profile ciphering algorithm 210 can be different than an eUICC profile key 107b used to authenticate eUICC 107 with eUICC identity 107a. Or, the same eUICC profile key 107b could be used to both cipher profile 107d and authenticate eUICC 107. Note that this fourth action in a step 302b could also take place at an earlier time than at step 302b, such that eUICC subscription manager

Petitioner Samsung Ex-1004, 0574

109 could assemble and cipher the profile 107d into a profile 107c at an earlier time, such as before receiving the eUICC identity 107a, or concurrent with a step 301a. Other possibilities exist as well for the timing and sequence for an eUICC subscription manager to assemble and process a profile 107c without departing from the scope of the present invention.

After a step 302b, the eUICC subscription manager 109 can send the authenticated eUICC 107 a profile 107c in a step 205, as depicted in Figure 3. Either the eUICC subscription manger 109 or the eUICC 107 can select the profile 107c to be received by the eUICC 107. In one embodiment, a module 101 can search for radio beacons from base stations 103 for wireless networks 102 surrounding the module 101, and upon finding new possible wireless network 102 to connect with, the module 101 or eUICC 107 could query or request the eUICC subscription manager 109 for a profile 107c associated with a mobile network operator 104 for a radio beacon observed by the module 101. Commercial business arrangements among the user of module 101, the eUICC subscription manager 109, and the mobile network operator 104 can determine the availability of a profile 107c for a module 101 with an eUICC 107.

In another embodiment, the eUICC subscription manager 109 could periodically send the module 101 and/or eUICC 107 new profiles 107c as they become available to a user 113 of a module 101 or available to the eUICC subscription manager 109. In a preferred embodiment, the eUICC subscription manager 109 can send the profile 107c to the module 101 using a network application 101x, where the network application 101x forwards the data to the eUICC 107. As described above in this Figure 3, the network application 101x could communicate with the eUICC 107 using the operating system 101h as illustrated in Figure 1e, and other possibilities exist as well. Note that eUICC subscription manager 109 sends the profile 107c, where the network access credentials (including the first key K 203) are encrypted with an eUICC profile key 107b, and in this manner intermediate nodes on the IP network 111 would not feasibly be able to read the data within the profile 107c.

In an exemplary embodiment, the eUICC subscription manager 109 can send the module 101 a pointer, uniform resource locator (URL), domain name, or related address for a location of

Petitioner Samsung Ex-1004, 0575

the eUICC profile 107c in a step 205 as opposed to the actual, full profile 107c. In this embodiment, the module 101 could receive the pointer, uniform resource locator, domain name, or related address for the location of the eUICC profile 107c and subsequently download the eUICC profile 107c from an IP address associated with the pointer, uniform resource locator, domain name, or related address for a location of the eUICC profile 107c.

As depicted in Figure 3, after receiving the profile 107c from the eUICC subscription manager 109 in a step 205, the eUICC 107 can receive data for decrypting the profile 107c in a step 303. Note that if eUICC profile key 107b (in the form of a symmetric key as illustrated in Figure 2b) has already be shared between the eUICC 107 and the eUICC subscription manager 109 before a step 206 below, then a step 303 could separately be omitted. For example, if an eUICC profile key 107b has been recorded with an eUICC 107 in a module 101 by a manufacturer of module 101, then that eUICC profile key 107b could be used in a step 206 below, and a separate step 303 could be omitted. In other exemplary embodiments, the eUICC 107 can receive data for processing or deriving the eUICC profile key 107b for a step 206 below using the step 303 illustrated in Figure 3. A step 303 can include the receipt by eUICC 107 of either (i) an encrypted eUICC key 218, or (ii) data for a key exchange. The encrypted eUICC key 218 received by an eUICC 107 in a step 303 could comprise an eUICC profile key 107b that is ciphered using a key ciphering algorithm 216 illustrated in Figure 2e. For embodiments where data for a key exchange is received in a step 303, the algorithms used with a key exchange could comprise a Diffie Hellman key exchange, or an Elliptic Curve Diffie Hellman key exchange (ECDH).

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. A summary of ECDH is included in the Wikipedia article titled “Elliptic Curve Diffie-Hellman” (http://en.wikipedia.org/wiki/Elliptic_curve_Diffie %E2%80%93Hellman from September 24, 2013, which is herein incorporated by reference. An ECDH key exchange in a step 303 could

Petitioner Samsung Ex-1004, 0576

comprise the message received by a eUICC 107 including a common base point G. The base point G could also be sent from an eUICC 107 to eUICC subscription manager 109. The base point G for an ECDH key exchange in a step 303 could also be recorded with the eUICC in a step 301 above, and in this case the message at a step 303 received by an eUICC 107 could comprise a signal to initiate or use a key exchange for deriving the eUICC profile key 107b. Note that the eUICC subscription manager 109 and the eUICC 107 could take additional steps to process the eUICC profile key 107b after an ECDH key exchange at step 303, such as taking the output of an ECDH key exchange and inputting that output into a secure hash algorithm in order to obtain the eUICC profile key 107b. Other algorithms besides an ECDH or Diffie Hellman key exchange can be utilized as well at a step 303, including a key exchange according to the American National Standards Institute (ANSI) standard X-9.63.

After completing a step 303, an eUICC 107 operating in a module 101 could read and utilize the eUICC profile key 107b. In embodiments where the eUICC profile key 107b in a step 303 above comprises an encrypted eUICC key 218, a step 217 from Figure 2e can be utilized by the eUICC 107 in order to decrypt the eUICC key 218 into a plaintext of eUICC profile key 107b. The plaintext eUICC profile key 107b can be used by the eUICC 107 in a step 206 to decrypt (x) the profile 107c received in a step 205 above into (y) a profile 107d. The use of an eUICC profile key 107b for a step 206 is also depicted and described in connection with Figure 2a above and also Figure 2b. Plaintext within a profile 107d can be read after a step 206, although in exemplary embodiments and as illustrated in Figure 2a, the profile 107d can continue to record ciphertext 208b and ciphertext 208c.

In an exemplary embodiment, after a step 206 in Figure 3 to convert received profile 107c to profile 107d, if (A) a ciphertext 208c that includes the first key K 203 is present in profile 107d (as depicted in Figure 2a above), then (B) eUICC 107 could also use a key deciphering algorithm 217 on ciphertext 208c in order to extract the plaintext first key K 203. Note that ciphertext 208a could be ciphered by an eUICC subscription manager 109 (using a profile ciphering algorithm 210) and ciphertext 208b and/or ciphertext 208c could be encrypted

Petitioner Samsung Ex-1004, 0577

by a mobile network operator 104 (using a key ciphering algorithm 216). In other words, a module 101 with an eUICC 107 can use (i) a profile deciphering algorithm 206 with an eUICC profile key 107b to decrypt ciphertext 208a, (ii) a key deciphering algorithm 217 with an eUICC private key 215 to decrypt ciphertext 208c, and/or (ii) a key K deciphering algorithm 207 with a symmetric key 127 to decrypt ciphertext 208b.

After reading plaintext in profile 107d, module 101 could then utilize the profile 107d to conduct a first authentication 304 with the mobile network operator 104. As depicted in Figure 3, the first authentication 304 can comprise (i) module 101 sending an attach message 305 with network module identity 202, (ii) the eUICC 107 and module 101 receiving a RAND 118, (iii) the eUICC 107 using a step 306 in order to calculate a RES 119, and (iv) the module 101 sending the RES 119. Although not illustrated in Figure 3, a first authentication 304 could include other data such as receiving the equivalent of an "OK" message upon successful authentication, the receipt of additional network parameters 202 after successful authentication, etc. The module 101 can use a profile 107d from a step 206 above in order to conduct the first authentication 304. The profile 107d in an eUICC 107 could be selected and activated in order to connect with a wireless network 102 associated with mobile network operator 104. As contemplated herein and throughout the present invention, an activated profile 107d can comprise a selected and enabled network access application state as illustrated in Figure D.1 of ETSI TS 103 383 v.2013-02 for the activated profile 107d, and other possibilities exist as well. As illustrated in Figure 3 after a step 206, the module 101 can use a network application 101x in order to attach to the wireless network 102 and communicate with the mobile network operator 104.

Within a first authentication 304, the module 101 can send a first attach message 305, and the first attach message 305 can include the first network module identity 202. With a 4G LTE network, the first attach message 305 could comprise a radio resource connection request message, or a similar message could be utilized with other wireless networking standards as well, such as LTE Advanced or WiMAX. An exemplary radio resource connection request is described in section 5.3.3 within ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal

Petitioner Samsung Ex-1004, 0578

Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification", which is herein incorporated by reference. Although not illustrated in Figure 3, the module 101 and wireless network 102/mobile operator 104 could take additional related steps before sending the exemplary first attach message 305, such as, but not limited to, module 101 synchronizing a clock 160 with wireless network 102, module 101 sending a message on a random access control channel (RACH) in order to have a timeslot and frequencies for sending the first attach message 305, etc.

As depicted in Figure 3, after receiving and processing the first attach message 305, the mobile network operator can send a first random number (RAND) 118. Although not illustrated in Figure 3, a network authentication token "AUTN" and a sequence number could be sent with the first RAND 118. An exemplary format for the use of a RAND 118 with a response RES 119 is described in ETSI standard TR 131 900 v.10.0.0 and related documents. In a first authentication 304 the module 101 and the eUICC 107 can receive the first RAND 118. The eUICC 107 can conduct a step 306 with an input of the first RAND 118 and the first key K 203 in order to calculate a first RES 119. The use of a RAND 118 with a RES 119 in a step 306 could comprise a general use of a message digest authentication, and another exemplary message digest authentication is also described in IETF RFC 2617, titled "HTTP Authentication: Basic and Digest Access Authentication". After receiving the exemplary first RAND 118 message, in order to conduct a first authentication 304, module 101 using an eUICC 107 could take steps to demonstrate to MNO 104 that module 101 has access to the same first key K 203 as recorded by the MNO 104 in a step 302a or step 302b above. MNO 104 could record the expected RES 119 value with a set of authentication vectors 117 for the first network module identity 202, as depicted in Figure 1d and Figure 1e.

Module 101 can properly respond to a challenge/nonce (such as a first RAND 118) in a message digest authentication by sending a secure hash value calculated using (i) the challenge/nonce and (ii) the first key K 203. The secure hash value can comprise the first RES 119. In exemplary embodiments, eUICC 107 and wireless network 102 could use algorithms

Petitioner Samsung Ex-1004, 0579

specified in ETSI TS 135 205 – 209, as well as subsequent and related standards, in order for module 101 using eUICC 107 to (i) calculate a secure hash value, and (ii) process related steps for a first authentication 304. After processing a first RES 119 in a step 306 using the first key K 203, the eUICC 107 could send the first RES 119 to the network application 101x in module 101. Module 101 could then send the first RES 119 to the mobile network operator 104 using the wireless network 102, as depicted in Figure 3 and thereby complete a first authentication step 304 for the module 101.

In another embodiment for a first authentication step 304, (i) module 101 could send (i) the first network module identity 202 a digital signature processed using a digital signature algorithm 221 and the eUICC private key 215, and (ii) MNO 104 could verify the digital signature using a digital signature algorithm 221 and the eUICC public key 214. Other possibilities exist as well for steps within a first authentication 304 using a eUICC private key 215 with the first network module identity 202 or the eUICC identity 107a in a first authentication step 304 without departing from the scope of the present invention. In an exemplary embodiment, as depicted in Figure 1f above, the eUICC 107 could include an IP address 106c with an interface identifier 106e associated with the eUICC 107, and in this case the module 101 could send the first RES 119 value from the eUICC 107 to the MNO 104 through the wireless network 102.

In a step 308a the mobile network operator 104 can receive the first RES 119. A server 105 such as a mobility management entity (MME) for the mobile operator network 104 associated with the wireless network 102 could compare the received first RES 119 with an internally recorded RES 119 from the authentication vector 117. As noted above, the authentication vector 117 could be received by the server 105 from the HSS of the mobile network operator 104 before a step 308a. If the received first RES 119 matches the internally stored first RES 119 value, the wireless network 102 and mobile network operator 104 can consider or process that the module 101 is authenticated for a step 308a. The wireless network 102, the MNO 104, and the module 101 can take subsequent steps (not shown) for the module

Petitioner Samsung Ex-1004, 0580

101 to access the IP network 111, in order to conduct authentication of the module 101 or a user associated with the module 101 with a second factor in a step 308b below.

In a step 308b, the mobile network operator 104 can conduct a separate authentication of either a user 113 associated with a module 101 or the module 101 using a second factor. In other words, the mobile network operator 104 can use a step 308b to authenticate the user 113 of module 101 or the module 101 using steps and a process that is different than the first authentication 304. Note that this use of a separate authentication step 308b can be different than conventional technology used in authenticating a module 101 in a step 304, since other values and tokens besides the first key K 203 can be used in the authentication step 308b. The additional authentication step 308b can be useful for a mobile network operator 104 to authenticate a module 101 with an eUICC 107 and profile 107d, since the profile 107d with the first key K 203 may be transferred to module 101 in a communications channel outside the control of mobile network operator 104. As one example, the profile 107d with the first network key K 203 could be transferred to an eUICC 107 from the eUICC subscription manager 109 using an IP network 111, as depicted in Figure 3 in a step 205. The mobile network operator 104 may not have control over the IP network 111 used in a step 205. The mobile network operator 104 may not have control over the security keys and algorithms used to encrypt the profile 107d into a profile 107c, and thus the security of the first key K 203 upon which the MNO 104 depends for authentication and ciphering of data with module 101 may be outside the control of MNO 104. As one example, the MNO 104 may not be able to separately authenticate the identity of a user of module 101 with the eUICC 107, before the profile 107d was received by module 101 and eUICC 107 in a step 205.

Consequently, without a separate authentication step 308b the user 113 of module 101 with the eUICC 107 may be unknown to MNO 104, and a separate identity of the user 113 or module 101 (other than network module identity 202) may preferably be authenticated in a step 308b. Thus, a MNO 104 may use a separate authentication step 308b in order to authenticate a user 113 of module 101 with the eUICC 107 and the first key K 203 in exemplary embodiments.

Petitioner Samsung Ex-1004, 0581

The user 113 can have a contractual or business relationship with MNO 104 in order to pay for voice and/or data services from the MNO 104, and thus the MNO 104 can preferably identify and authenticate a user 113 in a step 308b.

A step 308b can comprise the authentication and/or secure identification of (i) a user 113 of module 101 or (ii) module 101 using a second factor. Although a step 308b is depicted in Figure 3 as being performed after a first authentication 304, a step 308b could be performed before a step 304 (including with a step 302b as described in step 302b above). The use of a second factor in an authentication step 308b can comprise a two-factor authentication, where the first factor can be the successful completion of authentication using a step 304 and step 308a described above. The steps for authenticating a user 113 or module 101 in a step 308b could comprise many different forms without departing from the scope of the present invention. In one embodiment, where the user 113 of module 101 comprises a subscriber to telecommunication and data services from MNO 104, the user 113 could present identification to a representative of the MNO 104 in a step 308b. The identification could be in the form of a physical identity such as, but not limited to, a drivers license or a passport (along with a value that can be associated with the eUICC profile 107d such as the module identity 110 or the eUICC identity 107a). The representative of the MNO 104 could record the identification in a web browser with connectivity to a database shared by a server 105.

In another embodiment of an authentication of a user 113 of module 101 (with the eUICC profile 107d recorded with an eUICC 107 in module 101 from a step 205) could enter information into a web page provided by MNO 104, where the user 113 first (i) authenticates on the web page and then (i) enters identification information for the module 101 or eUICC 107. The user 113 could first authenticate with the MNO 104 via a web page by entering a valid identity and a password (where the identity and password for the web page in a step 308b could be previously established between the user 113 and the MNO 104 before a step 308b). In another embodiment for a step 308b, a user 113 could call a telephone number operated by or associated with a MNO 104 and provide identification information via voice or entering

Petitioner Samsung Ex-1004, 0582

information such as dual-tone multi-frequency (DTMF) digits via interactive voice response (IVR). The identification information could include either a credit card number or a personal identification number (PIN) for the user 113 (where the PIN may be previously shared or established between the user 113 and the mobile network operator 104). The user 113 could also send a text message to MNO 104 from module 101 (i) using the module 101 authenticated link with MNO 104 established in a first authentication 304, where (ii) the text message include identification information for a user 113.

In accordance with preferred exemplary embodiments for the verification of an identity of user 113 in a step 308b (including an authentication of user 113 in a step 308b), the user 113 can send data to a MNO 104 from module 101 using a data connection via wireless network 102 associated with (and established after) the first authentication 304. In this manner, data and voice connectivity between the MNO 104 and module 101 could be established with a first authentication step 304, and the user 113 and MNO 104 can conduct an authentication step 308b (or equivalently a verification of an identity of the user 113) to confirm the identity of the user 113 via the established data and voice connectivity using the wireless network 102. In other words, the user 113 could verify or authenticate an identity of the user 113 of module 101 through the wireless network 102 in a step 308b, where (a) module 101 had conducted a first authentication step 304 and 308a with MNO 104 using the first key K 203 recorded in a profile 107d, in order to (b) support or conduct a separate verification or authentication of a user 113. In an exemplary embodiment, the user 113 could enter identifying information for a step 308b in a web page accessed through a user interface 101j on module 101, where data connectivity for the web page is provided to module 101 through the wireless network 102 after a first authentication step 304.

The authentication or verification of user 113 identity in a step 308b can comprise authenticating module 101with a second factor, where the first factor can comprise the first key K 203 and the second factor can comprise information provided by a user 113 in a step 308b. Other possibilities exist as well for those of ordinary skill in the art for (a) a user 113 of module

Petitioner Samsung Ex-1004, 0583

101 with the first key K 203 to (b) authenticate or verify an identity of the user 113 in a step 308b without departing from the scope of the present invention. In these exemplary embodiments for a user 113 to authenticate or verify an identity for the user 113 for module 101 with the MNO 104, the MNO 104 could record information or data received from the user 113 in a database, such that a server 105 for MNO 104 sends the symmetric key 127 in a step 309 below after an identity of the user 113 is verified or authenticated in a step 308b. In exemplary embodiments illustrated in Figure 3, the module 101 can access the wireless network 102 with the first key K 203 in order to (i) establish communication with the IP network 111, (ii) support authentication of a user 113 in a step 308b through the IP network 111, and then (iii) subsequently receive a symmetric key 127 in order to decrypt a ciphertext 208b with a second key K 204a.

In other exemplary embodiments, module 101 could comprise a module supporting "machine-to-machine" applications and communications, and the module could be different than a traditional mobile phone or smartphone for (i) placing voice telephone calls or (ii) supporting a user interface 101j in the form of a touch screen and web browser. The module 101 could include a sensor 101f for collecting data and an actuator 101y for controlling or changing a state associated with a monitored unit for the module 101. In these embodiments, and as depicted and described in connection with Figure 1a, module 101 can be associated with an M2M service provider 115, and the M2M service provider 115 could be associated with a plurality of modules 101, as opposed to an individual with a telephone number for voice services to module 101.

Each of the different modules 101 in the plurality of modules 101 could include different values for module identities 110, eUICC identities 107a, profile identities 107e, and the first network module identities 202. In these embodiments for a step 308b where the module 101 supports M2M applications for an M2M service provider 115, in a step 308b in Figure 3, the MNO 104 could verify that (a) module 101 with eUICC 107 and the profile 107d from a step 304 is (b) properly associated with an M2M service provider 115. In exemplary embodiments, the MNO 104 ould conduct a step 308b by securely or properly determining that an identity from

Petitioner Samsung Ex-1004, 0584

module 101 is associated with M2M service provider 115, and an exemplary identity for module 101 include any of a module identity 110, an eUICC identity 107a, a profile identity 107e, and/or the first network module identity 202.

In exemplary embodiments where module 101 supports M2M application and the module 101 is associated with an M2M service provider 115, MNO 104 could take several possible actions in a step 308b for authenticating or verifying that an identity from module 101 in Figure 3 is associated with an M2M service provider 115. The proper association of an identity of module 101 with M2M service provider 115 may be necessary or useful for contractual and business relationships between MNO 104 and M2M service provider 115, such as, but not limited to, allowing MNO 104 to bill or invoice M2M service provider 115 for data services that MNO 104 provides to module 101. In a first exemplary embodiment for a step 308b in Figure 3 where module 101 supports M2M applications with a M2M service provider 115, MNO 104 could securely send to M2M service provider 115 an identity of module 101, such as, but not limited to module identity 110, eUICC identity 107a, profile identity 107e, and/or the first network module identity 202 through an IP network 111. The MNO 104 could also send the identity of module 101 in a query or request message. Although not illustrated in Figure 3, the MNO 104 could also send the M2M service provider 115 a digital signature received from module 101 before a step 308b, where the digital signature was (i) processed by module 101 using a digital signature algorithm 221 and an eUICC private key 215, and (ii) sent from the module 101 to the MNO 104.

In a step 308b, the M2M service provider 115 could (i) receive the identity of module 101 (such as, but not limited to module identity 110, eUICC identity 107a, profile identity 107e, and/or the first network module identity 202), (ii) verify or determine the identity of module 101 properly belongs to M2M service provider 115, and (iii) send a response confirming the module 101 with the identity is validly associated the M2M service provider 115. The response from the M2M service provider 115 (or data within a message from M2M service provider 115 to MNO 114) for a step 308b can comprise a second factor for MNO 104 in authenticating module 101

Petitioner Samsung Ex-1004, 0585

with eUICC 107 and profile 107d. In this manner, MNO 104 can confirm module 101 with the first network identity 202 is authenticated or verified as belonging to or being associated with M2M service provider 115 in a step 308b.

In another exemplary embodiment for a step 308b, the M2M service provider 115 could also send MNO 104 a list of pre-authorized identities for one or a plurality of modules 101 before a step 308b (and in this case the list can comprise the second factor to authenticate module 101). MNO 104 could query the list of identities received upon receiving an identity of module 101, such as, but not limited to, the first network module identity 202 received in the first attach message 305. Other possibilities exist as well for an MNO 104 to authenticate or verify that an identity of module 101 is associated with a M2M service provider 115 in a step 308b without departing from the scope of the present invention.

After successfully verifying or confirming in a step 308b that module 101 in Figure 3 is associated with a known user 113 or M2M service provider 115, MNO 104 can send a symmetric key 127 in a step 309. A network application 101x in the module 101 can receive the symmetric key 127 and the module 101 can forward the symmetric key 127 to the eUICC 107. As depicted and described in connection with Figure 2a and Figure 2c, the symmetric key 127 can be used by module 101 to decrypt the ciphertext 208b, where the ciphertext 208b can include a second key K 204a. The symmetric key 127 can also previously be used by MNO 104 to encrypt the ciphertext 208b. The ciphertext 208b could be delivered to eUICC subscription manager 109 for including the ciphertext 208b in the profile 107d, as described above in step 302a. The ciphertext 208b could be sent to module 101 from the eUICC subscription manager 109 across the IP network 111 as profile 107c in a step 205 as described above in this Figure 3.

In exemplary embodiments, the MNO 104 can send the symmetric key 127 in a step 309 through the wireless network 102, where the connection between module 101 and MNO 104 could be initiated by the first attach message 305 and authenticated by a first authentication 304. Since the MNO 104 controls the nodes and ciphering steps for the transmission of symmetric key 127, the symmetric key 127 can be securely sent by MNO 104 and received by module 101 with

Petitioner Samsung Ex-1004, 0586

ciphering and keys used at the data-link layer under the control of MNO 104 (whereas MNO 104 may not control the keys and ciphering of sending the first key K 203). Also note no entities, including the module 101, a user 113, an M2M service provider 115, an eUICC subscription manager 109, or unauthorized third parties could feasibly read the ciphertext 208b with the second key K 204a until they receive the symmetric key 127.

In an exemplary embodiment of a step 309 in Figure 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. As described in connection with a key ciphering algorithm 216 in Figure 2e, the MNO 104 could select and read the eUICC public key 214 (using a received associated identity such as the first network module identity 202), and use an asymmetric ciphering algorithm 219 to encrypt the symmetric key 127. 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 and the asymmetric ciphering algorithm 219. For a step 309 in Figure 3, the use of encryption for a symmetric key 127 with an asymmetric ciphering algorithm 219 is optional, and the symmetric key 127 could be sent in a form where encryption is applied at the data-link layer according to standards for the wireless network 102. Other possibilities exist as well for a module 101 to securely receive a symmetric key 127 in a step 309 without departing from the scope of the present invention. As described above in connection with a step 302b, in exemplary embodiments, the module 101 receives the symmetric key 127 after the MNO 104 authenticates or verifies that a user 113 or M2N service provider 115 is associated with module 101, and until the receipt of the symmetric key 127 the ciphertext 208b cannot be feasibly decrypted.

After a step 309, a module 101 with an eUICC 107 can use the symmetric key 127 to decrypt ciphertext 208b, where ciphertext 208b can include the second key K 204a. A module 101 or eUICC 107 can use a key K deciphering algorithm 207 with input from the received symmetric key 127 and the ciphertext 208b from profile 107d to output a plaintext second key K

Petitioner Samsung Ex-1004, 0587

204. Although not illustrated in a step 207 in Figure 3, but as illustrated in a step 207 in Figure 2a, a module 101 can use an eUICC 107 to also decrypt a second network module identity 209a for the second key K 204 using the symmetric key 127. The second network module identity 209a can be recorded in the ciphertext 208b. The second network module identity 209a can be different than the first network module identity 202, such as a different number or value for an IMSI. The second network module identity 209a can be the same length as the first network module identity 202. The use and operation of a key K deciphering algorithm 207 is also depicted and described in connection with Figure 2a and Figure 2e above.

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 such that the plaintext second key K 204 remains available to module 101 after power or a battery 101k is removed from module 101. The plaintext second key K 204 could also be recorded in a protected memory within module 101, such that the operating system 101h or CPU 101b may prevent read or write access to the protected memory by other processes than the eUICC 107. In other words, with a protected memory, other applications such as, but not limited to, applications that are downloaded from an "app store" or equivalent and installed by end users on the module 101 may be prevented by the operating system 101h from having access to the plaintext second key K 204 recorded in the protected memory.

In another embodiment, a module 101 may optionally not store the plaintext second key K 204 in nonvolatile memory, such that the second key K 204 continues to be recorded for a long-term basis only as ciphertext 208b in a nonvolatile memory such as flash 101w. The module 101 could perform a key K deciphering algorithm 207 each time a plaintext second key K 204 is needed for authentication purposes, including related key derivation of a CK and IK plus other derived keys. In this manner (by storing the second key K 204 in ciphertext 208b in module 101) a plaintext second key K 204 may not be (i) stored in module 101 for a relatively long time such as several hours or longer, and also (ii) recorded outside a nonvolatile memory.

Petitioner Samsung Ex-1004, 0588

In another embodiment, (A) the plaintext second key K 204 is recorded only in a volatile memory within CPU 101b such as a register or cache memory, where access to the register or cache memory is limited to the eUICC 107, and (B) after a successful authentication using the second key K 204, such as, but not limited to, a second authentication 311 below, the plaintext second key K 204 is flushed from the register or cache memory within CPU 101b. In this manner, after (A) a first time that module 101 conducts a step 207 to obtain a plaintext second key K 204 and the module 101 completes a full power cycling, then (B) the plaintext second key K 204 may not be recorded in any of a volatile memory, a non-volatile memory, or a protected memory within module 101 (but module 101 could record an encrypted second key K 204a in a ciphertext 208b).

For the embodiments where the second key K 204 is not recorded as plaintext in a nonvolatile memory within module 101, the module 101 can perform a step 207 with a ciphertext 208b recorded in a nonvolatile memory a second time to process or obtain the plaintext second key K 204. In other words, the second key K 204 can be recorded on a long-term basis as a ciphertext 208b for eUICC 107 within module 101, in an exemplary embodiment, thereby increasing the security of the second key K 204. In this case, either (i) the symmetric key 127 could be recorded in a nonvolatile memory 101w in order to allow decrypting of the ciphertext 208b, or (ii) the module 101 could receive the symmetric key 127 a second time by conducting a step 309 a second time. The module 101 can reconnect with the wireless network 102 and the MNO 104 using the first network identity 202 and the first key K 203 a second time, after the module 101 has already received the symmetric key 127 a first time. The MNO 104 may optionally authenticate the user 113 or M2M service provider 115 a second time such as a second step 308b (before sending the symmetric key 127 a second time) in order to confirm a second use of the first key K 203 is authorized.

After a module 101 with an eUICC 107 processes a key K deciphering algorithm 207 to obtain a plaintext second key K 204, the module 101 can connect with the wireless network 102 and mobile network operator 104 using the second network module identity 209 and the second

Petitioner Samsung Ex-1004, 0589

network key 204. The module 101 using a network application 101x could send a second attach message 305 with the second network module identity 209. In another embodiment, the module 101 could send the second attach message 305 with the first network module identity 202, and in this case the MNO 104 could record from the previous steps 302b and 308b that a key K associated with the first network module identity 202 should change to the second key K 204.

But, given existing deployed infrastructure and systems for a mobile network operator 104, the use of two different keys K with the same network module identity may be more difficult to support, and for this case and with preferred embodiments, the module 101 attaches with the MNO 104 the second time with the second network module identity 209 that has been deciphered from (i) a ciphertext 208b in a step 207 above, or (ii) a ciphertext 208a in a step 206 above. The second attach message 305 can be equivalent to the first attach message 305, but with a change of module 101 sending the second network module identity 209. With a 4G LTE network, the second attach message 305 could comprise a radio resource connection request message, or a similar message could be utilized with other wireless networking standards as well, such as LTE Advanced or WiMAX. An attach message such as 305 in Figure 3 could also comprise module 101 using a globally unique temporary identity (GTUI) that can be associated with the second network module identity 209. Other possibilities exist as well for the format or structure of an attach message 305 without departing from the scope of the present invention.

After sending the second attach message 305, the module 101 with a eUICC 107 can conduct a second authentication 310 with the mobile network operator 104. The module 101 and eUICC 107 could take the equivalent steps as the first authentication 304 depicted and described in this Figure 3, but with a difference of using the second network module identity 209 and the second key K 204. In a second authentication 310, the mobile network operator 104 could send the module 101 a second RAND value 118 through the wireless network 102. A server 105 associated with MNO 104, such as, but not limited to, a HSS could have previously processed an authentication vector 117 comprising at least (i) the second RAND value 118, (ii) a network authentication token AUTN and sequence number (not shown), and (iii) a response value RES

Petitioner Samsung Ex-1004, 0590

119 for the second network module identity 209 and the second key K 204. The server 105 or HSS associated with the MNO 104 could send the authentication vector 117 to a server or MME that module 101 communicates with through the wireless network 102. The module 101 could receive the second RAND 118 using the network application 101x, and forward the second RAND 118 to the eUICC 107. The communication steps between a network application 101x and an eUICC 107 in Figure 3 could also use the steps depicted and described in connection with Figure 1e.

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. The MNO could record the second key K 204 in an authentication vector 117 a step 302a or step 302b above. Module 101 can properly respond to a challenge/nonce (such as a second RAND 118) in a message digest authentication by sending a secure hash value calculated using (i) the challenge/nonce and (ii) the second key K 204. The secure hash value can comprise the second RES 119. In exemplary embodiments, the eUICC 107 and wireless network 102 could use algorithms specified in ETSI TS 135 205 – 209, as well as subsequent and related standards, in order for module 101 using eUICC 107 to (i) calculate a secure hash value, and (ii) process related steps for a second authentication 310. After processing a second RES 119 in a step 311 using the second key K 204, the eUICC 107 could send the second RES 119 to the network application 101x in module 101. Module 101 could then send the second RES 119 to the mobile network operator 104 using the wireless network 102, as depicted in Figure 3 and thereby complete a second authentication step 310 for the module 101. In an exemplary embodiment, as depicted in Figure 1f above, the eUICC 107 could include an IP address 106c with an interface identifier 106e associated with the eUICC 107, and in this case the module 101 could send the second RES 119 value from the eUICC 107 to the MNO 104 through the wireless network 102.

Petitioner Samsung Ex-1004, 0591

At a step 312, the mobile network operator can receive the second RES 119 from the module 101 using the wireless network 102. A server 105 for the mobile operator network 104 associated with the wireless network 102 could compare the received second RES 119 with an internally recorded RES 119. The server 105 could receive an authentication vector 117 comprising at least the second RAND 118, second RES 119, and AUTN token for the second network module identity 209 before sending the second RAND 118 in a step 310 above. If the received second RES 119 matches the internally stored second RES 119 value, the wireless network 102 and mobile network operator 104 can consider or process that the module 101 is authenticated for a step 312. The wireless network 102, the MNO 104, and the module 101 can take subsequent steps (not shown) for the module 101 to access the IP network 111, including allowing module 101 to place and receive telephone calls and/or access the public Internet.

In an exemplary embodiment that utilizes the steps illustrated in Figure 3, the fist key K 203 can comprise a null value or the number zero, which is contemplated in standards and supported by commercial wireless networks 102 in order to support emergency services for a module 101 without a valid UICC or eUICC. The MNO 104 and wireless network 102 can provide limited access to the IP network 111, such that a user 113 of module 101 with a null or zero value for the first key K 203 could performs steps to authenticate or verify the user 113 identity in a step 308b. The limited access to the IP network 111 may not include access to the public Internet, but could include access to a server such as a web server for the user 113 to enter identification information. The data-link layer may not be encrypted due to the use of a null value for the first key K 203, but the application or transport layer could secure communication from a web browser on the module 101 to the web server, such as using transport layer security (TLS). Other possibilities exist as well for ciphering or securing data at the application or transport layer in a step 308b to authenticate a user 113 without encryption at the data-link layer (such as without encryption by the wireless network 102 due to a null value for first key K 203). In this embodiment where the first key K 203 comprises a null or zero value, after authentication of a user 113 or M2M service provider 115 in a step 308b, the second key K 204 used with a

Petitioner Samsung Ex-1004, 0592

second authentication 310 can comprise a regular key K such as a non-null value or a random number.

Figure 4

Figure 4 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments. The processes and operations, described below with respect to all of the logic flow diagrams may include the manipulation of signals by a processor and the maintenance of these signals within data structures resident in one or more memory storage devices. For the purposes of this discussion, a process can be generally conceived to be a sequence of computer-executed steps leading to a desired result.

These steps usually require physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, or otherwise manipulated. It is convention for those skilled in the art to refer to representations of these signals as bits, bytes, words, information, elements, symbols, characters, numbers, points, data, entries, objects, images, files, or the like. It should be kept in mind, however, that these and similar terms are associated with appropriate physical quantities for computer operations, and that these terms are merely conventional labels applied to physical quantities that exist within and during operation of the computer.

It should also be understood that manipulations within the computer are often referred to in terms such as listing, creating, adding, calculating, comparing, moving, receiving, determining, configuring, identifying, populating, loading, performing, executing, storing etc. that are often associated with manual operations performed by a human operator. The operations described herein can be machine operations performed in conjunction with various input provided by a human operator or user that interacts with the computer.

Petitioner Samsung Ex-1004, 0593

In addition, it should be understood that the programs, processes, methods, etc. described herein are not related or limited to any particular computer or apparatus. Rather, various types of general purpose machines may be used with the following process in accordance with the teachings described herein.

The present invention may comprise a computer program or hardware or a combination thereof which embodies the functions described herein and illustrated in the appended flow charts. However, it should be apparent that there could be many different ways of implementing the invention in computer programming or hardware design, and the invention should not be construed as limited to any one set of computer program instructions.

Further, a skilled programmer would be able to write such a computer program or identify the appropriate hardware circuits to implement the disclosed invention without difficulty based on the flow charts and associated description in the application text, for example. Therefore, disclosure of a particular set of program code instructions or detailed hardware devices is not considered necessary for an adequate understanding of how to make and use the invention. The inventive functionality of the claimed computer implemented processes will be explained in more detail in the following description in conjunction with the remaining Figures illustrating other process flows.

Further, certain steps in the processes or process flow described in all of the logic flow diagrams below must naturally precede others for the present invention to function as described. However, the present invention is not limited to the order of the steps described if such order or sequence does not alter the functionality of the present invention. That is, it is recognized that some steps may be performed before, after, or in parallel other steps without departing from the scope and spirit of the present invention.

The processes, operations, and steps performed by the hardware and software described in this document usually include the manipulation of signals by a CPU or remote server and the maintenance of these signals within data structures resident in one or more of the local or remote memory storage devices. Such data structures impose a physical organization upon the collection

Petitioner Samsung Ex-1004, 0594

of data stored within a memory storage device and represent specific electrical or magnetic elements. These symbolic representations are the means used by those skilled in the art of computer programming and computer construction to most effectively convey teachings and discoveries to others skilled in the art.

At step 401, a module 101 can connect with a first wireless network 102. The first wireless network 102 could comprise a public land mobile network, a local area network such as WiFi, or the use of white-space spectrum. The module 101 could connect with the first wireless network 102 in order to obtain access to IP network 111 which could comprise the public Internet, although the IP network 111 could comprise a private network in some embodiments. Although not depicted in Figure 4, a step 401 could also comprise the module 101 connecting to a wired network through USB interface 101v. Upon conclusion of a step 401 the module 101 can use an IP address such as IP address 106b in Figure 1f in order to communicate with an eUICC subscription manager 109. As illustrated in Figure 1f, in an exemplary embodiment the eUICC 107 could also have an IP address 106c after a step 401, although the use of an IP address for eUICC 107 is not required and the module 101 can be associated with one IP address for all external communications.

The module 101 can then use a step 205 in order to receive an eUICC profile 107c. The eUICC profile 107c could be received from the eUICC subscription manager 109 using the wireless network 102 and/or IP network 111 from a step 401 above. The module 101 could record the received eUICC profile 107c with the eUICC 107, including sending the eUICC profile 107c to the eUICC 107 or sharing memory 101e or 101w between the eUICC 107 and a network application 101x. The module 101 could use a network application 101x in order to receive the eUICC profile 107 from the eUICC subscription manager in a step 205, as depicted and described in connection with Figure 3. The module 101 with an eUICC 107 could then decrypt the profile 107c in a step 206 using an eUICC profile key 107b. The eUICC profile key 107b could be recorded with an eUICC 107 before a step 206. The module 101 and/or eUICC 107 could receive the eUICC profile key 107b using a step 303 as depicted and described in

Petitioner Samsung Ex-1004, 0595

connection with Figure 3. The eUICC profile key 107b could be received using a key exchange, such as a Diffie-Hellman key exchange or an ECDH key exchange. Or, the eUICC profile key 107b could be recorded with the eUICC 107 by a module manufacturer. Other possibilities exist as well for a module 101 to record an eUICC profile key 107b before a step 206 without departing from the scope of the present invention. A module 101 and/or an eUICC 107 could use a profile deciphering algorithm 206 in a step 206, as depicted and described in connection with Figure 2a and Figure 2b. Upon conclusion of a step 206, a profile 107d could be recorded in an eUICC 107.

In a step 402, a module 101 can then select and activate the profile 107d from a step 206 in order to connect with a second wireless network 102. A module 101 could take several possible steps in order to select and activate the profile 107d. A module 101 could use radio 101z to search for radio beacons from base stations 103 for wireless networks 102 surrounding the module 101, and upon finding the second wireless network 102 to connect with, the module 101 could select the profile 107d. 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. A module 101 could receive an instruction from an eUICC subscription manager 109 in order to activate the profile 107d, where the instruction could be received through the first wireless network 102 in a step 401 above.

In another embodiment, a module 101 or eUICC 107 could query the eUICC subscription manager 109 through the first wireless network 102 before activating the profile 107d in a step 402. Commercial business arrangements among the user 113 of module 101, the eUICC subscription manager 109, and the mobile network operator 104 can determine the timing for activating a profile 107d for a module 101 with an eUICC 107 in a step 402, such as a user 113 entering a new contract for service with a MNO 104 for the profile 107d. As contemplated herein and throughout the present invention, an activated profile 107d can comprise a selected and enabled network access application state as illustrated in Figure D.1 of ETSI TS 103 383

Petitioner Samsung Ex-1004, 0596

v.2013-02 for the activated profile 107d. Other possibilities exist as well for a module 101 to activate a profile 107d in a step 402 without departing from the scope of the present invention.

In a step 304 in Figure 4, a module 101 using eUICC 107 can conduct a first authentication 304 with the second wireless network 102, using the first key K 203 recorded in the activated profile 107d. The module 101 could also send the first network module identity 202 from a profile 107d to the mobile network operator 104 in a step 304 in Figure 4. The second wireless network 102 in a step 304 in Figure 4 can be associated with a mobile network operator 104. The use of a first authentication 304 is also depicted and described in connection with Figure 3 above. As noted in a first authentication 304, the first key K 203 could comprise a key with a null value in an exemplary embodiment, although a random number could be used for a first key K 203 as well. As depicted in Figure 4, the steps 401 through 304 could comprise substeps within a step 403. The combined substeps comprising a step 403 can be used by a module 101 in exemplary embodiments including an embodiment illustrated in Figure 6 below.

Although not depicted in Figure 4, the mobile network operator 104 can conduct a separate step 308b to authenticate module 101 or a user 113 of module 101 using a second factor after a step 304. As described in a step 308b above, the second factor could comprise verifying or authenticating an identity of a user 113 associated with module 101. Note that the authentication of a user 113 can be conducted through the module 101 accessing a server 105 or a web page through the IP network 111 via the second wireless network 102 after the first authentication 304 using the first key K 203 (including embodiments where the first key K 203 comprises a null value).

In a step 309, the module 101 can receive a key from the second wireless network. The key in a step 309, as depicted in Figure 3 above, can comprise a symmetric key 127 in order to decrypt a ciphertext 208b within profile 107d. As also contemplated and described in connection with a step 309 in Figure 3, the key could comprise a module 101 receiving a ciphertext that includes a symmetric key 127 that has been ciphered with a key ciphering algorithm 216 using an asymmetric ciphering algorithm 219 and the eUICC public key 214, as illustrated in Figure

Petitioner Samsung Ex-1004, 0597

2e. For a key ciphering algorithm 216 used with a step 309, (i) the symmetric key 127 can comprise the plaintext (as opposed to the eUICC profile key 107b depicted in Figure 2e), and (ii) the MNO 104 could operate the key ciphering algorithm 216 instead of the eUICC subscription manager 109 depicted. In this embodiment of a step 309, a module 101 and/or an eUICC 107 could receive the key in the form of a ciphertext of symmetric key 127 in a step 309 and decrypt the ciphertext of symmetric key 127 with the eUICC private key 215 in order to read a plaintext symmetric key 127.

In a step 207 in Figure 4, the module 101 and/or eUICC 107 can decrypt the ciphertext 208b with the second key K 204a using the symmetric key 127. The module 101 can use a key K deciphering algorithm 207 as depicted and described in connection with Figure 2c above in order to read and record a plaintext second key K 204 from the ciphertext 208b in the profile 107d, where the profile 107d was previously decrypted and recorded using a step 206 above. As depicted in Figure 2a, the ciphertext 208b can also include a second network module identity 209a, so the eUICC 107 can also read the plaintext second network module identity 209 in a step 207, if a second network module identity 209a is included in a ciphertext 208b. In an exemplary embodiment, the second plaintext key K 204 is recorded in a protected, nonvolatile memory such as, but not limited to, a flash memory 101w. In this embodiment, the protected nonvolatile memory could comprise a memory address designated by the module 101, CPU 101b, operating system 101h, a module program 101i, or the eUICC 107 as a memory address that can only be written and read by the eUICC 107. Other possibilities exist as well to those of ordinary skill in the art for a plaintext second key K 204 to be recorded in a protected, nonvolatile memory in a step 207 without departing from the scope of the present invention.

In another embodiment, as described in a step 207 in Figure 3, the module 101 could record the encrypted second key K 204a in a nonvolatile memory, along with a symmetric key 127 (or an encrypted symmetric key 127 ciphered by a key ciphering algorithm 216). The module 101 or eUICC 107 could decrypt the encrypted symmetric key 127 in order to decrypt the ciphertext 208b that contains the second key K 204a each time the module 101 or eUICC 107

Petitioner Samsung Ex-1004, 0598

needs to read a plaintext second key K 204 for an conducting an authentication step 310, plus the subsequent derivation of additional keys such as CK and IK, Kasme, Kupenc, etc. using the plaintext second key K 204 and a RAND 118 value.

After reading a plaintext second key K 204 from a ciphertext 208b in a step 207 using the symmetric key 127, the module 101 and/or eUICC 107 can conduct a second authentication 310 step using the plaintext second key K 204, in order to authenticate with the second wireless network 102. The second wireless network 102 can comprise the same wireless network 102 the module 101 communicates with in a step 304 above. The use of a plaintext second key K 204 in a second authentication 310 step is depicted and described in connection with Figure 3. Although not illustrated in Figure 4, the module 101 could send a detach message or equivalent to temporarily disconnect from the second wireless network 102 after a step 309 and before a step 310 illustrated in Figure 4. A step 310 can comprise the module 101 sending a radio resource connection request to the second wireless network 102 with a network module identity associated with the second key K 204. A step 310 can be completed by a module 101 and/or an eUICC 107 sending a RES 119 value calculated using (i) a RAND 118 received and (ii) the second key K 204.

Although not illustrated in Figure 4, after a step 310 by a module 101 and/or an eUICC 107, the MNO 104 could verify the RES 119 and then the module 101 and the wireless network 102 associated with the MNO 104 could take subsequent steps for a module 101 to have access to the IP network 111 including the public Internet. The module 101 and/or eUICC 107 could derive session keys (such as, but not limited to a key CK) for encrypting data through the wireless network using a RAND 118 received in a step 310 and the second key K 204, and the module 101 and/or eUICC 107 could also derive an integrity key for a session (such as, but not limited to, an integrity key IK). Using an authenticated module 101 from a step 310, the MNO 104 can meter services rendered to a module 101 after a step 310 in order to bill or invoice a user 113 or M2M service provider 115.

Petitioner Samsung Ex-1004, 0599

Figure 5a

Figure 5a is a graphical illustration of a public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments. An eUICC 107 within a module 101 can include an eUICC private key 215, which can be associated with an eUICC public key 214. The eUICC private key 215 and eUICC public key 214 can comprise a public key infrastructure (PKI) key pair for eUICC 107. The MNO 104 can record the eUICC public key 214 along with an eUICC identity 107a, such that the MNO 104 can properly associate one of a plurality of eUICC public keys 214 with the proper eUICC 107. Although not illustrated in Figure 5a, a MNO 104 could record the eUICC public key 214 and an associated eUICC identity 107a in a database. The MNO 104 could receive the eUICC public key 214 and the eUICC identity 107a from an eUICC subscription manager 109 through an IP network 111 in a step 302a or step 302b of Figure 3. The use of, source, and additional details regarding an eUICC public key 214 and eUICC private key 215 are also depicted and described in connection with Figure 2d above.

The mobile network operator 104 could also be associated with an MNO private key 501 and an MNO public key 502, which could comprise a PKI key pair for the mobile network operator. The mobile network operator 104 could process or derive the PKI key pair using steps and algorithms equivalent to the steps and algorithms for an eUICC 107 to obtain the eUICC public key 214 and eUICC private key 215. The PKI keys depicted in Figure 5a could be processed using RSA algorithms or elliptic curve cryptography (ECC) algorithms, and other possibilities exist as well for the format of PKI keys without departing from the scope of the present invention. The public keys in Figure 5a can comprise keys recorded in an X.509 certificate, although the use of an X.509 certificates with public keys 214 and 502 are not required. The public key 214 and 502 in the form of an X.509 certificate can optionally be signed by a certificate authority. As illustrated in Figure 5a, the mobile network operator public key 502 can be recorded in the eUICC profile 107d. The MNO 104 could send the MNO public key 502 to the eUICC subscription manager 109 in a step 302a or 302b depicted and described in Figure 3, and the eUICC subscription manager 109 could include the MNO public key 502 in the

Petitioner Samsung Ex-1004, 0600

profile 107d. An eUICC profile 107d could also include the additional data for an eUICC profile 107d as depicted and described in Figure 2a, in addition to the MNO public key 502.

As illustrated in Figure 5a, the MNO 104 and eUICC 107 can both record a key derivation algorithm 503. Exemplary key derivation algorithm 503 could support a Diffie Hellman key exchange, an Elliptic Curve Diffie Hellman (ECDH) key exchange (ECDH), or similar algorithms for each node to mutually derive a key using public and private keys. For embodiments where (A) eUICC public key 214, eUICC private key 215, MNO public key 502, and MNO private key 501 utilize (i) elliptic curve cryptography (ECC) and (ii) a common, shared elliptic curve, then (B) a key derivation algorithm 503 in Figure 5a can comprise an algorithm for conducting an ECDH key exchange. The use of an ECDH key exchange was also described and contemplated between an eUICC subscription manager 109 and an eUICC 107 in step 303 in Figure 3 above. For embodiments where a key derivation algorithm 503 supports a Diffie Hellman key exchange, the key derivation algorithm 503 could record a multiplicative group of integers modulo p, where p is prime, and g is a primitive root mod p. In exemplary embodiments, p can be sufficiently large, such as, but not limited to, and exemplary prime number of at least 250 digits, and g can be a small number, such as, but not limited to, the number 5. In exemplary embodiments, additional values pertaining to the operation of a key derivation algorithm 503 can be transferred between two nodes using a token 505 described in a Figure 5b and Figure 5c below.

Figure 5b

Figure 5b is a graphical illustration of deriving a second key K using public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments. A mobile network operator 104 could process a MNO key exchange algorithm 504 in order to output or determine a second key K 204. A module 101 with an eUICC 107 could process an eUICC key exchange algorithm 505 in order to output or determine the same second key K 204. The MNO key exchange algorithm 504 and the eUICC key exchange algorithm 505 could include a key

Petitioner Samsung Ex-1004, 0601

derivation algorithm 503, and a key derivation algorithm 503 is also depicted and described in connection with Figure 5a above. The MNO 104 and module 101 could share or communicate a key exchange token 506 in order to operate the key exchange algorithm 505. In this manner, a module 101 with an eUICC 107 and a mobile network operator 104 could mutually derive or share the second key K 204 without MNO 104 transmitting or sending the second key K 204, even in an encrypted form such as a second key K 204a in a ciphertext 208b, to either (i) eUICC subscription manager 109 in a step 302a or step 302b, or (ii) to a module 101 in a profile 107c.

For a MNO key exchange algorithm 504, a mobile network operator 104 using a server 105 could input the mobile network operator private key 501, the eUICC public key 214, and a key exchange token 506 into a key derivation algorithm 503 in order to output the second key K 204. Note that the key derivation algorithm 503 in both a MNO key exchange algorithm 504 and an eUICC key exchange algorithm 505 can include additional or separate processing steps than those contemplated in a Diffie-Hellman key exchange and an ECDH key exchange. Additional steps than those contemplated in a Diffie-Hellman key exchange or ECDH key exchange for a key derivation algorithm 503 include transforming key output by these key exchange protocols into a key length and format compatible and suitable for a key K for use with wireless networks. In a key derivation algorithm 503, the output of a Diffie-Hellman key exchange and an ECDH key exchange could be input into a secure hash algorithm, such as SHA-256, which could then be truncated to select a 128 bit second key K 204 using a key derivation algorithm 503. For a MNO key exchange algorithm 504, the security key exchange token 506 can depend upon the algorithm used in a key derivation algorithm 503.

For embodiments where key derivation algorithm 503 comprises a Diffie-Hellman key exchange, the key exchange token 506 can comprise integer values of p and g. Or, with a Diffie-Hellman key exchange the security key exchange token 506 sent from a MNO 104 could comprise a value equal to g^a mod p where (x) the values or p and g have been previously shared between MNO 104 and eUICC 107, and (y) the value "a" can comprise the MNO private key 501. A security key exchange token 506 received by MNO 104 for input into a key derivation

Petitioner Samsung Ex-1004, 0602

algorithm for a eUICC 107 could comprise a value of g^b mod p, where b comprises the eUICC private key 215. For embodiments where key derivation algorithm 503 comprises an ECDH key exchange, the key exchange token 506 can a common base point G. The base point G could also be (i) recorded in an eUICC profile 107d, or (ii) sent from a mobile network operator 104 to module 101, or (iii) sent from the module 101 to the mobile network operator 104. Other algorithms besides an ECDH or Diffie Hellman key exchange can be utilized as well at a step 503, including a key exchange according to the American National Standards Institute (ANSI) standard X-9.63, and a key exchange token 506 could include a number or value associated with these other algorithms for a key derivation algorithm 503.

For an eUICC key exchange algorithm 505, a module 101 with an eUICC 107 could input the eUICC private key 215 and the mobile network operator public key 502 into a key derivation algorithm 503. Note that the input into the key derivation algorithm 503 could also optionally include a key exchange token 506. The key derivation algorithm 503 in an eUICC key exchange algorithm 505 could accept the input and output the second key K 204. The key derivation algorithm 503 in an eUICC key exchange algorithm 505 could be equivalent to the key derivation algorithm 503 in a MNO key exchange algorithm 504 described above. The key exchange token 506 in an eUICC key exchange algorithm 505 could comprise a value similar to the key exchange token 506 used in a MNO key exchange 504 described above. In a Diffie-Hellman key exchange for a key derivation algorithm 503 in a eUICC key exchange algorithm 505, the key exchange token 506 can comprise a value of either (i) integers p and g as described in a MNO key exchange 504, or (ii) number g^a mod p. In an ECDH key exchange for key derivation algorithm 503 in a eUICC key exchange algorithm 505, the key exchange token 506 can comprise a base point G. A key derivation algorithm 503 can output a second key K 204. Other possibilities exist as well for the use of PKI keys and tokens in key exchange algorithms for those of ordinary skill in the art without departing from the scope of the present invention.

Petitioner Samsung Ex-1004, 0603

Figure 5c

Figure 5c is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments. System 500 can include an eUICC subscription manager 109, an IP network 111, a mobile network operator 104, a mobile device 101. A module 101 can include a network application 101x and an eUICC 107. The operation of a system 500 can be similar to a system 300 in Figure 3, except for the steps noted in this Figure 5c where different steps can be taken than those within a Figure 3. As depicted for a system 500 in Figure 5c, like numerals for steps and messages for a system 500 in Figure 5c can comprise like steps and messages within a Figure 3. Different numerals discussed below can comprise different steps or messages for a system 500. Many of the same steps common for a system 500 in Figure 5c and a system 300 in Figure 3 will be summarized in this Figure 5c, while differences between the two systems (including the use of different numerals for different steps or messages) are described in more detail herein. As described in a step 302a and 302b in Figure 3, a mobile network operator 104 can send the eUICC subscription manager 109 information for a profile 107d in a step 302a or 302b, where the information can include the network parameters 201, the first network module identity 202, and the first key K 203. The listed exemplary data for a profile 107d from the previous sentence are also discussed for a profile 107d in Figure 2a.

For a step 507 in a system 500, the MNO 104 can omit sending an encrypted second key K 204a in a ciphertext 208b within the data for the profile 107d. In other words, the profile 107d can omit the second key K 204 in either a plaintext or ciphertext form after a step 507 in a system 500. The second key K 204 for a module 101 with eUICC 107 can be derived by a mobile network operator 104 in a MNO key exchange algorithm 504 and an eUICC key exchange algorithm 505 below in Figure 5c. Thus, in an embodiment illustrated in Figure 5c, the second key K 204 for a second authentication 310 does not need to be transferred to the eUICC subscription manager 109 from MNO 104 for the eUICC subscription manager 109 to include in a profile 107d. Similarly, in a system 500, the second key K 204 does not need to be transferred

Petitioner Samsung Ex-1004, 0604

to the eUICC 107 in a profile 107c. In embodiments where (x) the MNO sends network access credentials such as the first and second network module identities 202 and 209a and a first key K 203 are sent in a step 302b, then (y) a step 507 to omit the sending of the second key K 204 could take place with a step 302b instead of the step 302a as depicted. The MNO 104 can send the first and second network module identities 202 and 209a and a first key K 203 in a step 302a or a step 302b to the eUICC subscription manager 109. The MNO 104 can send to the eUICC subscription manager 109 the first and second network module identities 203 and 209a and a first key K 203 in a profile 107d in a step 302a or 302b, and the eUICC subscription manager 109 could receive the first and second network module identities 202 and 209a and a first key K 203 in a step 302a or a step 302b. Other possibilities for combinations of data sent from a MNO 104 to an eUICC subscription manager 109 in a step 302a, 302b, and 507 without departing from the scope of the present invention.

As depicted in Figure 5c, an eUICC 107 in module 101 could perform steps 301, then step 205 to receive a profile 107c, then receive an eUICC profile key 107b, and then convert the profile 107c into a profile 107d using the eUICC profile key 107b in a step 206. The eUICC profile key 107b could also be (i) ciphered with a key ciphering algorithm 216, sent from the eUICC subscription manager 109 as an encrypted eUICC profile key 218, (ii) and then deciphered by a module 101 and/or eUICC 107 with a step 217, as described in connection with Figure 2e above. The module 101 and/or an eUICC 107 could (i) receive an encrypted eUICC profile key 107b in the form of an key 218 and (ii) use a key deciphering algorithm 217 to decrypt the encrypted eUICC profile key 107b in order (iii) to read a plaintext eUICC profile key 107b and then (iv) use the plaintext eUICC profile key 107b to decrypt the ciphertext 208a.

As depicted in Figure 5c, after a module 101 sends a eUICC identity 107a and receives an eUICC profile 107c in a step 205, the module 101 can conduct a step 206 in order to decrypt a ciphertext 208a that can include a first key K 203 using an eUICC profile key 107b. For the embodiments contemplated in Figure 5c, where the second key K 204 can be derived or determined using a key exchange in steps 504 and 505 below, the second network module

Petitioner Samsung Ex-1004, 0605

identity 209a can be included in the ciphertext 208a (as opposed to being included in the ciphertext 208b as depicted in Figure 2a). One reason can be that a ciphertext 208b can be omitted from an eUICC profile 107d in embodiments where the second key K 204 can be mutually derived by the eUICC 107 and the MNO 104, so there may be no need to include a separate ciphertext 208b within the eUICC profile 107d.

After reading a first network module identity 202 and the first key K 203, the module 101 can conduct a first authentication 304. Note that the first key K 203 can comprise key with a null value, as contemplated in wireless network 102 standards which support the use of emergency services where a module 101 may not include a valid first key K 203. In this case where the first key K 203 comprises a null value, the use of a ciphertext 208a can also be optionally omitted, such that the receipt of an eUICC profile key 107b and the use of a ciphertext 208a could also be optionally omitted and a profile 107c could include plaintext for the first key K 203 and network module identity 202. As depicted and described in connection with Figure 3, a module 101 and MNO 104 could conduct a first authentication step 304 in order to authenticate the module 101 using the first key K 203. The first key K could comprise a non-null value in exemplary embodiments. A step 306 to calculate a first RES 119 value using the first key K 203 from a profile 107d could be included in a first authentication step 304.

The mobile network operator 104 could compare the first received RES 119 with a recorded RES 119 in order to authenticate the module 101 with the eUICC 107 in a step 308a. A mobile network operator 104 can authenticate the module 101 using a step 308a in order to provide access to the IP network 111, and the access to the IP network 111 can be limited (such as, but not limited to excluding access to the public Internet after a step 308a). The module 101 could use access to the limited or restricted IP network 111 in order for a user 113 of module 101 to conduct an authentication with the mobile network operator 104 using a second factor, as described in a step 308b in Figure 3.

After authenticating the module 101 with the first network module identity 202 and the first key K 203 in a step 308a, the mobile network operator 104 could authenticate a user 113 or

Petitioner Samsung Ex-1004, 0606

verify a M2M service provider 115 is associated with the module 101 in a step 308b. The authentication of a user 113 or M2M service provider 115 in a step 308b could comprise authenticating module 101 and/or eUICC 107 with a second factor, where the second factor comprises or includes a secure association of a user 113 or M2M service provider 115 with the module 101. As described in Figure 3 above, a step 308b could result in the secure association of an identity for the user 113 or the M2M service provider 115 with an identity of the module 101. After conduction a step 308b as depicted and described in connection with Figure 3 above, the MNO 104 can record the second network module identity 209 in the eUICC profile 107d is associated with a particular user 113 or a particular M2M service provider 115.

In a step 308b, the MNO 104 can also determine (i) the first network module identity 202 used in step 304 is associated with other identities such as module identity 110, profile identity 107e, eUICC identity 107a, and the second network module identity 209. By (i) authenticating a user 113 or (ii) verifying an identity for module 101 is associated with a M2M service provider 115 in a step 308b, MNO 104 can determine the second network module identity 209 (used in a subsequent authentication step 310) belongs to or is associated with a particular user 113 or M2M service provider 115. In other words, without a separate authentication step 308b in Figure 5 and Figure 3, MNO 104 may not be able to securely determine that the second network module identity 209 from a profile 107d belongs to a particular user 113 or M2M service provider 115. For embodiments where the module 101 is associated with a M2M service provider 115, then a step 308b in Figure 5c could comprise the MNO 104 verifying that an identity received in a first authentication 304 (such as, but not limited to, the first network module identity 202) is associated with an M2M service provider 115, such as checking the identity in a list of identities for modules 101 belonging to M2M service provider 115.

After successfully authenticating or verifying an identity of a user 113 or an M2M service provider 115 is associated with module 101 in a step 308b, MNO 104 could process an MNO key exchange algorithm 504 in order to record a second key K 204 for use in a subsequent second authentication 310 for module 101. The second authentication 310 can use different

Petitioner Samsung Ex-1004, 0607

network access credentials (i) associated with the module 101 and (ii) obtained by module 101 using an eUICC key exchange algorithm 505. Although not illustrated in Figure 5c, a MNO 104 could obtain the data for processing a MNO key exchange algorithm 504 in several different ways. A MNO 104 could receive the eUICC public key 214 for an MNO key exchange algorithm 504 from either (i) the module 101 or eUICC 107 directly after the first authentication 304 or (i) the eUICC subscription manager 109 in a step 302b above, where the eUICC subscription manager 109 could record the eUICC public key 214. Other possibilities exist as well for a MNO 104 to receive an eUICC public key 214 associated with an identity for module 101 such as the eUICC identity 107a. The recording of an eUICC public key 214 with an MNO 104 is also depicted and described in connection with Figure 5a above.

For a MNO key exchange algorithm 504 in Figure 5c, the MNO 104 could also input a key exchange token 506 and a MNO private key 501, in addition to the eUICC public key 214, as illustrated in Figure 5b above. After performing a MNO key exchange algorithm 504 in Figure 5c, the MNO 104 can record the second key K 204 for the second module identity 209 (which is associated with the first module identity 202 in the profile 107d). As contemplated for a key exchange token 506 in Figure 5a and Figure 5c, the key exchange token 506 could be any of the cases (A) initially processed, derived, or determined by the MNO 104, (B) shared between the MNO 104 and module 101 with the eUICC 107, such as, but not limited to, recording the key exchange token 506 in the profile 107d, or (C) initially processed, derived, or determined by module 101. Figure 5c illustrates an embodiment for case (A) with key exchange token 506, where the MNO 104 derives or determines the key exchange token 506 value and subsequent sends the key exchange token 506 value to the module 101 with the eUICC 107. The MNO 104 can send the key exchange token 506 in a message 508, and a network application 101x for the module 101 can receive the key exchange token 506 in the message 508 and forward the key exchange token 506 to the eUICC 107. For case (A) the MNO 104 can omit sending the key exchange token 506 until after the user 113 or M2M service provider 115 for module 101 has been successfully authenticated or verified in a step 308b.

Petitioner Samsung Ex-1004, 0608

In a related embodiment to the embodiment depicted in Figure 5c, for case (B) with key exchange token 506, a separate message 508, to communicate or transfer the key exchange token 506 between the MNO 104 and module 101 after a step 504, can optionally be omitted, since both sides (MNO 104 and module 101) could record the key exchange token 506 before a step 505 by a module 101 with an eUICC 107 below. For case (B), the MNO 104 could send a signal in a message 508 to the module 101 that the authentication step 308b of a user 113 or an M2M service provider 115 has been successfully completed, and thus module 101 could proceed with an eUICC key exchange algorithm 505 using the recorded key exchange token 506.

For case (C) with key exchange token 506, the eUICC 107 could derive or determine the key exchange token 506 and subsequently send the key exchange token 506 to the MNO in a message 508. In this case (C), the MNO 104 could receive the key exchange token 506 (i) before processing the MNO key exchange algorithm 504, and (ii) using the connection with the module 101 from the first authentication 304. For case (C), the MNO 104 can require the successful completion of an authentication step 308b for a user 113 or M2M service provider 115 before accepting the key exchange token 506 from the module 101.

In another exemplary embodiment, step 504 and step 505 can use different values for the key exchange token 506, and both MNO 104 and module 101 can send the tokens 506 in a message 508 to the other node. In exemplary embodiments, a message 508 comprising the key exchange token 506 can be transferred through the IP network 111, where access to the IP network 111 can be enabled by the first authentication 304 with the first key K 203. Other possibilities exist as well for the transfer of a key exchange token 506 between a MNO 104 and a module 101 with an eUICC 107 for conducting a key exchange without departing from the scope of the present invention.

As depicted in Figure 5c, a module 101 with an eUICC 107 can conduct an eUICC key exchange algorithm 505 in order to determine or read a second key K 204. As depicted and described for an eUICC key exchange algorithm 505 in Figure 5b above, the module 101 can input an MNO public key 502, an eUICC private key 215, and the key exchange token 506 into a

Petitioner Samsung Ex-1004, 0609

key derivation algorithm 503 in order to output the second key K 204. Note that the number, value, or sequence of bits for the second key K 204 determined by a MNO 104 in a step 504 can be equal to the number, value, or sequence of bits for the second key K 204 determined by a module 101 with an eUICC 107 in a step 505. The mutual derivation of the second key K 204 by a MNO 104 in a step 504 and a module 101 in a step 505 can be different and superior to conventional technology for either (i) a physical UICC or (ii) an eUICC, since the second key K 204 does not need to be transferred in either physical or electronic form, where the electronic form could include encrypting the second key K 204 into a ciphertext. Supporting the derivation of a second key K 204 as depicted and described herein can be superior to the electronic or physical distribution of a key K, since a different second key K 204 can be utilized by repeating steps 504 and 505 a second time, such as with a different key exchange token 506. In this manner, the second key K 204 associated with the second network module identity 209 could be rotated or changed periodically, thereby increasing the security of a system 500 compared to the use of a static, non-changing second key K 204 for the lifetime of a module 101 with a profile 107d.

After a step 505 in Figure 5c, the subsequent steps and messages for communication between the module 101 and the MNO 104 can be the same or equivalent to those in Figure 3 after a step 207. In other words, the second key K 204 as used by a module 101 and/or eUICC 107 for embodiments in a Figure 5c can be equivalent or similar to the processing and recording steps depicted and described in Figure 3, upon module 101 with an eUICC 107 reading the second key K 204 in a step 207 in Figure 3. In a system 500, the module 101 or eUICC 107 could record the second key K 204 in a protected, nonvolatile memory as described in a step 207 of Figure 3. Other possibilities exist as well without departing from the scope of the present invention for the location or techniques of storing the second key K 204 resulting from a step 505.

As depicted and described in connection with Figure 6 below, the module 101 could record the second key K 204 in a volatile memory (and not storing the second key K 204 in

Petitioner Samsung Ex-1004, 0610

nonvolatile memory), including potentially only within a register or cache memory of CPU 101b. In this manner, the security of the derived second key K 204 can be enhanced, since upon or after power off of a module 101, a third party could not probe or read nonvolatile memory looking for the second key K 204. Since a volatile memory could be flushed upon loss of power or other circumstances, a MNO 104 and module 101 could repeat the steps 504 and 505, respectively, including the transfer of a key exchange token 506, a subsequent time when a module 101 needs to process or derive a new, subsequent second key K 504. In other words, a module 101 can conduct a step 505 with a different key exchange token 506 at a later time after the first instance of a step 505 in order to derive a different, subsequent second key K 204.

After deriving the second key K 204 in a step 505 in Figure 5c, the module 101 with the eUICC 107 can authenticate with the MNO 104 using the wireless network 102, the second network module identity 209, the second key K 204. The module 101 could conduct a second authentication 310 with the mobile network operator using the second key K 204, as depicted in Figure 5c, which is also equivalent to the second authentication 310 depicted in Figure 3 above. Note that the module 101 could detach or disconnect from the wireless network 102 (i) after a sending/receiving a message 508 with key exchange token 506 and (ii) before sending the exemplary second attach message 303 with the second network module identity 209.

The eUICC 107 within module 101 could use (i) the second key K 204 from a step 505, and (ii) a second RAND 118 value from the MNO 104 to calculate a second RES 119 value in a step 311. The eUICC 107 can send the second RES 119 to the network application 101x, and the module 101 can send the second RES 119 to the mobile network operator 104 through the wireless network 102. The MNO 104 could compete the second authentication in a step 312 by verifying the second RES 119 is correct using (i) the second key K 204 derived by the MNO 104 in a step 504 above, and (ii) the second RAND 118 value sent to the module 101. Upon successful authentication using the second key K 204, as depicted and described in connection with Figure 3, the module 101 and MNO 104 could take subsequent steps after a step 312 for the module 101 to have access to the IP network 111 and also the public Internet.

Petitioner Samsung Ex-1004, 0611

In another embodiment contemplated in Figure 5c, the mobile network operator 104 can send the second key K 204 to the module 101 using the wireless network 102 in a message 508. In other words, the exemplary token 506 in Figure 5c could comprise the second key K 204, as opposed to an exemplary key exchange token 506. In this embodiment, the use of a key derivation algorithm 503 in a step 504 could use input of a random number from random number generator 128 into the key derivation algorithm 503 (instead of PKI keys), and the output could be the second key K 204. Or, the key derivation algorithm 503 in a step 504 could simply assign a random number to the second key K 204. After a step 308b and step 504, the mobile network operator 104 could send the second key K 204 in a message 508. The second key K 204 in a message 508 could be encrypted using a key ciphering algorithm 216. The message 508 with the second key K 204 as the token 506 could be received by the module 101 and decrypted using a key deciphering algorithm 217. In another embodiment, the token 506 received by a module 101 could comprise (i) the second key K 204 as plaintext at the application layer, but (ii) ciphered at the data-link layer using the first RAND value from a step 304 and the first key K 203. Other possibilities exist as well for a token 506 to comprise a second key K 204 without departing from the scope of the present invention.

The order of many of the steps and messages depicted within a system 500 could be changed without departing from the scope of the present invention. For example, a step 504 could also be conducted concurrently with a step 302b (instead of with a step 308b), such that a mobile network operator 104 could calculate a second key K 204 using a MNO key exchange algorithm 504 at the same time when MNO 104 sends the first network module identity 202 and first key K 203 to the eUICC subscription manager 109. After receiving (i) an eUICC identity 107a from an eUICC subscription manager 109 and (ii) and an eUICC public key 214 in a step 302b, the mobile network operator 104 can process a MNO key exchange algorithm 504 in order to calculate or process a second key K 204.

In an exemplary embodiment, a mobile network operator 104 could receive a list of eUICC public keys 214 and eUICC identities 107a from an M2M service provider 115 before

Petitioner Samsung Ex-1004, 0612

eUICC subscription manager 109 receives the eUICC identity 107a in a step 205. The MNO 104 could use the data received from a M2M service provider 115 (including a list of eUICC identities 107a and eUICC public keys 214) in order to derive the second key K 204 using a MNO key derivation algorithm 504 and the key exchange token 506. The MNO 104 could send the key exchange token 506 to an eUICC subscription manger 109 before the eUICC subscription manager 109 participates in a step 205 as illustrated in Figure 5c, and the eUICC subscription manager 109 could include the key exchange token 506 with the eUICC profile 107c, such that module 101 could receive the key exchange token 506 in the eUICC profile 107c.

In this embodiment (which can also comprise a case (B) for the transfer of key exchange token 506 for a message 508 as described above), a module 101 using an eUICC 107 with profile 107d and key exchange token 506 could potentially derive the second key K 204 before a step 308b, but in preferred embodiments the mobile network operator 104 does not allow the use of the second key K 204 until after an authentication step 308b of a user 113 or M2M service provider 115. In another embodiment, the values for the first network module identity 202 and the second network module identity 209 could be the same or equal, such that the module 101 uses the same network module identity for both first authentication 304 and a second authentication 310. In this case, the MNO 104 can support a change in key K used with the first network module identity 202 from the first key K 203 to the second key K 204. The first key K 203 can be included in a profile 107d, but the second key K 204 can be derived by an MNO 104 using a step 504 and a module 101 using a step 505. Other possibilities exist as well for a MNO 104 and a module 101 to mutually derive a second key K 204 for use with an eUICC 107 without departing from the scope of the present invention.

Figure 6

Figure 6 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments. An exemplary system 500 depicted and described in connection with Figure 5c can also support the

Petitioner Samsung Ex-1004, 0613

repeated derivation of a second key K 204 for a MNO 104 and module 101 with an eUICC 107. The use and support for different second keys K 204 over time can increase security, since the second key K 204 can be securely and periodically rotated, thereby enhancing the security and efficiency of a system 500, compared to either (i) physically changing a UICC each time a new key K is desired, or (ii) querying, downloading, and selecting a new profile 107c or profile 107d each time the use of a different key K is desired (including steps to communicate and record a second key K 204 in the profile 107d). In other words, the use of multiple second keys K 204 over time can be accomplished for the same profile 107d.

A step 403 in Figure 6 can comprise a module 101 with an eUICC 107 conducting the substeps for a step 403 as depicted and described in connection with Figure 4. In a step 403, a module 101 could connect with a first wireless network 102, receive an eUICC profile 107c, decrypt the profile 107c using an eUICC profile key 107b, activate the profile 107d, and authenticate with a second wireless network 102 using a first key K 203 from the profile 107d. As noted above, other possibilities exist as well for a module 101 to record an eUICC profile 107d, such as the loading of a profile 107d by a manufacturer, without departing from the scope of the present invention.

After successful authentication of the module 101 at the conclusion of a substep 304 in a step 403, a user 113 associated with the module 101 could conduct an authentication step 308b with the mobile network operator 104. A step 308b can be useful for a mobile network operator 104 to authenticate or securely associate (i) a module 101 with (ii) a legal entity contractually responsible for the services used by a module 101. The use of a step 308b is also described in Figure 3. Note that module 101 could be associated with an M2M service provider 115 instead of a mobile phone subscriber such as an individual, and in this case the M2M service provider 115 could take steps before a step 308b in order to inform or confirm with MNO 104 that module 101 with an identity such as module identity 110 or the first network module identity 202 belongs to or is associated with the M2M service provider 115.

Petitioner Samsung Ex-1004, 0614

In other words, a MNO 104 may not have control over the distribution or recipient of a profile 107c from an eUICC subscription manager 109 in a step 403, and a user authentication in a step 308b allows a MNO 104 to confirm, verify, or establish a contractual relationship with a user 113. Business contracts and procedures for an MNO 104 to provide service to a module 101 with an eUICC 107 with profile 107d could require that a user 113 successfully completes an authentication step 308b (with example steps described in Figure 3 above), before the MNO 104 provides service such as voice calls or access to the public Internet. The second factor in a step 308b can be data communicated between the MNO 104 and the user 113 to confirm an identity of the user 113. Examples of data for the second factor in a step 308b are described in connection with a step 308b in Figure 3. The first factor contemplated in a system 300 or system 500 can be the successful receipt of a RES 119 value in a first authentication 304. Upon conclusion of the step 308b the MNO 104 could securely determine and record that a module 101 with the first network module identity 202 and/or the second network module identity 209 from the profile 107d is associated with an authenticated user 113.

The module 101 could then perform a step 508 in order access a key exchange token 506. As described for a key exchange token 506 in Figure 5c, the module 101 could receive the token 506 in a step 508 (case A), or the module 101 could send the token 506 in a step 508 (case B). Step 508 can comprise sending or receiving the message 508 from Figure 5c. The key exchange token 506 could comprise a key exchange token 506 as depicted and described in connection with Figure 5b. Or, as described for a message 508 in Figure 5c, the key exchange token 506 could comprise the second key K 204, such as the second key K 204 encrypted by MNO 104 with a key ciphering algorithm 216 and decrypted by the module 101 with the eUICC 107 using a key deciphering algorithm 217. The key exchange token 506 at a step 508 could comprise parameters for a key derivation algorithm 503, such as a base point G if elliptic curve cryptography PKI keys are used with MNO public key 502, MNO private key 501, eUICC public key 214, and eUICC private key 215.

Petitioner Samsung Ex-1004, 0615

In another exemplary embodiment, key exchange token 506 with a Diffie Hellman key exchange for a key derivation algorithm 503 could comprise a multiplicative group of integers modulo p, where p is prime and g is primitive root mod p. Other possibilities for a key exchange token 506 in a message 508 exist as well without departing from the scope of the present invention, including the use of multiple values and numbers for a key exchange token 506. The key exchange token 506 transfer between MNO 104 and module 101 in a step 508 can use the second wireless network after the module 101 authenticates with the first key K 203, and thus the data-link layer for transfer of the key exchange token 506 could be ciphered using the first key K 203 (where a cipher key for the data-link layer is derived from the first key K 203 and a RAND 118 from a first authentication 304).

A module 101 with an eUICC 107 could then perform a step 505, which could comprise an eUICC key exchange algorithm 505 as depicted in Figure 5c using (i) the token 506 from a message 508 above, and (ii) the eUICC private key 215 and MNO public key 502. The output from an eUICC key exchange algorithm 505 can comprise the second key K 204. In an exemplary embodiment, the second key K 204 output from the eUICC key exchange algorithm 505 is recorded within a memory of module 101 on a temporary basis. After obtaining and reading the second key K 204 from a step 505, the module 101 can conduct a second authentication 310 with the MNO 104 using the second key K 204. The second key K 204 can be associated with a second network module identity 209, which could be recorded in the profile 107c and profile 107d for the eUICC 107 from a step 403 above. Exemplary details and steps for a second authentication 310 using the second key K 204 are depicted and described in connection with Figure 3 and Figure 5c above.

After the conclusion of the second authentication 310, the module 101 could have access to the public Internet through the IP network 111 of the wireless network 102. After a step 310 and before a subsequent step 601 below, the module 101 could continue using the second key K 204 with the second network identity 209 in many additional repeated steps 310, such that module 101 could use the second key K 204 for an exemplary period of time such as several

Petitioner Samsung Ex-1004, 0616

days or several months, and other possibilities exist as well for the continued use of a second key K 204 after a step 310 and before a step 601 in Figure 6. For example, a module 101 could repeat a step 311 in a second authentication 310 multiple times with the same wireless network 102 using the same number of value for the second key K 204 during a period of time before a step 601.

At a step 601 in Figure 6, a module 101 or a MNO 104 could determine if the use of a new second key K 204 is required or preferred. There could be several reasons that a different second key K 204 may be periodically preferred. Exemplary reasons include (i) the second key K 204 may only be temporarily stored within a volatile memory in CPU 101b, such that a power cycle of module 101 or CPU 101b could flush the volatile memory, and in this case module 101 and MNO 104 may need to derive a new second key K 204, (ii) ownership of module 101 may change, and business or legal contracts could stipulate that a previous second key K 204 with the prior owner of module 101 may no longer be valid and thus a new second key K 204 may be required, (iii) a MNO 104 and a module 101 or M2M service provider 102 may prefer to periodically rotate the second key K 204 in order to increase security of a system 500. For example, a module 101 may have a planned lifetime of more than a decade, and given the speed of change for mobile networking technology, a module 101 may prefer to support the change in a second key K 204 for accessing a wireless network 102 without downloading and installing a new, different profile 107d. Other possibilities exists as well for exemplary reasons why a module 101 and/or a MNO 104 could determine that the use of a new, second key K 204 is preferred or required in a step 601 without departing from the scope of the present invention. If a module 101 or MNO 104 determine a value of "no" for a step 601, then the module 101 could continue periodically performing repeated second authentication 310 steps using the same second key K 204, as illustrated in Figure 6.

As depicted in Figure 6, upon determination of a value of "yes" for a step 601, a module 101 could return to a step 508 and receive another key exchange token 506. As depicted in Figure 6, the module 101 could use a first authentication 304, which could comprise an

Petitioner Samsung Ex-1004, 0617

authentication with the first key K 203. A return to the first authentication 304 with the first key K 203 could be omitted in some embodiments, and thus the box for 304 depicted in Figure 6 is a dashed line.

In this embodiment where module 101 or MNO 104 determine or evaluates that a new second key K 204 is preferred at a step 601, the module 101 could return to a step 508 by attaching with the wireless network 102 again using the first network module identity 202 and the first key K 203. For example, if the second key K 204 is not available (such as being flushed from being stored only in a volatile memory, a potential error condition such as a reset of module 101, or the second key K 204 is no longer preferred to be used), then the module 101 with the eUICC 107 could use data recorded in the profile 107d to reconnect with the wireless network 102. For example, the first key K 203 and the first network identity 202 may be recorded in generally accessible nonvolatile memory, such as, but not limited to, a flash memory 101w within module 101 and subsequently the first key K 203 and the first network identity 202 could be used in a step 304 before a return to a step 508. Or, the module 101 and MNO 104 could continue to use the previous second key K 204 (if available) for a communications link to transfer the key exchange token 506, and thus the use of a step 304 with the first key K 203 is optional.

Upon return to a step 508 module 101 and MNO 104 could transfer a key exchange token 506 as described in a step 508 in Figure 6 above. Upon return to a step 508, the module 101 and MNO 104 could transfer a key exchange token 506 that has a different value or number from a key exchange token 506 transferred earlier (in order to support the derivation of a different second key K 204 than from a previous iteration). Using the new, different value for the key exchange token 506, the module 101 with the eUICC 107 could derive a new, different second key K 203. In this manner and by using the steps illustrated in Figure 6, a second key K 204 could operate as a key K for "temporary use", and a different second key K 204 for use in a subsequent authentication 310 could be obtained by a repeated use of a step 505 with a new,

Petitioner Samsung Ex-1004, 0618

different key exchange token 506 for module 101 connecting with the same wireless network 102.

The module 101 and MNO 104 could continue to use the same network module identity (such as a second network module identity 209) upon a return to steps 508 through 310, or the MNO 104 could also send the module 101 a new, different network module identity in a message 508 upon a return to steps 508 through 310. A MNO 104 and a module 101 can repeat the use the steps 508 through 601 depicted and described in this Figure 6 in order to derive a series over time of second keys K 204 for the module 101 with the eUICC 107. Each member of the series (comprising a different second key K 204) could be associated with the second network module identity 209, and the second network module identity 209 could remain constant or can also change to different numbers or values for use in a step 310. Supporting a change in the second key K 204 can both increase the flexibility and security of a system 500 and related systems for a user and a mobile network operator 104.

Conclusion

Various exemplary embodiments have been described above. Those skilled in the art will understand, however, that changes and modifications may be made to those examples without departing from the scope of the claims.

Petitioner Samsung Ex-1004, 0619

CLAIMS

What is claimed is:

1. A method comprising:

(a) generating a first message comprising:

(1) an identity of an embedded universal integrated circuit card;

(2) a nonce; and

(3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;

(b) sending the first message via a network application to a subscription manager system;

(c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;

(d) storing a subscription manager public key which corresponds to a subscription manager private key;

(e) deriving a profile key using a key exchange algorithm based on at least:

(i) the second eUICC private key, and

(ii) the stored subscription manager public key, wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key;

(f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;

(g) receiving the symmetric key;

(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;

(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and

(j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.

2. The method of claim 1, wherein the subscription manager public key is downloaded via the network application.

Petitioner Samsung Ex-1004, 0620

3. The method of claim 1, wherein the step of storing the subscription manager public key occurs at the time of manufacture of the embedded universal integrated circuit card.

4. The method of claim 1, wherein the key exchange algorithm is a Diffie-Hellman key exchange.

5. The method of claim 1, wherein the key exchange algorithm is an Elliptic Curve Diffie-Hellman key exchange.

6. The method of claim 1, wherein the encrypted profile is encrypted in a manner so that intermediate nodes on an IP network would not be able to read data within the profile in an unencrypted form.

7. The method of claim 1, wherein subscription manager system stores the ciphertext and the symmetric key before step (a).

8. The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the identity of the embedded universal integrated circuit card included in the first message.

9. The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the digital signature included in the first message.

10. The method of claim 1, wherein the decrypted ciphertext is stored in nonvolatile memory of the embedded universal integrated circuit card.

11. The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a machine-to-machine module.

Petitioner Samsung Ex-1004, 0621

12. The method of claim 11, wherein the module comprises a module of a type selected from the group consisting of: vending machine, automobile, alarm system, tracking device, monitoring device, security system and remote control device.

13. The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a wireless module.

14. The method of claim 13, wherein the module is configured to communicate using one or more wireless technologies of types selected from the group consisting of: WiFi, WiMax, General Packet Radio Services, Enhanced Data rates for GSM Evolution and 3rd Generation Partnership Project technology.

15. The method of claim 13, wherein the module comprises a module of a type selected from the group consisting of the following: wireless handset, cellular phone, smartphone, laptop computer, tracking device, computer with a radio, circuit board with a radio, hand-held device, netbook, portable computer, multiprocessor system, microprocessor based consumer electronic, programmable consumer electronic, network personal computer, minicomputer, mainframe computer and smartcard.

16. The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module, wherein the module is a wired module.

17. The method of claim 16, wherein the module is configured to communicate using one or more wired connections of types selected from the group consisting of: Ethernet, fiber optic connection and Universal Serial Bus connection.

18. The method of claim 16, wherein the module comprises a module of a type selected from the group consisting of: computer, security camera, security monitoring device and networked controller.

Petitioner Samsung Ex-1004, 0622

19. The method of claim 1, wherein the deriving step (c) is performed prior to the generating step (a).

20. The method of claim 1, wherein the generating step (a) is performed before the deriving step (c).

21. The method of claim 1, wherein the embedded integrated circuit card is operably connected to a module and a user accesses a user interface of the module to enter authentication information before the module receives the symmetric key.

22. The method of claim 1, wherein the subscription manager receives the ciphertext from a mobile network operator before the network application sends the first message.

Petitioner Samsung Ex-1004, 0623

ABSTRACT

A module with an embedded universal integrated circuit card (eUICC) can include a profile for the eUICC. The profile can include a first and second shared secret key K for authenticating with a wireless network. The first shared secret key K can be encrypted with a first key, and the second shared secret key K can be encrypted with a second key. The module can (i) receive the first key, (ii) decrypt the first shared secret key K with the first key, and (iii) subsequently authenticate with the wireless network using the plaintext first shared secret key K. The wireless network can authenticate the user of the module using a second factor. The module can then (i) receive the second key, (ii) decrypt the second shared secret key K, and (iii) authenticate with the wireless network using the second shared secret key K. The module can comprise a mobile phone.

Petitioner Samsung Ex-1004, 0624

Application Data Sheet 37 CFR 1.76

The Application Data Sheet is part of the provisional or non-provisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.

Inventor Information

of inventors: 1

1. **John A. Nix**

Residence Information
US Residency
Evanston, IL
UNITED STATES

Mailing Address
807 Davis Street, Unit 409
Evanston, IL 60201
UNITED STATES

Application Information

Customer number	1912 -
Correspondence address	---
Title of invention	**Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication**
Attorney docket number	63121/0226
Entity status	Small
Application type	Nonprovisional Application under 35 USC 111(a)

Petitioner Samsung Ex-1004, 0625

Subject matter	Utility
Total number of drawing sheets	12
Suggested figure for publication	----
Filing by reference	No
Publication request	Normal eighteen-month publication

Representative Information

of representatives: 1

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).

Customer number 1912

Domestic Benefit/National Stage Information

of benefit claims: 6

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c), 386(c), or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior app status	Pending
Application number	----
Continuity type	**Continuation of**
Prior app number	**17547990**
Filing Date	12/10/2021

Prior app status	Patented
Application number	**17547990**
Continuity type	**Continuation of**

Petitioner Samsung Ex-1004, 0626

Prior app number	16453682
Filing Date	06/26/2019
Patent number	11233780
Issue date	01/25/2022

Prior app status	Patented
Application number	16453682
Continuity type	Continuation in part of
Prior app number	16110804
Filing Date	08/23/2018
Patent number	10382422
Issue date	08/13/2019

Prior app status	Patented
Application number	16110804
Continuity type	Continuation of
Prior app number	15928848
Filing Date	03/22/2018
Patent number	10084768
Issue date	09/25/2018

Prior app status	Patented
Application number	15928848
Continuity type	Continuation of
Prior app number	14751119
Filing Date	06/25/2015
Patent number	9961060
Issue date	05/01/2018

Prior app status	Patented
Application number	14751119
Continuity type	Continuation of
Prior app number	14099329
Filing Date	12/06/2013
Patent number	9100175
Issue date	08/04/2015

Petitioner Samsung Ex-1004, 0627

Foreign Priority Information

of foreign priority claims: 0

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the Application Data Sheet constitutes the claim for priority as required by 35 U.S.C. 119 (b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Data was not provided for this section.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

Checking this box will cause the application to be examined under the first inventor to file provisions of the AIA.

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013. NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 2016, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization or Opt-Out of Authorization to Permit Access

When this Application Data Sheet is properly signed and filled with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE:
This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. **Priority Document Exchange (PDX)**
Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual

Petitioner Samsung Ex-1004, 0628

Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h) (1).

B. Search Results from U.S. Application to EPO

Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby grants the USPTO authority to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant DOES NOT authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant DOES NOT authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with the search results from the instant application.

NOTE:
Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Applicant Information

of applicants: 1

The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46.

1. **Network-1 Technologies, Inc.**
445 Park Avenue, Suite 912
New York, NY 10022
UNITED STATES

Phone: ----
Fax: ----
Email: ----

Applicant: Organization
Applicant type: Assignee

Assignee Information including Non-Applicant Assignee Information

of assignees: 0

Petitioner Samsung Ex-1004, 0629

An assignee-applicant identified in the "Applicant" section will appear on the patent application as an applicant.

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Data was not provided for this section.

Signature

NOTE:

This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c)**

This Application Data Sheet must be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, all joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of all joint inventor-applicants.

See CFR 1.4(d) for the manner of making signatures and certifications.

Signature	First name	Last name	Registration #	Date
/Keith J. Barkaus/	Keith J.	Barkaus	51,431	01/18/2024

Petitioner Samsung Ex-1004, 0630

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/416,534	01/18/2024 05:14:14 PM Z ET	63121/0226

Title of Invention

Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7559	FILED BY	Victoria GILMORE
PATENT CENTER #	63978386	AUTHORIZED BY	Keith Barkaus
CUSTOMER #	1912	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	John A. Nix

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1051	E20241HH15186969	Victoria GILMORE

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2202	EACH CLAIM IN EXCESS OF 20	40.00	2	80.00
2111	UTILITY PATENT APPL. SEARCH FEE	280.00	1	280.00
4011	BASIC FILING FEE- UTILITY	64.00	1	64.00
2311	EXAMINATION OF ORIGINAL PATENT APPLICATION	320.00	1	320.00
2081	UTILITY APPL. SIZE FEE > THAN 100 PAGES (FEE X PAGES >= 101 IN 50 PAGE INCREMENTS)	168.00	1	168.00
			TOTAL	$912.00

AMOUNT:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.